Universidad de Buenos Aires
Facultad de Ciencias Económicas

Los Delitos Informáticos

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 **delitos informáticos** constituyen conductas ilícitas cometidas mediante el uso de tecnologías digitales o dirigidas contra sistemas de información, redes, datos o infraestructuras tecnológicas. En el contexto de las Tecnologías de la Información (TI), estos delitos representan una de las principales amenazas para la integridad, disponibilidad y confidencialidad de los activos digitales organizacionales.

A diferencia de los delitos tradicionales, los delitos informáticos se caracterizan por su alcance transnacional, la dificultad de atribución, la velocidad de propagación y la sofisticación técnica. Su impacto no se limita al plano técnico, sino que afecta directamente la estabilidad financiera, la reputación corporativa, el cumplimiento normativo y la continuidad del negocio.

Para estudiantes de licenciatura en administración, comprender los delitos informáticos implica analizar cómo las organizaciones deben anticiparse a amenazas digitales, implementar controles preventivos y diseñar estrategias de mitigación que integren seguridad tecnológica, gobernanza corporativa y cumplimiento legal.

Desarrollo

1. Concepto y Clasificación de los Delitos Informáticos

Un delito informático puede definirse como cualquier acción ilegal en la que se utilizan sistemas informáticos como herramienta, objetivo o medio para la comisión del ilícito.

Se pueden clasificar en tres grandes categorías:

1. Delitos contra la confidencialidad.
2. Delitos contra la integridad.
3. Delitos contra la disponibilidad.

Estos tres ejes coinciden con el modelo **CIA (Confidentiality, Integrity, Availability / Confidencialidad, Integridad y Disponibilidad)**.

---

2. Delitos contra la Confidencialidad

Incluyen conductas orientadas a obtener información sin autorización.

2.1 Acceso Ilícito

El acceso no autorizado a sistemas, conocido como hacking, implica vulnerar mecanismos de seguridad para ingresar a plataformas protegidas.

Ejemplo:

Un atacante que accede a una base de datos financiera corporativa.

2.2 Intercepción de Comunicaciones

La interceptación indebida de datos transmitidos por red (por ejemplo, ataques Man-in-the-Middle – MITM / Intermediario malicioso) compromete la privacidad de la información.

2.3 Robo de Datos

El robo o exfiltración de información confidencial puede incluir:

- Datos personales.
- Secretos comerciales.
- Información estratégica.

Este tipo de delito genera alto impacto reputacional.

---

3. Delitos contra la Integridad

Se relacionan con la alteración indebida de datos o sistemas.

3.1 Manipulación de Información

La modificación fraudulenta de registros contables, financieros o administrativos constituye un delito que afecta la confiabilidad organizacional.

Ejemplo:

Alterar cifras en un sistema ERP para ocultar desvíos presupuestarios.

3.2 Fraude Informático

El fraude informático implica manipulación digital para obtener beneficios económicos.

Puede involucrar:

- Transferencias electrónicas indebidas.
- Uso de credenciales robadas.
- Ingeniería social.

---

4. Delitos contra la Disponibilidad

4.1 Ataques de Denegación de Servicio

El ataque DoS (*Denial of Service* / Denegación de Servicio) o DDoS (*Distributed Denial of Service* / Denegación de Servicio Distribuida) busca saturar sistemas y volverlos inaccesibles.

Ejemplo:

Una plataforma de comercio electrónico que queda inoperativa durante una campaña de ventas.

4.2 Ransomware

El ransomware cifra información y exige pago para su liberación.

Impacto:

- Paralización operativa.
- Pérdida de datos.
- Costos de recuperación.

---

5. Delitos Informáticos Internos

No todos los delitos provienen del exterior.

Amenazas internas incluyen:

- Abuso de privilegios.
- Sabotaje.
- Robo de información por empleados.

La falta de controles de acceso adecuados aumenta la vulnerabilidad.

---

6. Phishing e Ingeniería Social

El phishing consiste en engañar al usuario para obtener credenciales.

La ingeniería social explota vulnerabilidades humanas más que técnicas.

Ejemplo:

Correo falso solicitando actualización de contraseña.

La capacitación organizacional es clave para mitigar este riesgo.

---

7. Delitos Vinculados a Identidad Digital

Incluyen:

- Suplantación de identidad.
- Creación de perfiles falsos.
- Robo de credenciales.

El control de identidad mediante MFA (Multi-Factor Authentication / Autenticación Multifactor) reduce estos riesgos.

---

8. Impacto Organizacional

Los delitos informáticos generan:

- Pérdidas financieras.
- Sanciones regulatorias.
- Demandas judiciales.
- Daño reputacional.
- Interrupción del negocio.

Desde la administración, deben analizarse bajo la lógica de gestión de riesgos.

---

9. Prevención y Controles

Para mitigar delitos informáticos, las organizaciones deben implementar:

- Controles técnicos (firewalls, cifrado).
- Controles administrativos (políticas y auditorías).
- Controles físicos.
- Monitoreo continuo.
- Segregación de funciones.

La adopción del modelo Zero Trust (Confianza Cero) refuerza la seguridad.

---

10. Marco Normativo y Cumplimiento

Las organizaciones deben cumplir con marcos legales que tipifican delitos informáticos.

El incumplimiento puede derivar en:

- Responsabilidad penal.
- Multas.
- Intervenciones regulatorias.

La evidencia digital debe preservarse adecuadamente para investigaciones.

---

11. Gestión de Incidentes

Ante un delito informático, se requiere:

- Activación de protocolo de respuesta.
- Análisis forense digital.
- Comunicación estratégica.
- Recuperación operativa.

El DRP (Disaster Recovery Plan / Plan de Recuperación ante Desastres) y el BCP (Business Continuity Plan / Plan de Continuidad del Negocio) son esenciales.

---

12. Ejemplo Integrado

Una empresa sin cifrado ni monitoreo sufre ransomware.

Amenaza: software malicioso.

Vulnerabilidad: ausencia de actualización.

Impacto: paralización total.

Con:

- Backup 3-2-1.
- MFA.
- Segmentación de red.

El impacto se reduce significativamente.

---

13. Dimensión Estratégica

Para administradores, los delitos informáticos no deben analizarse únicamente como riesgos tecnológicos, sino como amenazas estratégicas que afectan:

- Confianza del mercado.
- Valor de marca.
- Estabilidad financiera.
- Cumplimiento normativo.

La inversión en seguridad constituye una decisión estratégica.

Conclusión

Los delitos informáticos representan una de las principales amenazas en el ecosistema digital contemporáneo. Su impacto trasciende lo técnico y compromete dimensiones financieras, jurídicas y reputacionales. En el contexto de las Tecnologías de la Información, la prevención requiere un enfoque integral que combine controles técnicos, administrativos y culturales.

Desde la perspectiva administrativa, la gestión de delitos informáticos implica integrar seguridad en la estrategia corporativa, fortalecer la gobernanza tecnológica y promover una cultura organizacional orientada a la prevención. En un entorno digital interconectado, la protección frente a delitos informáticos constituye una condición indispensable para la sostenibilidad y competitividad organizacional.

Preguntas de autoevaluación

1. ¿Cuál es la diferencia entre delitos contra la confidencialidad, integridad y disponibilidad?
2. ¿Cómo impacta el ransomware en la continuidad del negocio?
3. ¿Por qué la ingeniería social es difícil de prevenir exclusivamente con tecnología?
4. ¿Qué rol cumple la gestión de riesgos en la prevención de delitos informáticos?
5. ¿Por qué la seguridad frente a delitos informáticos debe considerarse una decisión estratégica?

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.