Universidad de Buenos Aires
Facultad de Ciencias Económicas

Delitos Realizados con el Uso de la Tecnología

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 cometidos por medio de la tecnología** comprenden un conjunto de conductas ilícitas en las que las herramientas digitales, las redes informáticas o los sistemas de información constituyen el medio principal para la ejecución del acto delictivo. A diferencia de los delitos informáticos "puros" —que atacan directamente la infraestructura tecnológica— estos delitos utilizan la tecnología como instrumento para afectar bienes jurídicos tradicionales como el patrimonio, la identidad, la privacidad o la confianza pública.

🏛 En este artículo solo trataremos los delitos realizados en organizaciones.

En el entorno organizacional contemporáneo, caracterizado por la digitalización de procesos, la interconexión global y la dependencia de plataformas tecnológicas, estos delitos representan un riesgo estratégico para empresas públicas y privadas. Modalidades como el **phishing**, el fraude electrónico, la suplantación de identidad digital, la estafa en comercio electrónico o la

manipulación de transferencias electrónicas afectan directamente la continuidad del negocio, la reputación corporativa y el cumplimiento normativo.

Para estudiantes de licenciatura en administración, comprender estos delitos implica integrar la dimensión tecnológica, jurídica y organizacional, evaluando cómo las vulnerabilidades humanas y técnicas pueden ser explotadas mediante medios digitales.

Desarrollo

1. Concepto General

Los delitos cometidos por medio de la tecnología se caracterizan por:

- Utilizar dispositivos digitales o redes como instrumento.
- Afectar bienes jurídicos tradicionales.
- Operar en entornos virtuales o híbridos.
- Tener alcance transnacional.

Desde la perspectiva de TI, estos delitos explotan debilidades en:

- Sistemas de autenticación.
- Procesos organizacionales.
- Gestión de identidad.
- Educación digital de usuarios.

La prevención requiere una combinación de controles técnicos y administrativos.

---

2. Phishing

El **phishing** es una modalidad de fraude digital que consiste en suplantar la identidad de una entidad legítima para obtener información confidencial.

Mecanismo:

- Envío de correos electrónicos falsos.
- Creación de sitios web fraudulentos.

- Solicitud de credenciales o datos bancarios.

Ejemplo organizacional:

Un empleado recibe un correo que aparenta provenir del banco corporativo solicitando actualización de credenciales. Al ingresar los datos, el atacante obtiene acceso a cuentas financieras.

Impacto:

- Robo de fondos.
- Pérdida de datos.
- Daño reputacional.

El phishing explota vulnerabilidades humanas más que técnicas.

---

3. Spear Phishing y Whaling

El **Spear Phishing** es una versión dirigida del phishing, orientada a personas específicas dentro de la organización.

El **Whaling** apunta a altos ejecutivos. (Whale significa Ballena en inglés)

Ejemplo:

Un atacante simula ser el CEO y solicita transferencia urgente de fondos.

La falta de verificación interna facilita el fraude.

---

4. Fraude Electrónico

El fraude electrónico implica manipulación digital para obtener beneficio económico.

Incluye:

- Transferencias no autorizadas.
- Manipulación de órdenes de pago.
- Intercepción de comunicaciones financieras.

Desde la administración, los procesos de doble validación y segregación de funciones son esenciales para prevenirlo.

---

5. Suplantación de Identidad Digital

La suplantación de identidad implica el uso indebido de credenciales ajenas.

Puede producirse mediante:

- Robo de contraseñas.
- Ataques de fuerza bruta.
- Ingeniería social.

La autenticación multifactor (MFA – Multi-Factor Authentication / Autenticación Multifactor) reduce significativamente este riesgo.

---

6. Ingeniería Social

La **ingeniería social** es una técnica que manipula psicológicamente a las personas para obtener información o acceso.

No requiere vulnerar sistemas técnicos; explota:

- Confianza.
- Urgencia.
- Autoridad.
- Desinformación.

Ejemplo:

Llamada telefónica simulando ser soporte técnico solicitando credenciales.

La capacitación organizacional es el principal mecanismo preventivo.

---

7. Estafas en Comercio Electrónico

Incluyen:

- Venta de productos inexistentes.
- Manipulación de plataformas de pago.
- Falsificación de identidades comerciales.

Las organizaciones deben implementar controles de verificación y monitoreo transaccional.

---

8. Ciberextorsión

La ciberextorsión utiliza amenazas digitales para exigir pagos.

Puede incluir:

- Amenaza de divulgación de datos.
- Bloqueo de sistemas.
- Manipulación de reputación online.

Desde la administración, la gestión de crisis y comunicación estratégica es clave.

---

9. Delitos Financieros Digitales

Incluyen:

- Lavado de activos mediante criptomonedas.
- Fraude en plataformas de inversión.
- Manipulación de sistemas contables digitales.

El monitoreo de transacciones y cumplimiento normativo es esencial.

---

10. Impacto Organizacional

Estos delitos pueden generar:

- Pérdidas económicas directas.
- Sanciones regulatorias.
- Demandas judiciales.
- Pérdida de confianza.
- Interrupción operativa.

La evaluación del riesgo debe integrar probabilidad e impacto.

---

11. Controles Preventivos

Las organizaciones deben implementar:

- MFA.

- Firewalls y filtros de correo.
- Detección de anomalías.
- Políticas de verificación de transferencias.
- Capacitación en seguridad.

El modelo Zero Trust (Confianza Cero) fortalece la prevención.

---

12. Gestión de Incidentes

Ante un delito digital:

1. Activar protocolo de respuesta.
2. Preservar evidencia digital.
3. Notificar autoridades.
4. Comunicar a partes afectadas.
5. Evaluar mejoras en controles.

La existencia de un DRP (Disaster Recovery Plan / Plan de Recuperación ante Desastres) y BCP (Business Continuity Plan / Plan de Continuidad del Negocio) es esencial.

---

13. Dimensión Jurídica y Global

La naturaleza transnacional de estos delitos exige cooperación internacional.

Las diferencias jurisdiccionales pueden dificultar:

- Identificación del autor.
- Aplicación de sanciones.
- Recuperación de fondos.

El cumplimiento regulatorio es parte de la estrategia organizacional.

---

14. Ejemplo Integrado

Empresa recibe correo falso del proveedor solicitando cambio de cuenta bancaria.

Amenaza: spear phishing.

Vulnerabilidad: ausencia de verificación telefónica.

Impacto: transferencia fraudulenta.

Implementando procedimiento de confirmación independiente, el fraude se evita.

Conclusión

Los delitos cometidos por medio de la tecnología representan una evolución de las conductas ilícitas tradicionales en el entorno digital. Modalidades como el phishing, la ingeniería social, el fraude electrónico y la suplantación de identidad explotan tanto vulnerabilidades técnicas como humanas.

Desde la perspectiva de la administración y las Tecnologías de la Información, la prevención requiere un enfoque integral que combine controles técnicos, administrativos y culturales. La gestión estratégica del riesgo digital es indispensable para proteger activos, garantizar continuidad operativa y preservar la confianza institucional.

En un entorno digital globalizado, la seguridad frente a delitos tecnológicos no es opcional, sino estructural para la sostenibilidad organizacional.

Preguntas de autoevaluación

1. ¿Cuál es la diferencia entre phishing y spear phishing?
2. ¿Por qué la ingeniería social puede ser más efectiva que un ataque técnico?
3. ¿Qué controles administrativos reducen el riesgo de fraude electrónico?
4. ¿Cómo impactan estos delitos en la reputación organizacional?
5. ¿Por qué la gestión estratégica del riesgo digital es clave para los administradores?

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.