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 y su Ocasión

Presentación del tema

En el ámbito de los Sistemas de Información (SI), 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. Su clasificación según la ocasión en que actúan —preventivos, detectivos, correctivos y recuperatorios— determina su eficiencia relativa y orienta las decisiones de inversión en seguridad.

El principio fundamental que subyace a esta clasificación es que el mejor control es el que evita problemas antes de que ocurran. Le siguen en eficiencia los controles que identifican un problema ya producido, permitiendo tomar medidas de investigación y corrección; y finalmente los controles destinados a corregir un problema una vez ocurrido. Para los estudiantes de la Licenciatura en Administración, comprender esta jerarquía permite diseñar arquitecturas de control más eficientes, proporcionales al riesgo y sostenibles en entornos tecnológicos complejos.

Controles preventivos

Los controles preventivos están diseñados para impedir que ocurra un evento no deseado. Actúan antes de que el riesgo se materialice y son considerados los más eficientes, ya que evitan pérdidas antes de que se produzcan. En TI, sus ejemplos más representativos son la autenticación multifactor (MFA), las validaciones de datos en sistemas, la segregación de funciones, las políticas de contraseñas robustas, los firewalls, la actualización de parches de seguridad y las restricciones de acceso basadas en roles (RBAC).

Desde la administración, invertir en prevención resulta significativamente más eficiente que asumir los costos de recuperación. Los controles preventivos reducen los costos asociados a incidentes de seguridad, fraudes, interrupciones operativas y sanciones regulatorias.

Controles detectivos

Los controles detectivos identifican eventos adversos después de que han ocurrido o mientras están ocurriendo. Su función principal es alertar y permitir acciones correctivas. Aunque no evitan el evento inicial, reducen el tiempo de exposición. En TI, sus ejemplos incluyen los sistemas SIEM, las alertas automáticas por intentos fallidos de acceso, las auditorías de registros (logs), las conciliaciones contables y las revisiones periódicas de permisos de usuario.

Desde la perspectiva administrativa, permiten detectar fraudes, identificar intrusiones, evaluar anomalías e iniciar investigaciones. Su efectividad depende de que sean revisados activamente: un log no monitoreado no cumple su función de control.

Controles correctivos

Los controles correctivos buscan revertir el daño producido por un incidente y restaurar el sistema a su estado anterior. Incluyen los planes de recuperación ante desastres (DRP), los respaldos (Backup), los procedimientos de restauración de sistemas, los planes de continuidad del negocio (BCP) y los protocolos de gestión de incidentes. En el plano técnico, también incluyen la aplicación de parches correctivos (hotfixes) y la restauración de versiones anteriores.

Controles recuperatorios

Los controles recuperatorios se centran en restablecer la capacidad operativa tras un evento disruptivo. Se diferencian de los correctivos en que su objetivo no es revertir el daño específico sino recuperar la capacidad de funcionamiento de la organización. Ejemplos incluyen la activación del sitio de recuperación (recovery site), la implementación del BCP y la comunicación de crisis.

La jerarquía de eficiencia y el análisis costo-beneficio

Tipo de control	Momento de acción	Eficiencia relativa	Costo si se omite
Preventivo	Antes del evento	Más alta	Mayor
Detectivo	Durante o post-evento	Alta	Elevado
Correctivo	Después del evento	Media	Menor si es temprano
Recuperatorio	Restauración operativa	Dependiente de la preparación	Muy alto

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. Marcos como COSO, COBIT e ISO 27001 integran esta clasificación en sus estructuras de control interno.

Conceptos clave

- La jerarquía de controles: prevenir es más eficiente que detectar o corregir.
- Controles preventivos: actúan antes del evento y tienen el mayor retorno.
- Controles detectivos: identifican el evento para limitar su exposición.
- Controles correctivos: reducen el impacto tras el incidente.
- Controles recuperatorios: restablecen la capacidad operativa.
- Análisis costo-beneficio como criterio de priorización de controles.

Preguntas de repaso del tema

1. ¿Por qué los controles preventivos son considerados los más eficientes?

2. ¿Qué diferencia existe entre controles detectivos y controles correctivos?
3. ¿Por qué un log no monitoreado no cumple su función de control?
4. ¿Qué relación existe entre la ecuación de riesgo y la clasificación de controles?
5. ¿Por qué la inversión en prevención resulta más eficiente que la inversión en recuperación?
6. ¿Cómo se integra esta clasificación en marcos como COBIT e ISO 27001?
7. ¿Qué ejemplos de controles preventivos son más relevantes en sistemas financieros?
8. ¿Cuándo es más conveniente fortalecer los controles detectivos en lugar de los preventivos?
9. ¿Qué papel cumple el análisis costo-beneficio en el diseño de controles?
10. ¿Cómo se relacionan los controles recuperatorios con los planes BCP y DRP?