Universidad de Buenos Aires
Facultad de Ciencias Económicas

Los Controles y su Ocasión

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

En el ámbito de los Sistemas de Información (SI – *Information Systems*), el concepto de **control** constituye un pilar esencial de la gobernanza, la seguridad y la gestión del riesgo organizacional. Un control puede definirse como cualquier política, procedimiento, mecanismo técnico o acción diseñada para prevenir, detectar, corregir o mitigar riesgos que puedan afectar los activos de información de una organización.

En entornos digitales complejos, donde los procesos operativos, financieros y estratégicos dependen de plataformas tecnológicas, los controles permiten reducir la probabilidad de errores, fraudes, interrupciones o pérdidas de datos. Desde la perspectiva de la administración, los controles no deben entenderse únicamente como herramientas técnicas, sino como instrumentos estratégicos que protegen la continuidad del negocio y la confiabilidad de la información.

En la teoría del control interno y en la práctica de auditoría, los controles suelen clasificarse en **preventivos**, **detectivos**, **correctivos** y **recuperatorios**. Esta clasificación responde a su función dentro del ciclo de gestión del riesgo. Es fundamental remarcar que:

> **El mejor control es el que evita problemas (controles preventivos), luego le siguen los que identifican un problema ya que permiten tomar medidas de investigación y corrección (controles detectivos) y por**

> **último los controles para corregir un problema (controles correctivos o de recuperabilidad).**

Comprender esta jerarquía permite a los futuros administradores diseñar arquitecturas de control más eficientes y sostenibles en entornos tecnológicos.

Desarrollo

1. Definición General de Control en Sistemas de Información

Un control es un mecanismo diseñado para reducir la probabilidad o el impacto de un riesgo. En el contexto de TI, los controles pueden aplicarse sobre:

- Hardware.
- Software.
- Bases de datos.
- Redes.
- Usuarios.
- Procesos.
- Servicios en la nube.

Desde el punto de vista metodológico, los controles forman parte del sistema de control interno, alineado con marcos como:

- **COSO (Committee of Sponsoring Organizations / Comité de Organizaciones Patrocinadoras)**.
- **COBIT (Control Objectives for Information and Related Technologies / Objetivos de Control para Tecnologías de la Información y Relacionadas)**.
- **ISO 27001** para gestión de seguridad de la información.

El diseño adecuado de controles responde a la ecuación de riesgo:

Riesgo = Amenaza × Vulnerabilidad × Impacto.

Los controles reducen vulnerabilidades y, en consecuencia, la exposición al riesgo.

---

2. Controles Preventivos

2.1 Concepto

Los **controles preventivos** son aquellos diseñados para impedir que ocurra un evento no deseado. Actúan antes de que el riesgo se materialice.

Son considerados los controles más eficientes, ya que evitan pérdidas antes de que se produzcan.

2.2 Ejemplos en TI

- Autenticación multifactor (MFA – *Multi-Factor Authentication* / Autenticación Multifactor).
- Validaciones de datos en sistemas.
- Segregación de funciones.
- Políticas de contraseñas robustas.
- Firewalls.
- Actualización de parches de seguridad.
- Restricciones de acceso basadas en roles (RBAC – *Role-Based Access Control* / Control de Acceso Basado en Roles).

2.3 Impacto Estratégico

Los controles preventivos reducen costos asociados a:

- Incidentes de seguridad.
- Fraudes.
- Interrupciones operativas.
- Sanciones regulatorias.

Desde la administración, invertir en prevención resulta más eficiente que asumir costos de recuperación.

---

3. Controles Detectivos

3.1 Concepto

Los **controles detectivos** identifican eventos adversos después de que han ocurrido o mientras están ocurriendo.

Su función principal es alertar y permitir acciones correctivas.

3.2 Ejemplos en TI

- Sistemas de monitoreo de eventos (SIEM – *Security Information and Event Management* / Gestión de Eventos e Información de Seguridad).
- Alertas automáticas por intentos fallidos de acceso.
- Auditorías de registros (logs).
- Conciliaciones contables.
- Revisiones periódicas de permisos de usuario.

3.3 Importancia

Permiten:

- Detectar fraudes.
- Identificar intrusiones.
- Evaluar anomalías.
- Iniciar investigaciones.

Aunque no evitan el evento inicial, reducen el tiempo de exposición.

---

4. Controles Correctivos

4.1 Concepto

Los **controles correctivos** actúan después de que se ha detectado un problema, con el objetivo de corregirlo o mitigar sus efectos.

4.2 Ejemplos

- Eliminación de malware.
- Bloqueo de cuentas comprometidas.
- Reconfiguración de sistemas vulnerables.

- Aplicación de parches posteriores a incidentes.

Estos controles restauran la situación, pero el daño inicial ya ocurrió.

---

5. Controles Recuperatorios

Los **controles recuperatorios** permiten restablecer operaciones luego de un incidente significativo.

5.1 Ejemplos

- Backups periódicos.
- Plan de Recuperación ante Desastres (DRP – *Disaster Recovery Plan*).
- Plan de Continuidad del Negocio (BCP – *Business Continuity Plan*).
- Replicación de bases de datos.

Su objetivo es minimizar la interrupción y recuperar información crítica.

---

6. Jerarquía de Eficiencia de los Controles

La eficacia de los controles puede representarse de la siguiente manera:

1. Preventivos (evitan el problema).
2. Detectivos (identifican el problema).
3. Correctivos/Recuperatorios (corrigen o mitigan el problema).

Desde el punto de vista económico y estratégico:

- La prevención reduce costos.
- La detección reduce impacto.
- La corrección restaura operaciones.

Una arquitectura de control madura prioriza prevención.

---

7. Ejemplo Integrado

Supongamos una empresa que gestiona pagos digitales.

Riesgo: fraude interno.

Controles preventivos:

- Segregación de funciones.
- Autenticación multifactor.
- Límites de autorización.

Controles detectivos:

- Alertas por transacciones inusuales.
- Auditoría de logs.

Controles correctivos:

- Bloqueo de cuenta.
- Investigación interna.

Controles recuperatorios:

- Recuperación de datos.
- Reversión de transacciones.

El diseño integral permite resiliencia organizacional.

---

8. Integración con Gestión de Riesgos

Los controles deben diseñarse tras identificar:

- Activos críticos.
- Amenazas.
- Vulnerabilidades.

No todos los riesgos requieren el mismo nivel de control; el análisis costo-beneficio es fundamental.

---

9. Dimensión Administrativa

Para los administradores, los controles:

- Garantizan confiabilidad de la información.
- Facilitan auditorías.

- Reducen responsabilidad legal.
- Fortalecen gobernanza.
- Mejoran confianza del mercado.

El diseño adecuado de controles es una decisión estratégica.

Conclusión

Los controles en los sistemas de información constituyen mecanismos fundamentales para gestionar riesgos en entornos digitales. Su clasificación en preventivos, detectivos, correctivos y recuperatorios permite comprender su función dentro del ciclo de protección organizacional.

Es esencial enfatizar que **el mejor control es el que evita problemas (controles preventivos)**, ya que reduce la probabilidad de materialización del riesgo. En segundo lugar, los controles detectivos permiten identificar situaciones adversas y tomar medidas correctivas. Finalmente, los controles correctivos y recuperatorios mitigan o restauran operaciones luego de ocurrido el incidente.

Desde la perspectiva de la administración y la gobernanza tecnológica, el diseño de una arquitectura de control equilibrada y priorizada en la prevención es indispensable para garantizar la sostenibilidad, resiliencia y competitividad organizacional en un entorno digital complejo.

Preguntas de autoevaluación

1. ¿Cuál es la diferencia entre un control preventivo y uno detectivo?
2. ¿Por qué los controles preventivos son considerados los más eficientes?
3. ¿En qué se diferencian los controles correctivos de los recuperatorios?
4. ¿Cómo se relacionan los controles con la gestión de riesgos en TI?
5. ¿Por qué el diseño estratégico de controles es responsabilidad de la administración?

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.