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**.

Delitos Realizados con el Uso de la Tecnología en Organizaciones

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 el entorno organizacional contemporáneo, caracterizado por la digitalización de procesos y la interconexión global, estas modalidades representan un riesgo estratégico significativo. El análisis de este capítulo se centra específicamente en delitos cometidos en contextos organizacionales, donde el impacto afecta directamente la continuidad del negocio, la reputación corporativa y el cumplimiento normativo.

Fraudes financieros digitales

Fraude en transferencias electrónicas. Modalidad en la que el atacante, generalmente mediante ingeniería social, logra que un empleado autorice una transferencia bancaria a cuentas fraudulentas. El Business Email Compromise (BEC) es la variante más frecuente: el atacante suplanta la identidad del CEO, del CFO o de un proveedor para solicitar pagos urgentes. Es uno de los delitos de mayor impacto financiero en el mundo corporativo.

Fraude en sistemas de pago y comercio electrónico. Incluye la manipulación de transacciones, el uso de datos robados de tarjetas para compras no autorizadas y la creación de cuentas ficticias para extracción de fondos.

Manipulación de sistemas contables. Modificación fraudulenta de registros contables digitales para encubrir desfalcos, inflar resultados o generar reportes falsos. Esta modalidad requiere acceso privilegiado a los sistemas ERP y la ausencia de controles de trazabilidad.

Fraudes de identidad digital

Suplantación de identidad en transacciones. El atacante utiliza credenciales o identidades robadas para realizar transacciones en nombre de terceros, comprometiendo contratos, órdenes de compra y pagos.

Creación de entidades ficticias. En sistemas con controles débiles de validación, la creación de proveedores, clientes o empleados ficticios permite extraer fondos del sistema de pagos de la organización.

Espionaje industrial digital. Robo de secretos comerciales, fórmulas, proyectos estratégicos o información de clientes mediante acceso indebido a sistemas o correos corporativos. Puede realizarse por un competidor o por empleados que se desvinculan hacia la competencia.

Acoso y amenazas digitales en el ámbito laboral

Las plataformas digitales corporativas pueden ser usadas para conductas de acoso, intimidación o amenazas. Los sistemas de información de la organización —incluyendo el correo corporativo, plataformas colaborativas y sistemas de mensajería— pueden convertirse en el medio y la evidencia de estas conductas.

Controles preventivos organizacionales

Los controles para mitigar estos delitos combinan medidas técnicas y administrativas: la segregación de funciones en procesos financieros; la verificación de identidad por canales alternativos antes de autorizar transferencias de alto valor; la validación de proveedores y cuentas bancarias antes del primer pago; el monitoreo de transacciones inusuales

mediante sistemas de analítica; la capacitación en reconocimiento de ingeniería social; y los procedimientos formales de autorización con doble firma para operaciones críticas.

La detección temprana requiere monitoreo de comportamientos anómalos: transferencias fuera de horario habitual, montos inusuales, cambios de datos bancarios no verificados o accesos desde ubicaciones atípicas.

Conceptos clave

- Distinción entre delitos informáticos puros y delitos cometidos con tecnología como medio.
- BEC como forma más frecuente de fraude financiero digital en organizaciones.
- Manipulación de sistemas contables como delito que requiere acceso privilegiado.
- Espionaje industrial digital como amenaza de activos intangibles.
- Segregación de funciones y verificación por canales alternativos como controles críticos.

Preguntas de repaso del tema

1. ¿Cuál es la diferencia entre un delito informático puro y uno cometido con tecnología?
2. ¿Cómo opera el Business Email Compromise y por qué es tan efectivo?
3. ¿Qué controles específicos reducen el riesgo de fraude en transferencias?
4. ¿Cómo puede prevenirse la creación de entidades ficticias en sistemas de pagos?
5. ¿Qué controles de trazabilidad reducen el riesgo de manipulación contable?
6. ¿Por qué la verificación por canales alternativos es un control crítico?
7. ¿Qué indicadores pueden alertar sobre transacciones fraudulentas?

8. ¿Cómo se relaciona el espionaje industrial digital con el ciclo de vida del empleado?
9. ¿Qué función cumple la segregación de funciones en la prevención de fraudes digitales?
10. ¿Por qué estos delitos requieren respuestas que combinen controles técnicos y administrativos?