



DIP. OLIVIA GARZA DE LOS SANTOS
GRUPO PARLAMENTARIO DEL PARTIDO ACCIÓN NACIONAL



Ciudad de México, a 29 de Enero de 2026

DIPUTADO JESÚS SESMA SUÁREZ
PRESIDENTE DE LA MESA DIRECTIVA DEL
CONGRESO DE LA CIUDAD DE MÉXICO.
III LEGISLATURA.
PRESENTE

La que suscribe, **Diputada Olivia Garza de los Santos**, integrante del Grupo Parlamentario del Partido Acción Nacional en la Tercera Legislatura del Honorable Congreso de la Ciudad de México, con fundamento en lo dispuesto por los artículos 71 fracción III, de la Constitución Política de los Estados Unidos Mexicanos; 122, apartado A, fracciones I y II, párrafo cinco de la Constitución Política de los Estados Unidos Mexicanos; 29, apartados A, numeral 1, y D, incisos a), f) y g) y 30, numeral 1, inciso b) de la Constitución Política de la Ciudad de México; 1, 4, fracción XXI, 12, fracción II y 13, fracciones LV, LVII, LXII y LXIII de la Ley Orgánica del Congreso de la Ciudad de México; 1, 2, fracción XXI, 5, fracción I, 82, 95, fracción II y 96 del Reglamento del Congreso de la Ciudad de México, someto a la consideración del Pleno de este Poder Legislativo la siguiente **INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE ADICIONA UNA FRACCIÓN X BIS AL ARTÍCULO 224 DEL CÓDIGO PENAL PARA EL DISTRITO FEDERAL**, al tenor de la siguiente:

PROBLEMÁTICA

Los avances tecnológicos aplicados a las actividades financieras están permitiendo una amplia facilidad en la realización de transacciones comerciales, entre ellas la compraventa de diversos artículos, pero también han incrementado el riesgo para que los delincuentes hagan uso de herramientas tecnológicas para sustraer desde información sensible hasta recursos económicos.



Uno de estos avances lo encontramos en las tarjetas bancarias con tecnología “contactless”, estas tarjetas permiten realizar pagos sin ingresar el plástico en alguna terminal bancaria y sin necesidad de registrar el Número de Identificación Personal (NIP) o firma electrónica. Con lo anterior se facilitan las compras rápidas, especialmente de montos pequeños en tiendas, restaurantes, supermercados o, incluso, en el transporte público¹ como el Metrobús, Sistema de Transportes Eléctricos y algunas rutas de transporte concesionado.

La tecnología NFC (Near Field Communication) es la que permite las transacciones sin contacto. En teoría, este tipo de tarjetas que incluyen la tecnología NFC utilizan un microprocesador “inteligente” que protege la comunicación entre la tarjeta y la terminal, además de que el chip es difícil de clonar y, si así lo decide el usuario, tiene límites en las transacciones, ofreciendo una supuesta protección adicional al usuario.

No obstante, esto no ha impedido que sea un medio susceptible de vulneraciones para cometer robos digitales sin contacto (contactless). Para ello los delincuentes utilizan dispositivos electrónicos portátiles con tecnología NFC como lectores de tarjetas inalámbricos que pueden conseguirse fácilmente en internet con los que replican las funciones de las terminales bancarias, los que acercan lo suficiente a la tarjeta, ubicada generalmente, en carteras guardadas en bolsillos o bolsas de mano, ejecutando una transacción sin que el propietario se percate de ello².

Por lo regular, este tipo de robo suele ejecutarse en lugares con alta concentración de personas, como el transporte público, centros comerciales o

¹ Fuente: [Robo de dinero en tarjetas contactless: Así funciona y cómo evitarlo- Grupo Milenio](#)

² Fuente: [¿Te pueden robar con tecnología NFC? Así funciona este método y así puedes protegerte \(xataka.com.co\)](#)



DIP. OLIVIA GARZA DE LOS SANTOS
GRUPO PARLAMENTARIO DEL PARTIDO ACCIÓN NACIONAL



eventos masivos, en donde además de ser fácil pasar desapercibido, a ciertas horas, es común la aglomeración de individuos.

En el transcurso de 2025 en diversos medios de comunicación se difundieron alertas por el incremento en la incidencia de robos electrónicos³. Sin embargo, al no encontrarse reconocida en la legislación penal esta modalidad de robo, no existen estadísticas oficiales que consideren la incidencia, frecuencia y lugares en los que estos robos se cometen.

Por su parte, ante el crecimiento del uso de pagos digitales y tarjetas sin contacto, **Scotiabank México** difundió una serie de recomendaciones para fortalecer la seguridad de las operaciones financieras realizadas mediante tecnología *Contactless*, un método que, aunque es rápido y práctico, también ha sido aprovechado por la delincuencia digital.

De acuerdo con información compartida por la institución bancaria, el fraude en medios electrónicos continúa en aumento. En México, durante 2023 se registraron más de ocho millones de reclamaciones por fraude financiero, de las cuales el 71 % correspondieron a operaciones cibernéticas, lo que ha encendido alertas entre autoridades financieras y usuarios del sistema bancario.

La tecnología *Contactless* permite realizar pagos acercando la tarjeta o el dispositivo móvil a una terminal, sin necesidad de introducirlo ni teclear un NIP en transacciones de bajo monto. No obstante, especialistas advierten que el descuido en el manejo de tarjetas y dispositivos puede abrir la puerta a cargos no reconocidos o al robo de información financiera.

Scotiabank explicó que este tipo de pagos cuenta con diversas capas de seguridad, entre ellas un alcance de comunicación muy limitado menor a cuatro centímetros, el uso exclusivo de terminales certificadas y, en algunos casos, códigos de seguridad dinámicos que cambian en cada operación. Además, para

³ Fuente: [Cuidado con el NFC: alertan por robos sin contacto en tarjetas y celulares \(expansion.mx\)](https://expansion.mx)



montos mayores, el sistema solicita la autenticación del usuario mediante NIP u otros mecanismos de verificación.

Pese a ello, la institución subrayó que la seguridad no depende únicamente de la tecnología, sino también de las prácticas cotidianas de los usuarios. Entre las principales recomendaciones se encuentra el uso de carteras con bloqueo RFID, la activación de notificaciones en tiempo real para cada movimiento bancario, la preferencia por pagos con autenticación biométrica y la reducción del número de tarjetas que se llevan diariamente.

Asimismo, se enfatizó la importancia de actuar con rapidez ante cualquier operación sospechosa, bloqueando de inmediato la tarjeta a través de la aplicación bancaria o los canales de atención telefónica, a fin de evitar afectaciones mayores al patrimonio de sus clientes.

Con esas acciones, la institución bancaria reiteró su compromiso de promover una cultura de prevención y uso responsable de los servicios financieros digitales, destacando que la adopción informada de nuevas tecnologías es clave para aprovechar sus beneficios sin comprometer la seguridad de los usuarios.⁴

Lo anterior también fue considerado en la siguiente nota periodística en la que se detallan los contratiempos que se enfrenta al hacer usos de las tecnologías que nos ocupan:

“Estudio revela auge preocupante del fraude digital en América Latina

*En América Latina advierte que la región enfrenta **niveles alarmantes de delitos digitales y pérdidas económicas asociadas a transacciones electrónicas**, impulsados por la rápida digitalización y debilidades regulatorias, según el informe Overcoming Latin America’s Digital Fraud Challenges publicado por la firma de ciberseguridad ThreatMark.*

⁴ <https://www.scotiabank.com.mx/blog/para-ti/la-seguridad-contactless-empieza-contigo>



*El documento destaca que **América Latina lidera el mundo en fraude con tarjetas de crédito**, con tasas **hasta 97 % más altas que en Norteamérica y 222 % superiores a las del Asia-Pacífico**, lo cual representa pérdidas económicas significativas para consumidores, comercios y la industria financiera.*

*De acuerdo con los datos recopilados, la amplia adopción de pagos digitales y de sistemas como Pix la plataforma de pagos en tiempo real de Brasil ha acelerado la inclusión financiera, pero también ha creado oportunidades para que los ciberdelincuentes exploten vulnerabilidades y tácticas fraudulentas como el llamado **fraude por pago push autorizado (APP)**.*

*En Brasil, por ejemplo, las pérdidas derivadas de este tipo de estafa alcanzaron **247 millones de dólares en 2022**, y se proyecta que podrían llegar a **más de 630 millones de dólares para 2027**, según estimaciones de ACI Worldwide y GlobalData.*

*Además, en países como **México**, se calcula que diariamente se registran cerca de **15 000 casos de fraude financiero**, y aproximadamente **uno de cada cinco usuarios ha sufrido algún tipo de fraude digital**, con un éxito delictivo en el 92 % de estos casos. En **Colombia**, las cifras oficiales señalan un **incremento de 409 % en delitos como el robo de identidad y fraude digital desde 2020**.*

El estudio también identifica una categoría emergente denominada fraude amigable, que ocurre cuando consumidores solicitan devoluciones o cargos por transacciones que realizaron legítimamente, provocando un impacto financiero considerable en comercios y bancos por errores de interpretación de cargos.

*De igual manera, ThreatMark subraya que **las lagunas en regulación y aplicación de la ley**, así como la falta de políticas claras sobre responsabilidad ante pérdidas por fraude, han limitado la capacidad de la región para mitigar estos delitos. Expertos citados en el informe señalan que*



problemas estructurales como bajos niveles de transparencia financiera y debilidad institucional contribuyen a agravar el fenómeno.

*Ante este panorama, el reporte recomienda **reforzar capacidades tecnológicas y utilizar soluciones avanzadas de prevención** que integren análisis de comportamiento de usuarios, detección de patrones sospechosos y monitoreo continuo de transacciones. Herramientas basadas en inteligencia artificial y plataformas de inteligencia de comportamiento han demostrado ser más eficaces que los métodos tradicionales al identificar y detener fraudes sofisticados antes de que ocurran.*

Además, la colaboración entre instituciones financieras, reguladores y empresas tecnológicas se plantea como un elemento clave para fortalecer el ecosistema digital y proteger tanto a consumidores como a proveedores de servicios financieros.”⁵

Se estima que esta falta de consideración en la legislación penal de la Ciudad de México de una conducta delictiva que está teniendo un preocupante incremento, por una parte, vulnera la certeza jurídica de las personas que se han visto afectadas por esas acciones y por otro lado limita la capacidad de reacción de las autoridades de seguridad pública (SSC) y de investigación (FGJCDMX) para estar en condiciones de enfrentar eficientemente a quienes cometen esta acción, integrar debidamente carpetas de investigación y, eventualmente, presentarlas ante las autoridades jurisdiccionales para su “judicialización” y que las personas que los cometen sean sancionadas.

Resulta impensable que esta incertidumbre legal permanezca y se prolongue por más tiempo, por ello se estima apremiante que esta Soberanía atienda la existencia de esta laguna jurídica que permite que la delincuencia actúe con impunidad y siga afectando el patrimonio de los ciudadanos, no sólo habitantes

⁵ <https://www.threatmark.com/latam-digital-fraud>



DIP. OLIVIA GARZA DE LOS SANTOS
GRUPO PARLAMENTARIO DEL PARTIDO ACCIÓN NACIONAL



de la Ciudad, sino también de visitantes y población flotante que acude de visita, a realizar actividades comerciales o laborales.

Esto genera la necesidad de que este Pleno se ocupe en tipificar la conducta ya descrita como delito, a efecto de que las autoridades investigadoras, esto es el Ministerio Público y la Policía de Investigación, cuenten con los elementos normativos que les permitan una debida integración de las carpetas de investigación que se deriven de las denuncias hechas por las personas perjudicadas por quienes, aprovechándose de los avances tecnológicos, merman el patrimonio de las personas mediante la utilización de dispositivos electrónicos y las tecnologías de la información sustraen de manera ilegal recursos económicos a través de las tarjetas habilitadas con tecnología NFC sin que los titulares de las mismas se percaten de dicha acción, aprovechándose de aglomeraciones o altas concentraciones de personas.

Así, la propuesta de adición planteada en la presente iniciativa cumple con el mandato constitucional y convencional de dar certidumbre jurídica a los ciudadanos al incluirse en la legislación penal una figura normativa que, por una parte acote con total claridad una conducta que será considerada como delito y, de esta forma, dote a la autoridad de la descripción de dicha acción para estar en condiciones de llevar a cabo los actos de investigación que le permitan la debida integración de la carpeta de investigación conducente, haciendo lo anterior en total congruencia con los estándares marcados no solamente por la Constitución General de la República, la de la Ciudad de México, el derecho convencional del que nuestro país sea parte, sino también de la Suprema Corte de Justicia de la Nación y de los organismos internacionales de derechos humanos.

Por lo anterior, se estima pertinente el análisis y eventual aprobación de la presente propuesta legislativa a la luz de los siguientes:



DIP. OLIVIA GARZA DE LOS SANTOS
GRUPO PARLAMENTARIO DEL PARTIDO ACCIÓN NACIONAL



**FUNDAMENTO LEGAL Y EN SU CASO SOBRE SU CONSTITUCIONALIDAD
Y CONVENCIONALIDAD**

MARCO FEDERAL

- Artículo 1o, artículo 2o, Literal D, párrafo segundo; 4o; Primer párrafo, Literal A, numerales I, II y III, del artículo 122 de la Constitución Política de los Estados Unidos Mexicanos.

MARCO LOCAL

- Artículo 1 De la Ciudad de México; Artículo 3 De los principios rectores; Artículo 4 Principios de Interpretación y Aplicación de los Derechos Humanos; Artículo 5 Ciudad Garantista; Artículo 9 Ciudad Solidaria.

Finalmente, la propuesta de redacción se detalla en el siguiente cuadro comparativo para facilitar la comprensión de la importancia del planteamiento que nos ocupa.

CÓDIGO PENAL PARA EL DISTRITO FEDERAL, TEXTO VIGENTE	CÓDIGO PENAL PARA EL DISTRITO FEDERAL, TEXTO PROPUESTO
ARTÍCULO 224. Además de las penas previstas en el artículo 220 de este Código: A) Se impondrá de dos a seis años de prisión, cuando el robo se cometa: I. a X. ...	ARTÍCULO 224. Además de las penas previstas en el artículo 220 de este Código: A) Se impondrá de dos a seis años de prisión, cuando el robo se cometa: I. a X. ...



DIP. OLIVIA GARZA DE LOS SANTOS
GRUPO PARLAMENTARIO DEL PARTIDO ACCIÓN NACIONAL



Sin correlativo	X. BIS. Mediante la utilización de dispositivos electrónicos o tecnologías de la información, sustraiga, sin el consentimiento de su titular, recursos económicos ejecutando o simulando operaciones bancarias, financieras o comerciales presuntamente realizadas con tarjetas de crédito o débito;
X. ...	X. ...
...	...

Por lo expuesto y fundado, someto a consideración de esta soberanía el siguiente proyecto de:

Decreto por el que se adiciona una fracción X BIS al artículo 224 del Código Penal para el Distrito Federal, para quedar como sigue:

Artículo Único. Se adiciona una fracción X BIS al artículo 224 del Código Penal para el Distrito Federal.

ARTÍCULO 224. Además de las penas previstas en el artículo 220 de este Código:

A) Se impondrá de dos a seis años de prisión, cuando el robo se cometa:

I. a X. ...

X. BIS. Mediante la utilización de dispositivos electrónicos o tecnologías de la información, sustraiga, sin el consentimiento de su titular, recursos



DIP. OLIVIA GARZA DE LOS SANTOS
GRUPO PARLAMENTARIO DEL PARTIDO ACCIÓN NACIONAL



económicos ejecutando o simulando operaciones bancarias, financieras o comerciales presuntamente realizadas con tarjetas de crédito o débito;

X. ...

...

Artículos Transitorios.

ÚNICO. El presente decreto entrará en vigor a partir del día siguiente de su publicación en la Gaceta Oficial de la Ciudad de México.

Palacio Legislativo de Donceles, a los 29 días del mes de Enero de 2026.

Suscribe
OLIVIA
GARZA DE LOS SANTOS
697BB1399B3EA76A731E05F0

Dip. Olivia Garza de los Santos

Certificado de firma

29/01/2026 13:13

Documento electrónico

Solicitante del proceso de firma Almacenado

Identificador: 697BB0B99F2D916BDC257E1A

Nombre y extensión: INICIATIVA Código Penal Robo Digital 1.pdf

Descripción:

Cantidad de páginas: 3

Estado: Firmado

Firmantes: 1

Huella digital del contenido del documento original:

159dec969a1d401772c3a852fa1b4a021c584343484a8e072286d091b1e592f2

Huella digital del contenido del documento firmado:

33c094b16d2bf24de02096d05d0ce77a2a1c9d44af8f34058ae5ce3ace20c7a9

Nombre: Olivia Garza De Los Santos

Compañía: SR LUZ SA DE CV

Correo electrónico: olivia.garza@congresocdmx.gob.mx

Teléfono:

Dirección IP: 2806:107e:d:3e5a:6004:77a3:88d1:3a63

Fecha y hora de emisión

(America/Mexico_City):

29/01/2026 13:10

Constancia de conservación del documento firmado

Información de la constancia NOM-151

Información del emisor de la constancia NOM-151

Fecha de emisión:

29/01/2026 19:13:04 UTC (29/01/2026 13:13:04 Hora local de la Ciudad de México)

Nombre y extensión:

cd91330d-7a1b-4284-9e18-205892be0bb1.cons

Huella digital contenida en la constancia:

33c094b16d2bf24de02096d05d0ce77a2a1c9d44af8f34058ae5ce3ace20c7a9

Prestador de Servicios de Certificación (PSC):

PSC WORLD S.A. DE C.V.

Certificado PSC válido desde: 2017-07-19

Certificado PSC válido hasta: 2029-07-19

Firmantes

Firmante 1. OLIVIA GARZA DE LOS SANTOS

Atributos

Firma

Fecha

Tipo de actuación: Por su Propio
DerechoID: 697BB1399B3EA76A731E05F0
IP: 2806:107e:d:3e5a:6004:77a3:88d1:3a63Enviado: 29/01/2026
13:12:24

Compañía:

Aceptó Aviso de

Método de notificación: Correo

Privacidad: 29/01/2026

Correo: olivia.garza@congresocdmx.gob.mx

13:12:46

Teléfono:

Visto: 29/01/2026 13:12:57

Emisor de la firma electrónica:

Confirmado:

Dibujada en dispositivo

29/01/2026 13:12:57.985

Plataforma: https://app.con-certeza.mx

Firmado:

29/01/2026 13:12:57.986

EL ESPACIO DEBAJO SE HA DEJADO EN BLANCO INTENCIONALMENTE

Método de validación de firmante:

Enlace de verificación

En el siguiente enlace se encuentra el portal para validar la constancia NOM-151 y el estado de integridad de este documento:
<https://app.con-certeza.mx/constancia/cd91330d-7a1b-4284-9e18-205892be0bb1>

