Universidad de Buenos Aires
Facultad de Ciencias Económicas

Controles para la Seguridad de Datos

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 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 (TI), 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 (Confidentiality, Integrity, Availability / Confidencialidad, Integridad y Disponibilidad)**, que define los tres atributos esenciales que deben preservarse. A partir de este modelo se diseñan controles que abarcan desde el cifrado (encryption) y la gestión de accesos hasta los respaldos, la clasificación de información y el monitoreo continuo.

Para estudiantes de 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.

Desarrollo

1. Naturaleza Estratégica de los Datos en las Organizaciones

En entornos digitales contemporáneos, los datos constituyen el insumo fundamental para:

- Toma de decisiones basada en evidencia.
- Inteligencia de negocios (BI – *Business Intelligence* / Inteligencia de Negocios).
- Analítica avanzada.
- Automatización de procesos.
- Transformación digital.

La pérdida, alteración o exposición indebida de datos puede generar:

- Sanciones regulatorias.
- Pérdidas financieras.
- Daño reputacional.
- Interrupción operativa.

En consecuencia, los controles de seguridad deben diseñarse en función del nivel de criticidad de la información.

---

2. Clasificación de los Controles de Seguridad de Datos

Los controles pueden clasificarse en:

1. Controles Preventivos.
2. Controles Detectivos.
3. Controles Correctivos.

Asimismo, pueden diferenciarse según su naturaleza:

- Técnicos.
- Administrativos.
- Físicos.

---

3. Controles Preventivos

Los controles preventivos buscan impedir que ocurra un incidente.

3.1 Cifrado (Encryption / Cifrado)

El cifrado transforma la información en un formato ilegible para usuarios no autorizados.

Tipos:

- Cifrado en tránsito (Data in Transit).
- Cifrado en reposo (Data at Rest).
- Cifrado de extremo a extremo (End-to-End Encryption).

Algoritmos como AES (Advanced Encryption Standard / Estándar Avanzado de Cifrado) son ampliamente utilizados en entornos corporativos.

El cifrado reduce significativamente el impacto de accesos indebidos.

3.2 Control de Acceso

Los mecanismos de control de acceso, tales como:

- RBAC (Role-Based Access Control / Control de Acceso Basado en Roles).
- MFA (Multi-Factor Authentication / Autenticación Multifactor).
- Principio de Mínimo Privilegio.

limitan quién puede visualizar, modificar o eliminar datos.

3.3 Clasificación de la Información

La clasificación de datos permite categorizar la información según su nivel de sensibilidad:

- Pública.

- Interna.
- Confidencial.
- Crítica.

Esta segmentación orienta el nivel de protección requerido.

---

4. Controles Detectivos

Los controles detectivos permiten identificar incidentes en curso o posteriores.

4.1 Sistemas SIEM

El **SIEM (Security Information and Event Management / Gestión de Información y Eventos de Seguridad)** centraliza registros de actividad y detecta comportamientos anómalos.

4.2 Monitoreo de Integridad

Herramientas de monitoreo verifican si archivos críticos han sido modificados sin autorización.

4.3 Auditorías

Auditorías internas y externas evalúan el cumplimiento de políticas y normativas.

---

5. Controles Correctivos

Estos controles reducen el impacto después de un incidente.

5.1 Respaldo de Información (Backup)

La estrategia de respaldo debe contemplar:

- Copias periódicas.
- Almacenamiento fuera de sitio.
- Pruebas de restauración.

La regla 3-2-1 establece:

- 3 copias.

- 2 medios diferentes.
- 1 copia fuera del sitio principal.

5.2 Plan de Recuperación ante Desastres

El **DRP (Disaster Recovery Plan / Plan de Recuperación ante Desastres)** define procedimientos para restaurar sistemas y datos tras incidentes graves.

---

6. Seguridad en la Nube

En entornos de **Cloud Computing (Computación en la Nube)**, la seguridad de datos requiere:

- Gestión de identidad (IAM – Identity and Access Management / Gestión de Identidad y Acceso).
- Configuraciones seguras.
- Cifrado obligatorio.
- Evaluación de proveedores.

Errores de configuración en servicios cloud representan una de las principales causas de filtraciones de datos.

---

7. Prevención de Pérdida de Datos

Las soluciones **DLP (Data Loss Prevention / Prevención de Pérdida de Datos)** monitorean y bloquean transferencias indebidas de información sensible.

Ejemplo:

- Bloqueo de envío de bases de datos por correo electrónico.
- Restricción de copiado en dispositivos USB.

---

8. Integridad y Calidad de Datos

La seguridad no se limita a la confidencialidad. La integridad implica que los datos no sean alterados sin autorización.

Controles de integridad incluyen:

- Hashing (funciones de resumen criptográfico).
- Validaciones automáticas.
- Registros de cambios (Logs).

La calidad de datos es un componente esencial para decisiones estratégicas confiables.

---

9. Protección contra Malware

Los datos pueden verse comprometidos por:

- Ransomware.
- Virus.
- Spyware.

Controles relevantes:

- Antivirus.
- Firewalls.
- Segmentación de red.
- Actualización de parches.

---

10. Cumplimiento Normativo

La seguridad de datos está vinculada con regulaciones como:

- Normas de protección de datos personales.
- Estándares ISO/IEC 27001.
- Regulaciones sectoriales financieras.

El incumplimiento puede derivar en multas significativas.

---

11. Gestión del Riesgo de Datos

El análisis de riesgo permite priorizar controles.

Riesgo = Amenaza × Vulnerabilidad × Impacto.

Si el impacto de una filtración financiera es alto, el nivel de cifrado y monitoreo debe ser proporcional.

---

12. Ejemplo Aplicado

Una empresa almacena información de clientes sin cifrado y sin respaldo externo.

Amenaza: ransomware.

Vulnerabilidad: falta de protección.

Impacto: paralización operativa y pérdida de datos.

Implementando cifrado, backup 3-2-1 y MFA, el riesgo disminuye sustancialmente.

---

13. Dimensión Administrativa

Desde la perspectiva de la administración, los controles de seguridad de datos deben:

- Integrarse en la planificación estratégica.
- Evaluarse mediante análisis costo-beneficio.
- Justificarse mediante métricas de riesgo.
- Alinearse con el gobierno corporativo.

La inversión en seguridad no debe concebirse como gasto, sino como protección del valor organizacional.

Conclusión

Los controles para la seguridad de datos constituyen un elemento estructural en la arquitectura de protección de los sistemas de información. A través de mecanismos preventivos, detectivos y correctivos, las organizaciones reducen la probabilidad de incidentes y minimizan su impacto.

La implementación de cifrado, control de accesos, clasificación de información, respaldo periódico y monitoreo continuo fortalece la resiliencia organizacional frente a amenazas crecientes en entornos digitales complejos. Desde la

perspectiva administrativa, la seguridad de datos debe abordarse como una inversión estratégica orientada a preservar la continuidad del negocio, el cumplimiento normativo y la confianza del mercado.

En una economía basada en información, proteger los datos equivale a proteger la esencia misma del modelo organizacional.

Preguntas de autoevaluación

1. ¿Qué diferencias existen entre controles preventivos, detectivos y correctivos en la seguridad de datos?
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 y no únicamente técnica?

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.