Universidad de Buenos Aires
Facultad de Ciencias Económicas

La Seguridad Informática en la Administración de Empresas

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

Seguridad Informática: concepto, importancia estratégica, alcance y políticas técnicas y administrativas para las empresas

1. Presentación del Tema

La **Seguridad Informática** puede definirse como el conjunto de políticas, procedimientos, controles técnicos y administrativos orientados a proteger los activos de información de una organización frente a amenazas internas y externas, garantizando la **confidencialidad (Confidentiality)**, **integridad (Integrity)** y **disponibilidad (Availability)** de los datos. Este triángulo conceptual es conocido como la **Triada CIA (Confidentiality, Integrity, Availability)** o **CID (Confidencialidad, Integridad y Disponibilidad)**.

Desde la perspectiva de las Tecnologías de la Información (TI), la seguridad informática no constituye únicamente un problema técnico vinculado a servidores, redes o contraseñas, sino una **dimensión estratégica del gobierno corporativo (Corporate Governance)**. Las organizaciones modernas dependen estructuralmente de sistemas de información (Information Systems, IS) que

soportan procesos críticos: facturación electrónica, comercio digital, gestión de recursos humanos, contabilidad, logística, inteligencia de negocios (Business Intelligence, BI), entre otros.

En consecuencia, una vulneración de la seguridad puede afectar no solo la operación tecnológica sino también la reputación, la responsabilidad legal, el cumplimiento normativo (compliance) y la sostenibilidad económica de la empresa. Para los estudiantes de licenciatura en administración, comprender la seguridad informática implica entender cómo se integran los controles tecnológicos con la estrategia empresarial, la gestión del riesgo y la toma de decisiones.

---

2. Desarrollo

2.1 Concepto ampliado y fundamentos

La seguridad informática se basa en la gestión del **riesgo (Risk Management)** aplicado a los activos digitales. Un riesgo se compone de tres elementos:

- **Activo (Asset)**: información, sistemas, bases de datos, infraestructura, software.
- **Amenaza (Threat)**: evento potencial que puede causar daño (ataque externo, error humano, malware).
- **Vulnerabilidad (Vulnerability)**: debilidad que puede ser explotada por una amenaza.

La ecuación conceptual puede expresarse como:

> Riesgo = Amenaza × Vulnerabilidad × Impacto

Desde el punto de vista organizacional, la seguridad informática debe alinearse con el **Gobierno de TI (IT Governance)**, entendido como el sistema mediante el cual se dirigen y controlan las tecnologías de la información para generar valor y mitigar riesgos.

2.2 Importancia estratégica

La seguridad informática posee relevancia estratégica por diversas razones:

a) Protección del capital informacional

La información constituye un activo intangible crítico. Bases de datos de clientes, algoritmos, planes financieros y propiedad intelectual forman parte del valor de mercado de la organización.

Ejemplo:

Una empresa de comercio electrónico cuya base de datos de clientes es filtrada puede enfrentar sanciones regulatorias, demandas judiciales y pérdida de confianza del mercado.

b) Cumplimiento normativo (Compliance)

Las empresas deben respetar regulaciones sobre protección de datos personales, ciberseguridad y responsabilidad empresarial. El incumplimiento puede generar multas significativas.

c) Continuidad del negocio (Business Continuity)

Un ataque de ransomware puede paralizar las operaciones. Por ello se requiere un **Plan de Continuidad del Negocio (BCP, Business Continuity Plan)** y un **Plan de Recuperación ante Desastres (DRP, Disaster Recovery Plan)**.

d) Reputación y confianza

La confianza digital es un activo estratégico. En la economía digital, la percepción de seguridad influye en la decisión del cliente.

2.3 Alcance de la Seguridad Informática

El alcance no se limita al departamento de sistemas. Incluye:

1. **Infraestructura tecnológica**: servidores, redes, dispositivos móviles.
2. **Aplicaciones y software**: ERP (Enterprise Resource Planning), CRM (Customer Relationship Management), sistemas contables.
3. **Datos estructurados y no estructurados**.
4. **Usuarios internos y externos**.
5. **Proveedores tecnológicos (Third-party vendors)**.
6. **Procesos organizacionales**.

Desde la mirada administrativa, el alcance debe abarcar tanto la dimensión técnica como la organizacional.

2.4 Políticas técnicas

Las políticas técnicas son controles implementados mediante herramientas tecnológicas.

1. Control de acceso (Access Control)

Basado en el principio de **mínimo privilegio (Least Privilege Principle)**.

Incluye modelos como:

- **RBAC (Role-Based Access Control)** – Control de acceso basado en roles.
- **MFA (Multi-Factor Authentication)** – Autenticación multifactor.

Ejemplo:

Un empleado del área contable no debería tener acceso a la configuración del servidor.

---

2. Cifrado (Encryption)

Protege la confidencialidad de la información mediante algoritmos criptográficos.

- **SSL/TLS (Secure Sockets Layer / Transport Layer Security)** – Seguridad en transmisión de datos.
- **AES (Advanced Encryption Standard)** – Estándar avanzado de cifrado.

---

3. Firewalls y sistemas de detección

- **Firewall**: controla tráfico entrante y saliente.
- **IDS/IPS (Intrusion Detection/Prevention System)** – Sistemas de detección y prevención de intrusiones.

---

4. Gestión de vulnerabilidades (Vulnerability Management)

Incluye escaneos periódicos, actualizaciones (patch management) y pruebas de penetración (Penetration Testing).

---

5. Copias de seguridad (Backups)

Política de respaldo con frecuencia definida y almacenamiento fuera del sitio (off-site backup).

2.5 Políticas administrativas

La seguridad informática no puede sostenerse únicamente con tecnología. Requiere un marco administrativo formal.

1. Política de Seguridad de la Información (Information Security Policy)

Documento rector aprobado por la alta dirección.

2. Clasificación de la información

Definición de categorías: pública, interna, confidencial, crítica.

3. Capacitación y concientización (Awareness Training)

La mayoría de los incidentes se originan por error humano.

Ejemplo:

Un empleado que abre un correo de phishing puede comprometer la red corporativa.

---

4. Gestión de incidentes (Incident Response Plan, IRP)

Procedimiento formal para detectar, contener, erradicar y recuperar ante un incidente.

---

5. Auditorías internas y externas

Permiten verificar el cumplimiento de políticas y controles.

---

6. Gobierno y responsabilidad

Designación de un **CISO (Chief Information Security Officer)** o responsable de seguridad.

2.6 Relación con la estrategia empresarial

La seguridad informática debe integrarse al **Planeamiento Estratégico (Strategic Planning)**.

Desde la administración, se deben considerar:

- Evaluación costo-beneficio de controles.
- Modelo **ROSI (Return on Security Investment)** – Retorno sobre la inversión en seguridad.

- Análisis de impacto financiero ante incidentes.

La inversión en seguridad no es gasto, sino mitigación de riesgo estratégico.

2.7 Gestión del riesgo en TI

El proceso incluye:

1. Identificación de activos.
2. Identificación de amenazas.
3. Evaluación de vulnerabilidades.
4. Cálculo de impacto.
5. Implementación de controles.
6. Monitoreo continuo.

Se trata de un ciclo permanente, no de una acción puntual.

2.8 Seguridad en entornos digitales modernos

Las empresas actuales operan en:

- **Cloud Computing (Computación en la nube)**
- **IoT (Internet of Things, Internet de las Cosas)**
- **Trabajo remoto (Remote Work)**
- **Big Data**

Cada entorno amplía la superficie de ataque (Attack Surface). Por lo tanto, la seguridad debe adaptarse a arquitecturas distribuidas.

2.9 Cultura organizacional de seguridad

La seguridad informática es una cuestión cultural.

Debe promoverse:

- Responsabilidad compartida.
- Reporte temprano de incidentes.
- Integración entre áreas de negocio y TI.

Desde la administración, el liderazgo es clave para consolidar esta cultura.

---

3. Conclusión

La seguridad informática constituye un pilar estratégico en la gestión empresarial contemporánea. No se limita a herramientas tecnológicas aisladas, sino que representa un sistema integral de políticas técnicas y administrativas orientadas a proteger los activos informacionales.

Desde la perspectiva de las Tecnologías de la Información, la seguridad debe integrarse al gobierno corporativo, al planeamiento estratégico y a la gestión del riesgo. La implementación efectiva requiere controles tecnológicos (cifrado, firewalls, autenticación multifactor), políticas organizacionales formales (clasificación de información, capacitación, auditorías) y liderazgo directivo comprometido.

Para los futuros licenciados en administración, comprender la seguridad informática implica asumir que la información es un activo crítico cuya protección condiciona la continuidad del negocio, la reputación corporativa y el cumplimiento normativo. En un entorno digitalizado, la seguridad no es opcional: es un requisito estructural para la sostenibilidad organizacional.

Preguntas de autoevaluación

1. ¿Cómo se relaciona la Triada CIA con la gestión estratégica de una empresa?
2. ¿Cuál es la diferencia entre una política técnica y una política administrativa en seguridad informática?
3. Explique el concepto de riesgo en seguridad informática y sus componentes.
4. ¿Por qué la seguridad informática debe integrarse al planeamiento estratégico y no limitarse al área de TI?
5. ¿Cómo puede justificarse financieramente una inversión en seguridad mediante el modelo ROSI?

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.