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**.

Controles para la Seguridad de los Datos

Presentación del tema

Los controles para la seguridad de datos constituyen el conjunto de mecanismos técnicos, administrativos y organizacionales destinados a proteger la información frente a accesos no autorizados, alteraciones indebidas, pérdidas accidentales o destrucción maliciosa. En el contexto de las Tecnologías de la Información (IT), los datos representan uno de los activos más valiosos de la organización: contienen información financiera, estratégica, comercial, operativa y personal cuya protección resulta crítica para la sostenibilidad del negocio.

La seguridad de los datos se estructura en torno al modelo clásico CIA —confidencialidad, integridad y disponibilidad—, que define los tres atributos esenciales que deben preservarse. Para los estudiantes de la Licenciatura en Administración, comprender los controles de seguridad de datos implica reconocer que la protección de la información no es únicamente un asunto técnico, sino una decisión estratégica vinculada con la gestión del riesgo, el cumplimiento normativo, la reputación corporativa y la ventaja competitiva.

Controles preventivos

Los controles preventivos buscan impedir que ocurra un incidente.

Cifrado (Encryption). Transforma la información en un formato ilegible para usuarios no autorizados. Puede aplicarse en tránsito (Data in Transit), en reposo (Data at Rest) y de extremo a extremo (End-to-End Encryption). El cifrado reduce significativamente el impacto de accesos indebidos incluso si el sistema es comprometido.

Control de acceso. Los mecanismos RBAC, MFA y el principio de mínimo privilegio limitan quién puede visualizar, modificar o eliminar datos.

Clasificación de la información. Categoriza los datos según su nivel de sensibilidad —pública, interna, confidencial y crítica— orientando el nivel de protección requerido para cada categoría.

Prevención de pérdida de datos (DLP). Las soluciones DLP (Data Loss Prevention) monitorean y bloquean transferencias indebidas de información sensible, como el envío de bases de datos por correo electrónico o la copia en dispositivos USB.

Controles detectivos

Los controles detectivos identifican incidentes en curso o posteriores. El SIEM centraliza registros de actividad y detecta comportamientos anómalos. El monitoreo de integridad verifica si archivos críticos han sido modificados sin autorización. Las auditorías internas y externas evalúan el cumplimiento de políticas y normativas.

Controles correctivos

Los controles correctivos reducen el impacto después de un incidente. El respaldo de información (Backup) debe contemplar copias periódicas, almacenamiento fuera de sitio y pruebas de restauración. La regla 3-2-1 establece tres copias en dos medios diferentes, con al menos una copia fuera del sitio principal. El DRP define procedimientos para restaurar sistemas y datos tras incidentes graves.

Integridad, calidad y cumplimiento normativo

La seguridad no se limita a la confidencialidad: la integridad implica que los datos no sean alterados sin autorización. Los controles de integridad incluyen funciones de resumen criptográfico (Hashing), validaciones automáticas y registros de cambios. La calidad de los datos es un componente esencial para decisiones estratégicas confiables.

La seguridad de datos está vinculada con regulaciones de protección de datos personales, estándares ISO/IEC 27001 y regulaciones sectoriales. El incumplimiento puede derivar en multas significativas, pérdida de licencias y daño reputacional. La inversión en

seguridad de datos no debe concebirse como gasto, sino como protección del valor organizacional.

Conceptos clave

- CIA como modelo de los tres atributos esenciales de la seguridad de datos.
- Controles preventivos, detectivos y correctivos como categorías complementarias.
- Cifrado en tránsito y en reposo como mecanismo esencial de protección.
- DLP para prevenir filtraciones de información sensible.
- Regla 3-2-1 como estrategia de respaldo de información.
- Integridad de los datos como condición de la calidad informacional.

Preguntas de repaso del tema

1. ¿Cuáles son las diferencias entre controles preventivos, detectivos y correctivos?
2. ¿Por qué el cifrado es un mecanismo esencial en la protección de información crítica?
3. ¿Qué función cumplen los sistemas DLP en la prevención de filtraciones?
4. ¿Cómo se integra la gestión del riesgo en el diseño de controles de seguridad de datos?
5. ¿Por qué la seguridad de datos debe considerarse una decisión estratégica?
6. ¿Qué implica la regla 3-2-1 en la estrategia de respaldo de información?
7. ¿Por qué la integridad de los datos es igualmente importante que la confidencialidad?

8. ¿Cómo se vincula la clasificación de la información con el nivel de protección requerido?
9. ¿Qué consecuencias regulatorias puede tener una brecha de seguridad de datos?
10. ¿Cómo afectan los controles de seguridad de datos a la calidad de las decisiones estratégicas?