



"2026, AÑO DEL BICENTENARIO DEL NATALICIO DE MARGARITA MAZA PARADA, EJEMPLO DE DIGNIDAD, LEALTAD Y SERVICIO A LA NACIÓN"

**Haydeé
REYES**

Diputada Local Distrito 13 - Oaxaca de Juárez

OFICIO NÚMERO: LXVI/HCEO/HIRS/015/2026.
ASUNTO: SE PRESENTA INICIATIVA.

San Raymundo Jalpan, Oax; a 13 de febrero de 2026.

LIC. FERNANDO JARA SOTO.
SECRETARIO DE SERVICIOS PARLAMENTARIOS
DEL H. CONGRESO DEL ESTADO DE OAXACA.
EDIFICIO.

DIPUTADA HAYDEÉ IRMA REYES SOTO, integrante del Grupo Parlamentario del Partido MORENA de la LXVI Legislatura Constitucional del H. Congreso del Estado Libre y Soberano de Oaxaca, con fundamento en lo dispuesto por los artículos 50, fracción I, de la Constitución Política del Estado Libre y Soberano de Oaxaca; 30, fracción I y 104, fracción I de la Ley Orgánica del Poder Legislativo del Estado de Oaxaca; 3 fracción XVIII y 54 fracción I del Reglamento Interior del Congreso del Estado, me permito presentar a consideración de este Honorable Congreso del Estado para su estudio, discusión y aprobación la iniciativa y proposición con Punto de Acuerdo de Urgente y Obvia resolución siguientes:

ÚNICO: INICIATIVA CON PROYECTO DE DECRETO POR LA QUE SE ADICIONA EL ARTÍCULO 382 BIS AL CÓDIGO PENAL PARA EL ESTADO LIBRE Y SOBERANO DE OAXACA, EN MATERIA DE FRAUDE DIGITAL.

Sin otro particular, reciba un cordial saludo.

H. CONGRESO DEL ESTADO DE OAXACA

LXVI LEGISLATURA

RECIBIDO
13 FEB 2026
15:49 h

Secretaría de Servicios Parlamentarios

HIRS/avpm
C.c.p. minutarlo

ATENTAMENTE

"EL RESPETO AL DERECHO AJENO ES LA PAZ"

DIP. HAYDEÉ IRMA REYES SOTO

H. CONGRESO DEL ESTADO DE OAXACA

LXVI LEGISLATURA

RECIBIDO
13 FEB 2026

Dirección de Apoyo Legislativo
y Comisiones



GOBIERNO CONSTITUCIONAL
DEL ESTADO DE OAXACA
PODER LEGISLATIVO

LXVI LEGISLATURA
DIP. HAYDEÉ IRMA REYES SOTO
OAXACA DE JUÁREZ
DISTRITO 13

DIPUTADA EVA DIEGO CRUZ.
PRESIDENTA DE LA MESA DIRECTIVA DEL SEGUNDO AÑO DE
EJERCICIO LEGAL DEL H. CONGRESO DEL ESTADO DE OAXACA.
P R E S E N T E.

1

DIPUTADA HAYDEÉ IRMA REYES SOTO, integrante del Grupo Parlamentario del Partido MORENA de la LXVI Legislatura Constitucional del H. Congreso del Estado Libre y Soberano de Oaxaca, con fundamento en lo dispuesto por los artículos 50, fracción I, de la Constitución Política del Estado Libre y Soberano de Oaxaca; 30, fracción I y 104, fracción I de la Ley Orgánica del Poder Legislativo del Estado de Oaxaca; 3 fracción XVIII y 54 fracción I del Reglamento Interior del Congreso del Estado, me permito presentar a consideración de este Honorable Congreso del Estado, para su estudio, análisis, dictaminación y aprobación, la siguiente:

INICIATIVA CON PROYECTO DE DECRETO POR LA QUE SE ADICIONA EL ARTÍCULO 382 BIS AL CÓDIGO PENAL PARA EL ESTADO LIBRE Y SOBERANO DE OAXACA, EN MATERIA DE FRAUDE DIGITAL.

Fundamento lo anterior, al tenor de la presente:

EXPOSICIÓN DE MOTIVOS

PRIMERO. La Constitución Política de los Estados Unidos Mexicanos establece en su artículo 1° que todas las personas gozarán de los derechos humanos reconocidos en esta Constitución y en los tratados internacionales de los que el Estado Mexicano sea parte, así como de las garantías para su protección, cuyo ejercicio no podrá restringirse ni suspenderse, salvo en los casos y bajo las condiciones que esta Constitución establece. Asimismo, señala que, todas las autoridades tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos de todas las personas de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad y que en todas las decisiones se otorgará a las personas la protección más amplia. Dentro de este catálogo se encuentran contemplados los derechos contenidos en los tratados internacionales en materia de derechos humanos.

En el mismo tenor, el artículo 12 de la Constitución Política del Estado Libre y Soberano de Oaxaca establece que en el Estado todas las personas gozarán de los derechos humanos reconocidos en la Constitución Política de los Estados Unidos Mexicanos, los tratados internacionales de los que el Estado Mexicano sea parte y esta Constitución. El poder público garantizará su protección cuyo ejercicio no podrá restringirse ni suspenderse, salvo en los casos y bajo las condiciones que la Constitución Política de los Estados Unidos Mexicanos establece.

Asimismo, señala que la interpretación de las normas relativas a los derechos humanos, se hará conforme a lo establecido en la Constitución Política de los Estados Unidos Mexicanos, favoreciendo en todo tiempo a las personas la protección más amplia. Para el ejercicio de los derechos humanos y las garantías constitucionales no se exigirán condiciones o requisitos que no estén establecidos en la Constitución o la ley. Ninguna norma jurídica podrá restringir los derechos humanos ni sus garantías.

2

En el ámbito internacional, la **Convención Americana sobre Derechos Humanos "Pacto San José"**, establece¹:

Artículo 1. Obligación de Respetar los Derechos

1. *Los Estados Partes en esta Convención se comprometen a respetar los derechos y libertades reconocidos en ella y a garantizar su libre y pleno ejercicio a toda persona que esté sujeta a su jurisdicción, sin discriminación alguna por motivos de raza, color, sexo, idioma, religión, opiniones políticas o de cualquier otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición social.*
2. *Para los efectos de esta Convención, persona es todo ser humano.*

Artículo 2. Deber de Adoptar Disposiciones de Derecho Interno

Si el ejercicio de los derechos y libertades mencionados en el artículo 1 no estuviere ya garantizado por disposiciones legislativas o de otro carácter, los Estados Partes se comprometen a adoptar, con arreglo a sus procedimientos constitucionales y a las disposiciones de esta Convención, las medidas legislativas o de otro carácter que fueren necesarias para hacer efectivos tales derechos y libertades.

Por otra parte, la Corte Interamericana de Derechos Humanos (CIDH) en la Jurisprudencia denominada: Postulados tomados del Derecho Internacional de los Derechos Humanos, en el Punto 3.- Los instrumentos o medios procesales destinados a garantizar los derechos humanos, deben ser efectivos, señala que el Derecho Internacional de los Derechos Humanos, es un ordenamiento jurídico dirigido en dos vías; la primera de ellas hacia la protección efectiva de las víctimas de violaciones, y la segunda para evitar violaciones, (sentido preventivo). Este corpus jurídico, ha desarrollado una máxima que estipula, que tanto los instrumentos jurídicos que consagran derechos, como especialmente los medios procesales para salvaguardarlos, deben ser efectivos.²

Respecto al marco jurídico nacional, el **Código Penal Federal** establece las reglas generales sobre delitos, definiendo al delito, los tipos de delitos y formas de comisión ya sea por acción u omisión de forma dolosa o culposa y la responsabilidad.

¹ Convención Americana sobre Derechos Humanos (Pacto San José) Visible en el link: https://www.oas.org/dil/esp/1969_Convencion_Americana_sobre_Derechos_Humanos.pdf

² CIDH. Instituto de Relaciones Internacionales. LA JURISPRUDENCIA DE LA CORTE INTERAMERICANA: POSTULADOS TOMADOS DEL DERECHO INTERNACIONAL DE LOS DERECHOS HUMANOS. Visible en el link: https://www.iri.edu.ar/publicaciones_iri/IRI%20COMPLETO%20-%20Publicaciones-V05/Publicaciones/T4/T407.html

En nuestro **Código Penal para el Estado Libre y Soberano de Oaxaca**, se establece un Título específico denominado Aplicación de Sanciones, dentro del cual el Capítulo I "Graduación de la culpabilidad e individualización de la pena" se establecen las reglas generales para la imposición de las sanciones, así como los criterios para la individualización de las penas y medidas de seguridad.

En ese sentido, conforme al marco jurídico internacional, nacional y estatal se establece que todas las autoridades tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos de todas las personas de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad y que en todas las decisiones se otorgará a las personas la protección más amplia, así como los lineamientos jurídicos que se deben observar para la aplicación e imposición de las sanciones y los criterios para la individualización de las penas y medidas de seguridad que se aplicarán por la autoridad jurisdiccional.

SEGUNDO. En la actualidad una nueva forma de comisión de los delitos en México ha sido a través de las redes sociales, internet, los medios digitales y de los dispositivos electrónicos, particularmente en el caso del delito de fraude.

El **fraude electrónico** en México es un problema creciente que incluye phishing, smishing, vishing, suplantación de identidad y uso de IA (deepfakes), para robar datos o dinero a través de correos, SMS, llamadas o sitios falsos, con pérdidas económicas significativas y un aumento en la sofisticación de los ataques.

En otro aspecto, el **fraude cibernético** es cualquier tipo de engaño, estafa o actividad delictiva realizada a través de internet y dispositivos electrónicos, con el objetivo de obtener beneficios económicos, robar datos personales o información confidencial. Se basa principalmente en la manipulación humana y el engaño, utilizando técnicas como phishing, suplantación de identidad y sitios web falsos para engañar a usuarios.³

El **fraude** conforme a nuestro Código Penal del Estado se comete cuando se engañe a una persona o se aproveche del error en que ésta se encuentre, para hacerse ilícitamente de alguna cosa o alcance un lucro indebido. Este delito se castiga conforme a las penas establecidas en el artículo 380, señalando como penas las siguientes:

Artículo 380. ...

1.- Con prisión de tres meses a tres años y multa de cinco a cien veces el valor de la Unidad de Medida y Actualización vigente, cuando el valor de lo defraudado no exceda de esta última cantidad;

³ Hubler Ciberseguridad. Qué es un fraude cibernético. 14 de septiembre de 2020. Visible en el link: <https://www.google.com/url?sa=i&source=web&rct=j&url=https://hubler.es/que-es-un-fraude-cibernetico/&ved=2ahUKEwITrommteSAxXGLkQIHcmKMRsQ1fkOegQIBhAC&opi=89978449&cd&psig=AOvVaw2rdIkOYE7uIN-ITM3ts6xo&ust=1771097588103000>

"2026, AÑO DEL BICENTENARIO DEL NATALICIO DE MARGARITA MAZA PARADA, EJEMPLO DE DIGNIDAD, LEALTAD Y SERVICIO A LA NACIÓN"

II.- Con prisión de tres a seis años y multa de cien a ciento cincuenta veces el valor de la Unidad de Medida y Actualización vigente, cuando el valor de lo defraudado exceda de cien veces el valor de la Unidad de Medida y Actualización vigente; pero no de quinientas veces;

III.- Con prisión de seis a doce años y multa de ciento cincuenta a quinientas veces el valor de la Unidad de Medida y Actualización vigente, cuando el valor de lo defraudado exceda de ésta última cantidad.

En México, la **Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros** ha reportado un crecimiento constante de **fraudes electrónicos o digitales** vinculados a redes sociales y transferencias bancarias.⁴

La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (**Condusef**) ha revelado que los **fraudes digitales** son cada vez más comunes y el Internet es la principal vía de ataque. Señala que las compras en **Redes sociales falsas** han ganado popularidad gracias a que utiliza anuncios falsos para atraer la confianza de los usuarios, incluso con promesas de beneficios económicos.

El fraude cibernético señala la **CONDUSEF** son aquellas estafas que utilizan la red, para realizar transacciones ilícitas. Muchas veces las personas que realizan este tipo de fraudes, se aprovechan del desconocimiento o del poco cuidado que las personas tienen al utilizar los servicios financieros en línea, convirtiéndose en un blanco fácil para los estafadores.⁵ Por su parte en entrevista para UNAM Global, Juan Manuel Aguilar Antonio, investigador postdoctoral, y Lorena de la Barrera, doctorante en ética de tecnologías emergentes e inteligencia artificial, ambos del **El Centro de Investigaciones sobre América del Norte (CISAN)** señaló que Facebook, Instagram, TikTok, WhatsApp todas concentran estafas de distintos tipos. Promociones tentadoras, sorteos falsos, perfiles clonados o audios con voces modificadas por IA forman parte del arsenal de los ciberdelinquentes. En 2023, el **80% de los fraudes digitales se originaron en plataformas sociales**. Y el 69% de los usuarios fue expuesto a contenidos fraudulentos.⁶

Por otra parte, el fraude en redes sociales presenta las características particulares siguientes⁷:

- **Engaño digital estructurado** (publicidad simulada, perfiles apócrifos).
- **Aprovechamiento del entorno tecnológico** para inducir error.
- **Transferencia patrimonial electrónica inmediata**.
- **Desaparición o bloqueo inmediato del perfil**.
- **Posible utilización de identidades robadas**.

⁴El Universal, Aumentan los fraudes digitales: esto debes evitar según Condusef, 2026, disponible en <https://www.eluniversal.com.mx/techbit/aumentan-los-fraudes-digitales-esto-debes-evitar-segun-condusef/>

⁵ Condusef, tipos de fraude, disponible en <https://www.condusef.gob.mx/?p=tipos-de-fraude>

⁶UNAM, Global Revista, Fraudes digitales y ciberseguridad: cómo protegerte en redes sociales, apps y correos, 2025. disponible en https://unamglobal.unam.mx/global_revista/fraudes-digitales-ciberseguridad-proteccion-redes-apps-correos/

⁷Gobierno de México, Fraudes cibernéticos, 2023, disponible en <https://www.gob.mx/gncertmx/articulos/105209>

- Además, vulnera bienes jurídicos como el patrimonio, la seguridad en las transacciones electrónicas, la confianza pública en el comercio digital y la protección de datos personales.

Lo anterior, ha sido derivado principalmente del **comercio en redes sociales**, pues se ha convertido en una alternativa económica para microemprendedores locales; sin embargo, también ha sido aprovechado por sujetos que operan desde la informalidad y la anonimidad. En razón de ello, ante la ausencia de una figura penal específica se dificulta la clasificación jurídica del hecho, se obstaculiza la integración de carpetas de investigación, se reduce la posibilidad de agravantes y lo más triste es que genera impunidad técnica.

TERCERO.- El crecimiento exponencial del comercio electrónico y el uso masivo de plataformas digitales han generado nuevas oportunidades de negocio, pero también han facilitado esquemas de engaño que vulneran el patrimonio de las personas mediante perfiles falsos, ofertas inexistentes, y pagos sin entrega de bienes o servicios. Legislar el **fraude digital asociado a compras en línea** en Oaxaca no solo permitiría armonizar la normatividad estatal con las necesidades tecnológicas actuales, sino también fortalecerá el marco de protección para personas usuarias de servicios digitales.

Lo anterior es así, ya que el comercio electrónico en redes sociales o social commerce permite comprar productos directamente dentro de plataformas como Instagram, TikTok y Facebook, integrando la experiencia de compra en el contenido social sin salir de la aplicación. Esta tendencia aumenta las conversiones, reduce la fricción de compra y facilita el descubrimiento de productos.

El **comercio social** es una tendencia emergente que combina las redes sociales y el comercio electrónico para proporcionar una experiencia de compra más integrada. Las plataformas de redes sociales están introduciendo funciones de comercio electrónico, permitiendo a los usuarios comprar productos directamente desde las publicaciones y las historias.

Esto reduce la fricción en el proceso de compra, ya que los consumidores no tienen que abandonar la aplicación para realizar una compra. Sin embargo, esto también plantea desafíos en términos de logística y servicio al cliente, ya que las empresas deben ser capaces de gestionar los pedidos y resolver los problemas de los clientes en una variedad de plataformas.

Por su parte, las **redes sociales** son una plataforma efectiva para la publicidad de productos. Las empresas pueden utilizar la segmentación detallada para llegar a su público objetivo con anuncios relevantes. Sin embargo, la publicidad en redes sociales también presenta desafíos.

En ese sentido, si bien el comercio electrónico en redes sociales ofrece accesibilidad y dinamismo económico; también, presenta **vacíos regulatorios, alta exposición a fraude, debilidad en**

mecanismos de protección al consumidor y riesgos en el manejo de datos personales, lo que lo convierte en un entorno de **alta vulnerabilidad jurídica y financiera**, especialmente en mercados locales donde no existe supervisión constante.

Al respecto, los *fraudes comunes relacionados con comercio en redes sociales en México son los relacionados con:*⁸

- **Tiendas y anuncios falsos:** Los estafadores crean perfiles o páginas que parecen legítimas, a menudo con ofertas y descuentos imposibles para atraer a las víctimas.
- **Productos que no llegan:** El fraude más sencillo: pagas por un artículo y nunca lo recibes.
- **Phishing:** Envían mensajes con enlaces maliciosos para robar tus datos personales y bancarios.
- **Cuentas falsas:** Utilizan perfiles falsos para interactuar contigo, generar confianza y luego cometer la estafa.

Bajo ese contexto, considero que Oaxaca no se debe quedar al margen y también debe regular en el Código Penal del Estado esta conducta que cada vez va en aumento, pues la incidencia delictiva cometida con el uso de las herramientas tecnológicas va en aumento, por tal motivo, legislar para establecer en nuestra norma penal que esta conducta pueda ser sancionada en la comisión del delito de fraude, representa un avance significativo en la imposición de sanciones, pues nuestra Ley debe actualizarse a las nuevas formas de comisión de delitos. Aunado a que incorporar esta conducta como agravante significaría alinear la legislación estatal con las tendencias nacionales e internacionales, así como consolidar un marco jurídico que garantice la impartición de justicia.

CUARTO. En los últimos años, México ha enfrentado una transformación de la delincuencia que implica cada vez con mayor intensidad el **uso de tecnología como medio para cometer delitos que afectan la seguridad pública y el orden social**. Por tal motivo, para mayor ilustración, se presentan estadísticas de delitos cometidos con el uso de medios o herramientas tecnológicas.

1. Ciberdelitos con impacto económico y seguridad pública.

Una de las formas más significativas de delitos tecnológicos en México es el **fraude y el phishing masivo**, donde los delincuentes emplean herramientas digitales, ingeniería social, aplicaciones y sistemas de comunicación para engañar a víctimas y obtener recursos o datos sensibles. En 2024, México registró aproximadamente **6 millones de casos de phishing**, lo que representa un incremento sostenido de estos delitos en años recientes, con pérdidas económicas que **superan los 20 000 millones de pesos** para las víctimas afectadas.

⁸Gobierno de México, *Compras en Línea que no llegaron, 2020*, disponible en <https://www.gob.mx/profeco/articulos/compras-en-linea-que-no-llegaron?idiom=es>

Tipo de delito tecnológico	Estadística en México (2024)	Fuente
Ciberacoso (personas)	18.9 millones de víctimas (21% usuarios)	INEGI MOCIBA 2024 (INEGI)
Ciberacoso por sexo	22.2% mujeres, 19.6% hombres	INEGI MOCIBA 2024 (INEGI)
Fraude cibernético	6 millones casos con >20,000 M pesos pérdida	CIU y reportes de 2025 (El País)
Intentos de ciberataques	>31 mil millones intentos en 6 meses	Reuters / Fortinet (Noticias Sociales MX)
Empresas atacadas	39% sufrió ciberataque (costos altos)	Informe KPMG 2024 (IT Masters Mag)
Investigaciones y ciberpatrullajes	242,943 ciberpatrullajes est.	Guardia Nacional/Policías cibernéticas (La Verdad Noticias)

Además, estudios de seguridad digital indican que **48 % de los usuarios mexicanos de dispositivos móviles reportaron haber sufrido algún tipo de ciberataque o fraude en su teléfono**, cifra que está por encima del promedio global, lo cual muestra la magnitud del fenómeno dentro del país.

2. Intentos masivos de ataques a infraestructura tecnológica.

México ha sido identificado como uno de los países con mayor exposición a ataques cibernéticos en América Latina. En la primera mitad de 2024 se estimó que el país concentró alrededor del **55 % de todos los intentos de ataques cibernéticos en la región**, con un total de **más de 31 mil millones de intentos de intrusión o amenazas detectadas**.⁹ Esto incluye intentos de acceso no autorizado, malware, ransomware y actividades automatizadas contra redes empresariales y gubernamentales.

3. Tecnologías usadas para delitos tradicionales.

Además del cibercrimen puramente digital, la tecnología también ha **facilitado delitos tradicionales que impactan directamente la seguridad pública física**.

- El uso de **sistemas de comunicación y dispositivos electrónicos** para coordinar extorsiones, amenazas y cobros ilegales ha aumentado en varios estados del país. En 2025 se reportó un crecimiento significativo de extorsiones que a menudo comienzan o se sustentan mediante llamadas, mensajes y aplicaciones de mensajería, afectando negocios, familias y comunidades.
- La **suplantación de identidad con fines de fraude** (por ejemplo, fraudes de "paquetería fantasma" donde se suplanta a empresas como Amazon o DHL para obtener dinero) ha crecido notablemente, con aumentos porcentuales de más del 200% ¹⁰ en ciertos periodos, reflejando cómo acciones tecnológicas simples mensajes y llamadas se convierten en delitos de alto impacto económico.

⁹ Reuters. (2024, 9 de octubre). *Mexico faces over half of Latin American cybercrimes due largely to U.S. ties*. Reuters. <https://www.reuters.com/world/americas/mexico-faces-over-half-latin-american-cybercrimes-due-largely-us-ties-2024-10-09/>

¹⁰ El País. (2024, 11 de diciembre). *Los fraudes por paquetería fantasma en Ciudad de México aumentan un 222 %; Amazon y DHL, entre las empresas más suplantadas*. El País.

En estos casos, si bien el resultado puede no ser un ataque físico directo, la **tecnología actúa como herramienta principal para la comisión del delito**, con consecuencias tangibles para la seguridad económica y social de las víctimas.

✦ 4. La influencia de grupos criminales y tecnología avanzada

Aunque no es un fenómeno exclusivamente moderno, la **criminalidad organizada ha incorporado tecnología de distinta complejidad en sus operaciones delictivas**. Esto abarca desde el uso de teléfonos encriptados y redes para coordinar actividades delictivas, hasta sistemas de rastreo para evadir a las autoridades o planear ataques y extorsiones con mayor precisión.

Estos patrones muestran cómo los grupos del crimen organizado integran soluciones tecnológicas no solo para proteger sus comunicaciones, sino para facilitar delitos que afectan la seguridad pública en términos más amplios.

✦ Conclusión: La Tecnología como Medio para Delitos con Impacto en la Seguridad Pública

En México, la tecnología ha dejado de ser únicamente un facilitador de delitos exclusivamente digitales para convertirse en una **herramienta habitual dentro de la comisión de delitos que afectan la seguridad física, económica y social de la población**.

Los datos recientes muestran que:

- Millones de personas sufren **fraudes tecnológicos y phishing** con impactos económicos **significativos**.
- México enfrenta **decenas de miles de millones de intentos de ataques tecnológicos** a sistemas informáticos e infraestructura digital.
- Delitos tradicionales como la **extorsión y el fraude de identidad** están cada vez más vinculados a medios tecnológicos de comunicación.

1. Ciberdelitos prevenidos por la Policía Cibernética de Oaxaca (enero–julio 2025)

La **Unidad de Policía Cibernética de Oaxaca** informó que, de enero a julio de 2025, logró impedir pérdidas económicas por más de **\$17 382 866 pesos¹¹** derivado de delitos tecnológicos como:

- **Extorsión cibernética**
- **Suplantación de identidad**
- **Fraude electrónico**
- **Cobranza ilegal**

2. Delitos cibernéticos atendidos por reporte ciudadano (diciembre 2025)

<https://elpais.com/mexico/2024-12-11/los-fraudes-por-paqueteria-fantasma-en-ciudad-de-mexico-aumentan-un-222-amazon-y-dhl-entre-las-empresas-mas-suplantadas.html>

¹¹ Gobierno del Estado de Oaxaca. (2025). *Evita SSPC pérdidas por más de 17 millones de pesos en ciberdelitos en Oaxaca*. Secretaría de Seguridad y Protección Ciudadana del Estado de Oaxaca.
<https://www.oaxaca.gob.mx/comunicacion/evita-sspc-perdidas-por-mas-de-17-mdp-en-ciberdelitos-en-oaxaca/>

"2026, AÑO DEL BICENTENARIO DEL NATALICIO DE MARGARITA MAZA PARADA, EJEMPLO DE DIGNIDAD, LEALTAD Y SERVICIO A LA NACIÓN"

Entre 20 y 26 de diciembre de 2025, la Policía Cibernética de Oaxaca atendió 160 acciones de prevención e investigación de delitos tecnológicos en el estado, donde se registraron:

- 112 casos por reportes ciudadanos
- 45 denuncias formales por extorsión u otros delitos
- 10 solicitudes de colaboración con la Fiscalía

9

Distribución porcentual de los delitos delictivos electrónicos registrados:

- 40.2 % extorsión
- 23.2 % suplantación de identidad
- 17.9 % fraude informático
- 14.2 % otros incidentes digitales ¹²
- 2.7 % extorsión sexual
- 1.8 % cobranza ilegal

Esto demuestra que los delitos tecnológicos más recurrentes en Oaxaca son la extorsión, fraude y suplantación, todos cometidos mediante medios digitales.

3. Acciones de la Policía Cibernética (enero 2026)

Del 10 al 23 de enero de 2026, la Unidad de Policía Cibernética de Oaxaca realizó un total de 406 acciones de prevención e investigación de delitos tecnológicos, lo que incluye atención de reportes, investigaciones y medidas de protección digital. ¹³

4. Reportes y acciones semanales de ciberdelitos (2025)

Durante la semana del 30 de agosto al 5 de septiembre de 2025, la Policía Cibernética de Oaxaca:

- Atendió 90 reportes ciudadanos relacionados con delitos tecnológicos.
- Realizó 180 acciones de prevención e investigación.
- Evitó pérdidas económicas por \$293 280 pesos.
- Los delitos detectados incluyeron:
 - Fraudes (23.3 %)
 - Extorsiones (21.1 %)
 - Suplantación de identidad (14.4 %)
 - Cobranza ilegal (5.6 %)
 - Extorsión sexual (2.2 %) ¹⁴

5. Patrón geográfico de ciberdelitos en Oaxaca (2025)

En diciembre de 2025, la región que concentró más casos de delitos tecnológicos fue Valles Centrales, con 38 reportes semanales, seguida por Mixteca y el Istmo de Tehuantepec.

¹² El Imparcial de Oaxaca. (2025). Extorsión, principal delito cibernético en Oaxaca. <https://imparcialoaxaca.mx/oaxaca/extorsion-principal-delito-cibernetico-en-oaxaca/>

¹³ GPS Noticias Oaxaca. (2025). Policía Cibernética de Oaxaca evitó pérdidas económicas por más de 293 mil pesos en una semana. <https://gpsnoticias.com.mx/2025/09/14/policia-cibernetica-de-oaxaca-evito-perdidas-economicas-por-mas-de-293-mil-pesos-en-una-semana/>

¹⁴ Noticias Voz e Imagen de Oaxaca. (2025). Valles Centrales, foco rojo de ciberdelitos en Oaxaca. <https://nvinoticias.com/roja/delitos/valles-centrales-foco-rojo-de-ciberdelitos/180761>

"2026, AÑO DEL BICENTENARIO DEL NATALICIO DE MARGARITA MAZA PARADA, EJEMPLO DE DIGNIDAD, LEALTAD Y SERVICIO A LA NACIÓN"

Los delitos más frecuentes fueron:

- **Fraude informático**
- Cobranza ilegal
- Suplantación de identidad
- Extorsión ¹⁵

10

Resumen de cifras recientes (2025–enero 2026) — Tecnologías y delitos en Oaxaca¹⁶

Periodo	Indicador principal	Datos
Ene–Jul 2025	Pérdidas evitadas por ciberdelitos	\$17 382 866 pesos prevenidos
Dic 20–26, 2025	Casos atendidos	160 acciones (112 reportes, 45 denuncias)
Ene 10–23, 2026	Acciones de prevención/investigación	406 acciones
Sep 30–Sep 5, 2025	Reportes semanales y pérdidas evitadas	90 reportes \$293 280 pesos prevenidos
Dic 2025	Regiones con más ciberdelitos	Valles Centrales: 38 casos/semana

Además, en 2024 el **mercado de ventas en línea en México** alcanzó un valor de 789,700 millones de pesos, lo que representa un crecimiento del 20% en comparación con el año anterior según datos de la Asociación Mexicana de Ventas Online (AMVO).¹⁷

Esto ubica a México en el **top 15 de los países con mayor contribución** del canal online a las ventas retail o comercio minorista, al representar el 15.8% de las ventas totales del comercio al por menor, superando a Polonia, Japón, Argentina, pero debajo de Estados Unidos. Más **67.2 millones de mexicanos** compararon algún producto o servicio en línea durante el 2024, y el 69% fue por medio de dispositivos móviles. Las principales razones de comprar en línea son: comodidad y facilidad, de acuerdo con la AMVO.

Las temporalidades clave, como el Hot Sale y El Buen Fin, contribuyeron significativamente al aumento del índice de ventas a lo largo del año, junto con Semana Santa y las festividades de diciembre.

El estudio de venta online 2025, de la AMVO destaca que la penetración de compradores digitales en México fue de **84%**, superior a la de mercados como India (63%) y al promedio global (60%).

¹⁵ Policía Cibernética Oaxaca. (2026). *Acciones realizadas del 10 al 23 de enero de 2026 por la Unidad de Policía Cibernética*. Facebook. <https://www.facebook.com/policiacibernetica0axaca/>

¹⁶ NVINoticias Oaxaca. (2025). *Extorsión, el ciberdelito más denunciado en Oaxaca*. <https://nvinoticias.com/oaxaca/general/extorsion-ciberdelito-mas-denunciado-en-oaxaca-policia-cibernetica/164507>

¹⁷ Comercio electrónico en México: La guía más completa del mercado, 2025, disponible en [https://enviame.io/comercio-electronico-en-mexico/#:~:text=Top%2010%20e-commerce%20en%20M%C3%A9xico%202025%20,millones\)%20%20Palacio%20de%20Hierro%20\(5.1%20millones\)](https://enviame.io/comercio-electronico-en-mexico/#:~:text=Top%2010%20e-commerce%20en%20M%C3%A9xico%202025%20,millones)%20%20Palacio%20de%20Hierro%20(5.1%20millones))

Además, América Latina es la segunda región de más rápido crecimiento, por encima de Norteamérica, Asia y Europa.¹⁸

Las regiones donde más compran online, se encuentra CDMX y zona Metropolitana del Valle de México con el 29%, mientras que la zona 3 Occidente representa el 18%, y la zona 6 Sureste abarca el 17%. Más de **67.2 millones de mexicanos** compararon algún producto o servicio en línea durante el 2024, y el 69% fue por medio de dispositivos móviles. Las principales razones de comprar en línea son: comodidad y facilidad, de acuerdo con la AMVO. Además, se mantiene un comprador mixto, debido a que el 49% son hombres y el 51% mujeres y la **edad promedio es de 37 años**, con un predominio en la Ciudad de México y zona metropolitana.

De acuerdo con Daniela Orozco, directora de estudios de mercado e inteligencia de negocios de la AMVO, la velocidad de crecimiento se ha mantenido a doble dígito por seis años consecutivos. El método de pago preferido es con **tarjeta de débito para el 75%** de los consumidores, seguido de crédito (49%) y está ganando terreno el pago en efectivo en cadenas comerciales (26%).

Dado que las transacciones comerciales se realizan en línea, existe un alto riesgo de fraude. Algunos consumidores prefieren interactuar con un vendedor en persona para hacer preguntas y obtener más información sobre un producto. Esto no es posible con el **comercio electrónico**, ya que las transacciones se hacen totalmente a través de **internet**.

Esto puede afectar negativamente la experiencia de compra y la fidelización del cliente. Puede haber problemas con la entrega: las empresas de comercio electrónico tienen que confiar en los servicios de entrega para hacer llegar los productos a sus clientes. A veces esto puede ser poco fiable, especialmente si la empresa utiliza un servicio de entrega de terceros. También existe el riesgo de daños o robos durante el envío, lo que aumenta los costos de envío. Gastos de envío y espera del producto: algunos consumidores no están dispuestos a esperar a que se les envíe un producto. También los puede desanimar el costo del envío, que puede ser caro, sobre todo si se trata de artículos grandes o pesados.

Esto representa una de las principales desventajas del **e-commerce** frente a una tienda física, donde se puede obtener el producto inmediatamente. Imposibilidad de ver el producto antes de comprarlo: la principal razón por la que no se puede ver el producto antes de comprarlo en el modo de comercio electrónico es el costo y el tiempo asociados al envío de productos físicos. A una empresa le resultaría muy caro y le llevaría mucho tiempo enviar cada producto a cada cliente que quisiera verlo antes de comprarlo, por lo que la mayoría de las empresas optan por no ofrecer esta opción. Esta limitación también pone en desventaja al comercio electrónico frente al comercio tradicional. Las devoluciones pueden ser difíciles: las devoluciones pueden ser difíciles porque el cliente no puede ver o tocar el

¹⁸El economista, Comercio electrónico en México creció 20% en 2024, alcanzó un valor de 789,000 millones de pesos, 2025, disponible en el siguiente lin: <https://www.eleconomista.com.mx/el-empresario/comercio-electronico-mexico-crecio-20-2024-alcanzo-valor-789-000-millones-pesos-20250312-750213.html#:~:text=El%20valor%20del%20comercio%20electr%C3%B3nico,de%20Norteam%C3%A9rica%2C%20Asia%20y%20Europa.&text=Esto%20cooca%20a%20M%C3%A9xico%20en,de%20las%20formas%20de%20pago.>

producto antes de comprarlo. Esto puede llevar a que los clientes pidan productos con los que no estén contentos al recibirlos. Para evitarlo, muchas empresas tienen políticas de devolución estrictas que los clientes deben cumplir, lo que puede generar una mala experiencia de compra.¹⁹

En ese sentido, resulta indispensable que se incorpore al Código Penal del estado de Oaxaca como una agravante en el delito de fraude cuando para su comisión se empleen redes sociales, al tratarse de una medida necesaria, proporcional y acorde con la realidad tecnológica actual, ya que estas herramientas cuando son utilizadas con fines ilícitos, potencian la capacidad control y ejecución del delito, reducen el riesgo para el agresor y colocan a la víctima en una situación de mayor indefensión, lo que incrementa de manera significativa el daño social.

QUINTO. En virtud de todo lo anteriormente expuesto y fundado, respecto a la aplicación de las penas y medidas de seguridad, la Suprema Corte de Justicia de la Nación (SCJN) establece que la imposición de sanciones y responsabilidad penal debe basarse en la legalidad, tipicidad y proporcionalidad, diferenciando claramente las sanciones administrativas de las penales.

Bajo este parámetro, se propone incorporar como agravante del delito de fraude tipificado en nuestra legislación penal estatal, el uso de las tecnologías de la información y comunicación, medios digitales o dispositivos electrónicos en su comisión, incrementándose en una mitad las penas correspondientes conforme al valor de lo defraudado, ya que como lo refiere el tipo penal genérico depende del valor de lo defraudado la imposición de la pena.

Cabe señalar que se propone que se consideren tanto las Tecnologías de la Información y la Comunicación (TIC) como los medios digitales, ya que las TIC son el conjunto de herramientas, hardware y software (internet, computadoras, redes) que permiten procesar, almacenar y transmitir información y los medios digitales son los canales y plataformas (redes sociales, sitios web, blogs) que utilizan esas tecnologías para comunicar, interactuar y difundir contenidos específicos, por ende, se propone considerar ambos, así como los dispositivos electrónicos que son los equipos que utilizan energía eléctrica para procesar, gestionar y transmitir información mediante componentes activos como semiconductores, transistores y circuitos integrados (Teléfonos móviles, computadoras, televisores inteligentes, consolas de videojuegos, cámaras digitales, y sistemas de sonido).

Por lo que, incorporar esta conducta a nuestra legislación penal, permitiría: Proteger la vida privada y la tranquilidad de las personas; dar certeza jurídica tanto a la ciudadanía como a la autoridad y atender el problema desde la prevención y la convivencia, no sólo desde la sanción.

¹⁹ Indeed, *Ventajas y desventajas del e-commerce, 2025*, disponible en <https://mx.indeed.com/orientacion-profesional/como-encontrar-empleo/ventajas-desventajas-e-commerce>

Además, se trata de una regulación flexible que puede adaptarse al contexto de Oaxaca y a las capacidades reales de las autoridades locales. Aunado a que, la tipificación del uso de las redes sociales y los medios digitales en la comisión del delito de fraude no busca prohibir la tecnología, sino establecer límites claros para que su uso no afecte derechos fundamentales. Contar con reglas sencillas, comprensibles y aplicables permitiría prevenir conflictos y responder de manera adecuada a una realidad tecnológica que ya está presente en la vida cotidiana de la población.

Bajo ese contexto, vengo a presentar una iniciativa con proyecto de decreto por la cual se propone adicionar un artículo a nuestro Código Penal del estado Libre y Soberano de Oaxaca para considerar como agravante el uso de las redes sociales y los medios digitales en la comisión del delito de fraude, ya que con ello, permitirá cerrar vacíos normativos, fortalecer la función preventiva del derecho penal y dotar a las autoridades de un instrumento jurídico eficaz para inhibir el uso de tecnologías emergentes con fines delictivos. Asimismo, la medida se alinea con los principios de seguridad pública, protección de la privacidad y tutela reforzada de los derechos humanos, especialmente de niñas, niños, adolescentes y otros grupos en situación de vulnerabilidad, contribuyendo a un marco normativo moderno, coherente y sensible a los nuevos riesgos que enfrenta la sociedad oaxaqueña.

En virtud de lo anteriormente expuesto y fundado, propongo la siguiente iniciativa de reformas y adiciones al Código Penal para el Estado Libre y Soberano de Oaxaca, para lo cual se formula el siguiente cuadro comparativo:

TEXTO VIGENTE DEL CÓDIGO PENAL DEL ESTADO	TEXTO QUE PROPONE LA DIPUTADA HAYDEÉ REYES SOTO AL CÓDIGO PENAL
ARTÍCULO 382.- Se impondrá prisión de seis meses a ocho años y multa de cinco mil a diez mil pesos, o sólo la prisión al que, para hacerse de una cantidad de dinero en numerario, en papel moneda o billetes de banco, de un documento que importa obligación, liberación o transmisión de derechos o de cualquiera otra cosa ajena mueble, logre que se le entregue por medio de maquinaciones, engaños o artificios.	ARTÍCULO 382.- Se impondrá prisión de seis meses a ocho años y multa de cinco mil a diez mil pesos, o sólo la prisión al que, para hacerse de una cantidad de dinero en numerario, en papel moneda o billetes de banco, de un documento que importa obligación, liberación o transmisión de derechos o de cualquiera otra cosa ajena mueble, logre que se le entregue por medio de maquinaciones, engaños o artificios.
SIN CORRELATIVO	ARTÍCULO 382 BIS.- Cuando para la comisión del delito de fraude sean utilizadas las tecnologías de la información y comunicación, medios digitales o dispositivos electrónicos, las penas correspondientes conforme al valor de lo defraudado se aumentarán en una mitad.

Debido a los motivos anteriormente expuestos y con fundamento en los artículos 50, fracción I y 59 fracción XXXIX de la Constitución Política del Estado Libre y Soberano de Oaxaca; 30, fracción I y 104, fracción I de la Ley Orgánica del Poder Legislativo del Estado de Oaxaca; 3 fracción XVIII y 54

"2026, AÑO DEL BICENTENARIO DEL NATALICIO DE MARGARITA MAZA PARADA, EJEMPLO DE DIGNIDAD, LEALTAD Y SERVICIO A LA NACIÓN"

fracción I, del Reglamento Interior del Congreso del Estado, vengo a someter a consideración del Pleno de esta LXVI Legislatura del H. Congreso del Estado, el siguiente proyecto de:

DECRETO

ARTÍCULO ÚNICO. Se adiciona el artículo 382 Bis al Código Penal para el Estado Libre y Soberano de Oaxaca, para quedar como sigue:

ARTÍCULO 382 BIS.- Cuando para la comisión del delito de fraude sean utilizadas las tecnologías de la información y comunicación, medios digitales o dispositivos electrónicos, las penas correspondientes conforme al valor de lo defraudado se aumentarán en una mitad.

ARTÍCULOS TRANSITORIOS

PRIMERO: Publíquese el presente decreto en el Periódico Oficial del Gobierno del Estado Libre y Soberano de Oaxaca.

SEGUNDO: El presente decreto entrará en vigor al día siguiente de su publicación en el Periódico Oficial del Gobierno del Estado Libre y Soberano de Oaxaca.

ATENTAMENTE
"EL RESPETO AL DERECHO DE LOS ES LA PAZ"

DIPUTADA HAYDEÉ IRMA REYES SOTO
San Raymundo Jalpan, Oaxaca; a 17 de febrero de 2026.



GOBIERNO CONSTITUCIONAL
DEL ESTADO DE OAXACA
PODER LEGISLATIVO

LXVI LEGISLATURA
H. DIPUTADA HAYDEÉ IRMA REYES SOTO
OAXACA DE JUÁREZ
DISTRITO 13