SLLM
CIUDAD DE MÉXICO

2026
JULIO

STAR-CI-HUB

SLLM ALERT

PHISHING: LA GESTIÓN DEL RIESGO DIGITAL

THE STRATEGY OF EXCELLENCE

SLLM ALERT

Phishing: la gestión del riesgo digital

El 22 de julio de 2026 se publicó en la Gaceta Oficial de la Ciudad de México la adición del artículo 231 Bis al Código Penal local.

La modificación legal castiga el uso de plataformas o canales digitales falsos diseñados para **engañar** a las personas y obtener **de forma ilícita sus accesos, datos personales o información financiera.**

La sanción prevista es de **tres a seis años de prisión** y de **200 a 600 unidades de medida y actualización (UMA)**. La pena podrá aumentar hasta en una mitad cuando las víctimas sean personas con discapacidad, personas mayores o menores de edad.
Para las empresas, el cambio implica que un caso de suplantación ya no debe gestionarse únicamente como incidente tecnológico. Puede requerir **preservación de evidencia, análisis de datos comprometidos y coordinación jurídica** para una eventual denuncia.

¿Qué estableció la reforma?

Conducta tipificada
El *phishing* se reconoce como delito autónomo cuando se emplean medios digitales que aparentan ser legítimos para obtener información personal, financiera o de autenticación.

Sanciones
- Prisión: 3 a 6 años.
- Multa: 200 a 600 UMA.
- Agravante: incremento de hasta la mitad de la pena si la víctima pertenece a grupos vulnerables.
-

Alcance
Aplica en la Ciudad de México y complementa otras figuras como fraude, acceso ilícito a sistemas y delitos informáticos.

PREGUNTAS CLAVE PARA LAS EMPRESAS

¿Es sólo un tema de TI? (Tecnologías de Información)	No. Ahora también es un asunto penal con sanciones específicas.
¿Debe denunciarse?	Sí. La empresa puede requerir coordinación jurídica para presentar denuncia y preservar evidencia.
¿Aplica a intentos fallidos?	Sí, la conducta se tipifica por el engaño digital, independientemente de si se logró el acceso.
¿Qué cambia en la gestión interna?	El cierre de incidentes con "cambio de contraseña y capacitación" puede ser insuficiente; se requiere trazabilidad y análisis legal.
¿Es aplicable a todo México?	La reforma es local, pero puede marcar precedente para otras entidades federativas.

Implicaciones por sector

- **Tecnología y plataformas digitales –** Mayor responsabilidad en detección, reporte y preservación de evidencia.
- **Fintech y servicios financieros –** Casos de suplantación pueden derivar en denuncias penales, además de reportes regulatorios.
- **Retail y atención al público –** Necesidad de protocolos claros para clientes afectados por intentos de fraude digital.
- **Salud y asistencia social –** Protección reforzada de datos sensibles de pacientes y beneficiarios.

PHISHING EN OTROS PAÍSES

País	Norma	Sanciones principales	Dato relevante
EE. UU.	Computer Fraud and Abuse Act (CFAA), CAN-SPAM Act	Prisión hasta 5 años + multas de 250,000 USD	Se persigue como fraude informático y abuso de sistemas.
Canadá	Criminal Code, secciones sobre fraude electrónico	Prisión hasta 14 años	Considerado fraude agravado cuando afecta datos financieros.
Reino Unido	Computer Misuse Act 1990	Prisión hasta 10 años	Se sanciona como acceso no autorizado y fraude digital.
China	Cybersecurity Law (2017)	Multas severas + prisión	Obliga a empresas a proteger datos y sanciona suplantación digital.
Brasil	Código Penal + Marco Civil da Internet	Prisión de 1 a 5 años	Tipifica fraude digital y responsabilidad de proveedores.

Dato curioso: Colombia fue uno de los primeros países en América Latina en tipificar expresamente el phishing como delito penal. Desde 2009, su Código Penal incluye el artículo 269G sobre "suplantación de sitios web para capturar datos personales", con penas de 48 a 96 meses de prisión y multas de 100 a 1000 salarios mínimos.

EN MÉXICO

El **Estado de México y Jalisco** concentran más del 40% de denuncias de fraude digital, pero aún procesan casos bajo figuras **genéricas como fraude o acceso ilícito.**

No existe tipificación autónoma en otros códigos penales estatales, aunque la tendencia apunta a que podrían replicar el modelo **de CDMX.**

La tipificación del ***phishing*** confirma que los incidentes digitales ya no son **únicamente un tema de ciberseguridad.** Se convierten en un **riesgo penal directo** para las empresas, colaboradores y clientes. La gestión corporativa debe evolucionar hacia esquemas que prevean:

- **Contención tecnológica.**
- **Preservación de evidencia digital.**
- **Evaluación jurídica y penal.**
- **Comunicación clara con usuarios y autoridades.**

Identificar áreas críticas de exposición digital

Actualizar protocolos de respuesta a incidentes para incluir preservación de evidencia.

Coordinar con áreas legales

Capacitar usuarios en prevención y reporte inmediato.

Documentar medidas como parte de la estrategia de continuidad y cumplimiento.

En SLLM asesoramos a nuestros clientes en la identificación, evaluación y atención preventiva de riesgos legales, tecnológicos y reputacionales que puedan impactar su operación. Nuestro enfoque busca brindar claridad para la toma de decisiones y asegurar que las medidas adoptadas sean consistentes con sus obligaciones legales y estrategia empresarial.