DIP. JESÚS SESMA SUÁREZ

PRESIDENTE DE LA MESA DIRECTIVA DE LA

DEL CONGRESO DE LA CIUDAD DE MÉXICO, III LEGISLATURA

P R E S E N T E

La que suscribe Diputada Elizabeth Mateos Hernández, integrante del Grupo Parlamentario de Morena, de la III Legislatura del Congreso de la Ciudad de México, con fundamento en lo dispuesto por el artículo 122 de la Constitución Política de los Estados Unidos Mexicanos; apartado D del artículo 29 de la Constitución Política de la Ciudad de México; artículos 4 fracción XXXVIII y 13 de la Ley Orgánica del Congreso de la Ciudad de México; así como los artículos 5 fracciones I y II, 99 fracción II, 100 y 120 del Reglamento del Congreso de la Ciudad de México, somete a consideración de esta soberanía la siguiente: **PROPOSICIÓN CON PUNTO DE ACUERDO, POR EL QUE SE EXHORTA RESPETUOSAMENTE A LA SECRETARÍA DE SEGURIDAD CIUDADANA DE LA CIUDAD DE MÉXICO, LA AGENCIA DIGITAL DE INNOVACIÓN PÚBLICA, ASÍ COMO LA PROCURADURÍA FEDERAL DEL CONSUMIDOR, PARA QUE, EN EL ÁMBITO DE SUS RESPECTIVAS ATRIBUCIONES Y CONFORME A SU DISPONIBILIDAD PRESUPUESTAL, FORTALEZCAN LAS ACCIONES DE PREVENCIÓN DE FRAUDES TELEFÓNICOS Y DIGITALES, MEDIANTE EL DISEÑO E IMPLEMENTACIÓN DE CAMPAÑAS PERMANENTES DE INFORMACIÓN Y ALERTA DIRIGIDAS A LA CIUDADANÍA, A TRAVÉS DE REDES SOCIALES, ASÍ COMO LA INCORPORACIÓN DE MENSAJES PREVENTIVOS, ALERTAS VISIBLES Y NOTIFICACIONES OFICIALES DENTRO DE LAS PROPIAS APLICACIONES DE COMERCIO ELECTRÓNICO, CON EL OBJETIVO DE PREVENIR LA SUPLANTACIÓN DE IDENTIDAD Y PROTEGER LOS DATOS PERSONALES Y EL PATRIMONIO DE LAS PERSONAS USUARIAS,** bajo los siguientes:

ANTECEDENTES

Hoy, en la Ciudad de México, basta una llamada o un mensaje para que una persona pase, en cuestión de minutos, de la tranquilidad a la incertidumbre. Un número desconocido aparece en el teléfono, alguien informa sobre un supuesto paquete pendiente, una entrega retenida o un envío que requiere verificación. El mensaje parece legítimo, incluso cotidiano. Después de todo, comprar en línea ya es parte de la vida diaria.

Sin embargo, detrás de esa aparente normalidad, se esconde una modalidad de fraude que ha evolucionado con rapidez y sofisticación, aprovechando la confianza de las personas en las plataformas digitales y en los servicios de mensajería.

Sin embargo, detrás de esa aparente normalidad, se esconde una modalidad de fraude que ha evolucionado con rapidez y sofisticación, aprovechando la confianza de las personas en las plataformas digitales y en los servicios de mensajería.

El crecimiento del comercio electrónico ha transformado profundamente los hábitos de consumo de la población. Cada vez más personas recurren a plataformas digitales para adquirir bienes y servicios, impulsadas por la facilidad, rapidez y accesibilidad que ofrecen estas herramientas. De acuerdo con el Estudio de Venta Online 2025 de la **Asociación Mexicana de Venta Online (AMVO)**[1], el comercio electrónico en México registró en 2024 un crecimiento cercano al **20%**, alcanzando un valor aproximado de **789 mil millones de pesos**, lo que refleja la consolidación de este modelo de consumo en la vida cotidiana.

Esta dinámica ha consolidado un ecosistema digital que forma parte esencial de la vida diaria, particularmente en una ciudad tan dinámica y conectada como la

[1] Disponible en: https://www.eleconomista.com.mx/el-empresario/comercio-electronico-mexico-crecio-20-2024-alcanzo-valor-789-000-millones-pesos-20250312-750213.html

nuestra. Pero ahí, precisamente donde hay confianza, también han encontrado espacio nuevas formas de engaño.

En los últimos meses, se ha identificado un incremento en los fraudes que utilizan como mecanismo la suplantación de plataformas de comercio electrónico, en los que delincuentes se hacen pasar por servicios de entrega mediante llamadas telefónicas, mensajes de texto, enlaces digitales o incluso anuncios en redes sociales.

El contacto inicial suele parecer inofensivo. Un mensaje breve, una notificación o una llamada que alude a una compra reciente o a un envío en proceso. En muchos casos, ni siquiera resulta extraño: la mayoría de las personas espera paquetes, realiza pedidos o consulta promociones con frecuencia. Esa familiaridad es justamente la puerta de entrada.

A partir de ahí, el discurso se construye sobre la urgencia. Se advierte sobre la posible cancelación de un envío, la necesidad de confirmar datos o la oportunidad de acceder a un beneficio limitado. La premura no es casual; reduce el margen de duda y empuja a actuar sin verificar.

El siguiente paso suele trasladar la interacción a un enlace o a un proceso guiado. Las personas son dirigidas a sitios que replican con gran precisión la imagen de plataformas de comercio electrónico, o bien, son acompañadas durante una llamada en la que se les solicita información específica. Todo ocurre con una narrativa coherente, cuidada, que busca no despertar sospechas.

En ese contexto, se solicitan datos personales, contraseñas, códigos de verificación o información bancaria bajo la apariencia de un procedimiento legítimo. La confianza ya ha sido construida y el entorno parece familiar, lo que dificulta identificar el engaño en el momento.

En algunos casos, la estrategia no se limita a un solo canal. Se combinan mensajes, llamadas y enlaces digitales para reforzar la credibilidad, generando

una experiencia que, para la persona usuaria, resulta consistente con el funcionamiento habitual de las plataformas que utiliza.

Una vez obtenida la información, las consecuencias son inmediatas. Se realizan cargos no reconocidos, transferencias o compras en línea, y en otros escenarios, los datos son utilizados posteriormente para esquemas más amplios de suplantación de identidad o fraudes financieros.

De acuerdo con información difundida por autoridades y medios de comunicación, una de las modalidades más recientes consiste en la creación de sitios web falsos que imitan la apariencia de plataformas de comercio electrónico, con el objetivo de obtener datos personales y bancarios de las personas usuarias.

Estos sitios fraudulentos suelen difundirse a través de enlaces enviados por mensaje de texto, redes sociales o incluso mediante anuncios en línea, presentando supuestas promociones, descuentos o beneficios exclusivos. En otros casos, el engaño inicia con una llamada telefónica en la que se informa sobre un paquete retenido o con problemas de entrega, generando un sentido de urgencia que busca inhibir la verificación de la información.

Las personas, al confiar en la veracidad del mensaje, acceden a estos enlaces o proporcionan información sensible, sin advertir que se trata de un esquema de suplantación de identidad. En muchos casos, los sitios apócrifos replican con gran precisión la imagen, logotipos y diseño de plataformas legítimas, lo que dificulta su identificación y aumenta la probabilidad de éxito del fraude.

El impacto de estas prácticas va más allá de una afectación económica inmediata. Una vez que los delincuentes obtienen datos personales o financieros, pueden utilizarlos para cometer otros delitos, como la suplantación de identidad, la contratación indebida de servicios financieros o la realización de operaciones ilícitas a nombre de las víctimas.

Asimismo, se ha observado un incremento en fraudes telefónicos vinculados a estas prácticas, en los que se solicita a las personas proporcionar códigos de

verificación, realizar depósitos o compartir información confidencial bajo distintos pretextos relacionados con envíos o entregas.

Este tipo de esquemas, conocidos como vishing y smishing, combinan técnicas de ingeniería social con el uso de tecnologías de comunicación, lo que les permite generar escenarios creíbles y ejercer presión inmediata sobre las víctimas.

Además de la percepción cotidiana del problema, existen datos que dimensionan con claridad la magnitud de esta situación. En México, más de 13. 5 millones de personas han sido víctimas de fraudes cibernéticos, 23.1% han perdido dinero, en promedio $8,750 pesos[2]; lo que refleja no solo la expansión de estas conductas delictivas, sino también su impacto directo en la vida de millones de personas que utilizan herramientas digitales de manera habitual.

Esta cifra implica que una parte significativa de la población ha estado expuesta a esquemas de engaño que operan, en su mayoría, a través de medios electrónicos, confirmando que el entorno digital se ha convertido en un espacio prioritario tanto para la actividad económica como para la comisión de delitos.

Por su parte, la **Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros**[3] ha señalado que los fraudes relacionados con operaciones digitales y comercio electrónico han mostrado un crecimiento del 76.9% en los últimos años, destacando que una proporción importante de las reclamaciones presentadas por las personas usuarias está vinculada con consumos no reconocidos, transferencias electrónicas no autorizadas y el uso indebido de datos personales.

[2] Disponible en: https://www.theciu.com/publicaciones-2/2025/6/16/phishing-en-mxico-amenaza-creciente-y-llamado-a-la-accin

[3] Disponible en: https://www.eleconomista.com.mx/finanzaspersonales/cuida-bolsillo-fraudes-bancarios-dia-presentan-14-000-quejas-delito-20260324-805220.html#:~:text=Crecen%20fraudes%20en%20l%C3%ADnea%20en%20el%20pa%C3%ADs&text=Informaci%C3%B3n%20de%20la%20Condusef%20se%C3%B1ala,y%20corroborar%20con%20la%20instituci%C3%B3n.

Asimismo, se ha advertido que muchos de estos fraudes se concretan a partir de técnicas de ingeniería social, en las que las personas son persuadidas para proporcionar información confidencial bajo esquemas que simulan ser comunicaciones oficiales o procesos legítimos.

Uno de los factores que explica la efectividad de estas modalidades es el uso de canales cotidianos y de alta confianza para la ciudadanía. Estos fraudes no operan en espacios ajenos o desconocidos, sino en los mismos entornos digitales que las personas utilizan todos los días: sus teléfonos móviles, sus redes sociales y las aplicaciones de comercio electrónico.

En este sentido, el problema no radica únicamente en la existencia de estas conductas delictivas, sino en la forma en que logran insertarse en la vida cotidiana de las personas, aprovechando hábitos, rutinas y niveles de confianza previamente construidos.

Por otro lado, es importante reconocer que el Estado mexicano ha impulsado acciones relevantes para atender delitos como la extorsión, entre ellas la iniciativa para que este delito sea perseguido de oficio, trasladando la carga de la denuncia del ciudadano al Estado. Este tipo de medidas representa un avance significativo en la protección de las víctimas y en el fortalecimiento de la respuesta institucional.

No obstante, la evolución constante de los fraudes digitales plantea la necesidad de complementar estas acciones con estrategias preventivas más eficaces, particularmente aquellas que permitan anticipar los riesgos y reducir la probabilidad de que las personas sean víctimas.

Actualmente, si bien existen campañas informativas y recomendaciones emitidas por autoridades, estas no siempre logran llegar de manera oportuna a la ciudadanía, especialmente en el momento en que se enfrenta a un posible intento de fraude.

Por ello, resulta fundamental replantear las estrategias de prevención, orientándolas hacia esquemas más directos, visibles y permanentes, que

permitan llevar la información a los espacios donde realmente ocurre la interacción digital.

En este contexto, las redes sociales y las aplicaciones de comercio electrónico se convierten en herramientas clave para la difusión de alertas y mensajes preventivos, al concentrar una parte significativa de la actividad digital de la población.

La incorporación de alertas visibles, notificaciones oficiales y mensajes preventivos dentro de estas plataformas permitiría advertir a las personas usuarias en tiempo real sobre posibles riesgos, reduciendo significativamente la posibilidad de que sean engañadas.

De igual manera, el fortalecimiento de campañas permanentes en redes sociales contribuiría a generar una mayor cultura de prevención, facilitando la identificación de conductas sospechosas y promoviendo una participación más informada por parte de la ciudadanía.

CONSIDERANDOS

PRIMERO. Que el artículo 1° de la **Constitución Política de los Estados Unidos Mexicanos**[4] establece que,

"*Todas las autoridades, en el ámbito de sus competencias, tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad. En consecuencia, el Estado deberá prevenir, investigar, sancionar y reparar las violaciones a los derechos humanos, en los términos que establezca la ley".*

SEGUNDO. Que el artículo 6°, segundo párrafo de la **Constitución Política de los Estados Unidos Mexicanos** reconoce lo que a la letra señala:

[4] Disponible en: https://mexico.justia.com/federales/constitucion-politica-de-los-estados-unidos-mexicanos/titulo-primero/capitulo-i/#articulo-1o

"Reconoce el derecho de acceso a la información, lo que implica que el Estado debe generar y difundir información clara, oportuna y accesible que permita a la población identificar riesgos asociados al uso de plataformas digitales y servicios en línea. (…)".

TERCERO. Que la **Constitución Política de la Ciudad de México** reconoce, en su artículo 7, apartado E, numerales 1 y 3, que:

"ARTÍCULO 7 CIUDAD DEMOCRÁTICA

E. Derecho a la privacidad y a la protección de los datos personales

1. *Toda persona tiene derecho a que se respete y proteja su privacidad individual y familiar, a la inviolabilidad del domicilio y de sus comunicaciones.*
3. *Se prohíbe y será sancionada cualquier injerencia arbitraria, oculta o injustificada en la vida de las personas".*

CUARTO. Que la **Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México**[5] dispone en su **artículo 6** que:

"El Estado garantizará la privacidad de los individuos y deberá velar porque terceras personas no incurran en conductas que puedan afectarla arbitrariamente.

El derecho a la protección de los datos personales solamente se limitará por razones de seguridad nacional, en términos de la ley en la materia, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros".

RESOLUTIVO

ÚNICO. - SE EXHORTA RESPETUOSAMENTE A LA SECRETARÍA DE SEGURIDAD CIUDADANA DE LA CIUDAD DE MÉXICO, LA AGENCIA DIGITAL DE INNOVACIÓN PÚBLICA, ASÍ COMO LA PROCURADURÍA FEDERAL DEL CONSUMIDOR, PARA QUE, EN EL ÁMBITO DE SUS RESPECTIVAS ATRIBUCIONES Y CONFORME A SU DISPONIBILIDAD PRESUPUESTAL, FORTALEZCAN LAS ACCIONES DE PREVENCIÓN DE FRAUDES TELEFÓNICOS Y DIGITALES, MEDIANTE EL DISEÑO E IMPLEMENTACIÓN DE CAMPAÑAS PERMANENTES DE INFORMACIÓN Y ALERTA

[5] Disponible en : https://www.scjn.gob.mx/sites/default/files/marco_normativo/documeto/2025-04/Ley-General-de-Proteccion-Datos-Personales-en-Posesion-Sujetos-Obligados-DOF-20250320.docx

DIRIGIDAS A LA CIUDADANÍA, A TRAVÉS DE REDES SOCIALES, ASÍ COMO LA INCORPORACIÓN DE MENSAJES PREVENTIVOS, ALERTAS VISIBLES Y NOTIFICACIONES OFICIALES DENTRO DE LAS PROPIAS APLICACIONES DE COMERCIO ELECTRÓNICO, CON EL OBJETIVO DE PREVENIR LA SUPLANTACIÓN DE IDENTIDAD Y PROTEGER LOS DATOS PERSONALES Y EL PATRIMONIO DE LAS PERSONAS USUARIAS

Dado en el Recinto del Congreso de la Ciudad de México, a los siete días del mes de mayo de dos mil veintiséis.

ATENTAMENTE

Elizabeth Mateos Hernández

DIP. ELIZABETH MATEOS HERNÁNDEZ

SUITE LEGAL con certeza

ACTA DE PROCESO DE FIRMA

Certificado de firma 04/05/2026 11:01

Documento electrónico

Identificador: 69F8CFA25DEFE560F06DE0BB
Nombre y extensión: P.A ESTAFA COMERCIO ELECTRONICO firmado).pdf
Descripción:
Cantidad de páginas: 3
Estado: Firmado
Firmantes: 1
Huella digital del contenido del documento original:
1f75611c0525b11d3567cb57c9bc7290acb0b79d4ea7fffa4346ed3a1102e06f
Huella digital del contenido del documento firmado:
d9d90f5f5d526913aa1348c80d735e9efb207a504b035dc30d1582f25dd6e879

Solicitante del proceso de firma Almacenado

Nombre: Elizabeth Mateos Hernández
Compañía: SR LUZ SA DE CV
Correo electrónico: elizabeth.mateos@congresocdmx.gob.mx
Teléfono:

Dirección IP: 2806:107e:10:8964:f4eb:70e7:c62d:5c84

Fecha y hora de emisión
(America/Mexico_City):
04/05/2026 10:56

Constancia de conservación del documento firmado

Información de la constancia NOM-151

Fecha de emisión:
04/05/2026 17:01:35 UTC (04/05/2026 11:01:35 Hora local de la Ciudad de México)
Nombre y extensión:
d236c5ee-724c-4540-a430-444f165ee87f.cons
Huella digital contenida en la constancia:
d9d90f5f5d526913aa1348c80d735e9efb207a504b035dc30d1582f25dd6e879

Información del emisor de la constancia NOM-151

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. Elizabeth Mateos Hernández

Atributos	Firma	Fecha
Tipo de actuación: Por su Propio Derecho Compañía: Método de notificación: Correo Correo: elizabeth.mateos@congresocdmx.gob.mx Teléfono: Emisor de la firma electrónica: Dibujada en dispositivo Plataforma: https://app.con-certeza.mx	ID: 69F8D0E8BB309657003856C7 IP: 2806:107e:10:8964:f4eb:70e7:c62d:5c84 Firma con texto Elizabeth Mateos Hernández	Enviado: 04/05/2026 11:00:16 Aceptó Aviso de Privacidad: 04/05/2026 11:01:28 Visto: 04/05/2026 11:01:28 Confirmado: 04/05/2026 11:01:29.099 Firmado: 04/05/2026 11:01:29.1

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/d236c5ee-724c-4540-a430-444f165ee87f