CONSEJO CIUDADANO
DE SEGURIDAD

“Ciberdelitos”

Ejercicio Consultivo



Contenido

1. GLOSARIO 3
2. PROPUESTA Y JUSTIFICACIÓN DEL TEMA 4
3. PLANEACIÓN ESTRATÉGICA 6
   a. Facultades del Consejo Ciudadano de Seguridad 6
   b. Programa Anual de Trabajo 2025 6
4. APARTADOS Y CONTENIDOS TEMÁTICOS 7
   4.1 Introducción 7
   4.2 Objetivos 9
   4.3 Alcances y limitaciones 10
5. MARCO NORMATIVO 11
   5.1 Internacional 11
   5.2 Nacional 13
   5.3 Estatal 14
6. METODOLOGÍA 15
   a. Fuentes y técnicas utilizadas: 15
7. INTERPRETACIÓN DE LOS DATOS OBTENIDOS EN EL ANÁLISIS 17
   7.1 Mesas de Trabajo 2025 sobre Ciberdelitos y Violencia Digital en Jalisco 24
   7.2 Buenas Prácticas Internacionales: 27
8. POSIBLES EFECTOS DE LAS CIRCUNSTANCIAS Y ESCENARIOS 30
   8.1 Contexto a nivel internacional 30
   8.2 Contexto a nivel nacional 31
   8.3 Contexto a nivel estatal 31
   8.4 Causas del problema 33
   8.5 Causas estructurales 34
   8.6 Posibles efectos por grupos etarios vulnerables 35
9. ÁRBOL DE PROBLEMAS 37
10. CONCLUSIONES Y RECOMENDACIONES 38
   10.1 Conclusiones 38
   10.2 Recomendaciones 39
   10.3 Hallazgos 42
11. RESULTADOS Y ACCIONES ESPERADAS 43
   11.1 Corto plazo 43
   11.2 Mediano plazo 44
   11.3 Largo Plazo 45
12. REFERENCIAS BIBLIOGRÁFICAS 47

1. GLOSARIO

Término / Sigla	Definición
Alfabetización digital	Conjunto de conocimientos y habilidades para usar tecnologías digitales de manera segura y eficiente.
Ataque de denegación de servicio (DoS/DDoS)	Estrategia que busca saturar un sistema o servicio para interrumpir su funcionamiento.
Big Data	Análisis de grandes volúmenes de datos para identificar patrones, tendencias o conductas anómalas.
Ciberdelito	Actividad ilícita realizada mediante medios digitales o sistemas informáticos.
Ciberseguridad	Conjunto de medidas destinadas a proteger redes, dispositivos y datos frente a ataques o accesos no autorizados.
Deepfake	Contenido audiovisual manipulado con IA para falsificar identidades o difundir información engañosa.
Denuncia anónima	Mecanismo para reportar ciberdelitos sin revelar la identidad del denunciante.
Educación digital	Procesos de enseñanza orientados al uso seguro y responsable de herramientas tecnológicas.
Extorsión digital	Amenaza realizada mediante entornos digitales con el objetivo de obtener dinero o beneficios indebidos.
Factor de riesgo	Circunstancia que aumenta la probabilidad de que se cometa un ciberdelito.
Firewall	Sistema que controla el tráfico de red para bloquear accesos no autorizados.
Fraude electrónico	Obtención indebida de dinero o información mediante engaños digitales.
Hashing	Técnica criptográfica que transforma información en una cadena de caracteres irreversibles para proteger datos.
Inteligencia Artificial (IA)	Tecnología que simula procesos de inteligencia humana para análisis y automatización.
IP (Internet Protocol)	Dirección única que identifica un dispositivo en una red.
Malware	Programa malicioso diseñado para dañar, robar o comprometer sistemas informáticos.
MFA (Multi-Factor Authentication)	Sistema de autenticación que utiliza más de un método de verificación para acceder a un

	servicio.
Phishing	Técnica fraudulenta que busca obtener datos personales simulando ser una entidad confiable.
Política pública	Conjunto de acciones gubernamentales para atender problemas sociales, como la ciberseguridad.
Protección de datos personales	Conjunto de medidas para evitar el uso indebido de información personal (imagen,voz y datos).
Ransomware	Software malicioso que bloquea archivos o sistemas a cambio de un rescate económico.
Redes sociales	Plataformas digitales para interacción social que pueden ser usadas para fraudes o engaños.
Spam	Envío masivo de mensajes no solicitados con fines comerciales o maliciosos.
Suplantación de identidad	Uso indebido de datos personales para hacerse pasar por otra persona.
Vulnerabilidad	Debilidad en un sistema que puede ser explotada por un ciberdelincuente.

2. PROPUESTA Y JUSTIFICACIÓN DEL TEMA

Entre las facultades que le otorga al Consejo Ciudadano de Seguridad, la Ley del Sistema de Seguridad Pública para el Estado de Jalisco, se encuentran la de emitir opiniones respecto al sistema de seguridad pública, así como realizar los estudios relacionados con la situación estatal y, en su caso, municipal, en el área de la protección ciudadana, así como analizar la problemática en las zonas con mayor índice de delincuencia para proponer los objetivos y políticas para su adecuada solución.

De conformidad con el Programa de Trabajo 2025 del Consejo Ciudadano de Seguridad, en seguimiento a las actividades allí mencionadas, se llevará a cabo el siguiente documento, que aborda el tema de “ciberdelitos”.

La elección del tema obedece a la necesidad de comprender y enfrentar un fenómeno delictivo en constante evolución que impacta de forma transversal a la ciudadanía, empresas, instituciones educativas y organismos gubernamentales. En un contexto donde la

digitalización de la vida cotidiana es irreversible, los ciberdelitos representan un desafío urgente para la seguridad pública, la protección de datos personales y la confianza en las tecnologías de la información.

Este ejercicio consultivo se justifica por su potencial para generar insumos relevantes que contribuyan a la formulación de políticas públicas integrales, el diseño de estrategias preventivas basadas en evidencia y el fortalecimiento de las capacidades institucionales en materia de ciberseguridad. Asimismo, busca fomentar una cultura de prevención, denuncia y resiliencia digital en el Estado de Jalisco, mediante el análisis sistemático de datos, normativas y actores clave involucrados en la dinámica de los ciberdelitos.

Su pertinencia radica en la posibilidad de ofrecer un panorama claro, documentado y propositivo que sirva de base para la toma de decisiones en los ámbitos legislativo, ejecutivo, educativo y social. En este sentido, el estudio se convierte en una herramienta estratégica que permite enfrentar con eficiencia los desafíos que impone la criminalidad digital, con un enfoque multidisciplinario y prospectivo que favorezca la prevención del delito, la justicia digital y la cohesión institucional frente a riesgos emergentes.

En el contexto actual, el avance tecnológico ha generado una amplia gama de oportunidades en diversos sectores, pero también ha dado lugar a nuevas formas de criminalidad, entre ellas, los ciberdelitos. Estos delitos, que incluyen fraudes electrónicos, robo de identidad, acoso cibernético, extorsión en línea, y ataques a sistemas informáticos, entre otros, son fenómenos que afectan tanto a personas físicas como morales, y cuya expansión es cada vez más preocupante a nivel global y, particularmente, en México.

México ha experimentado un incremento en la incidencia de ciberdelitos en los últimos años, convirtiéndose en una de las principales preocupaciones en materia de seguridad pública. En este contexto, el Estado de Jalisco no ha sido ajeno a esta tendencia, destacándose como uno de los estados con mayores tasas de incidencia de estos delitos en el país. De acuerdo a datos proporcionados por la Fiscalía del Estado de Jalisco se tiene que, del 2020 al 2024 se tuvo

un incremento de reportes de más del 96.4%, lo que justifica la necesidad de un ejercicio consultivo preciso y detallado sobre la situación actual.

El uso de la Inteligencia Artificial (IA) en la prevención, detección y resolución de ciberdelitos es una tendencia que ha venido tomando relevancia. La intersección de estos delitos con la Inteligencia Artificial, no solo influye en la perspectiva de los criminales que pueden utilizarla para cometer delitos, sino también en su aplicación para la detección y prevención de los mismos. Según datos reportados por la Fiscalía del Estado de Jalisco, los tipos más frecuente de ciberdelitos reportados, son: el fraude financiero representando el 35% de los casos, seguido por el robo de identidad con un 25% y otros delitos como extorsión digital, acceso no autorizado a sistemas y ataques de malware representan el 40% restante.

Por esta razón, el uso estratégico de IA orientado a la prevención permite no solo anticipar ataques y reducir vulnerabilidades, sino también fomentar una educación digital más segura y resiliente frente al constante avance de las amenazas cibernéticas.

3. PLANEACIÓN ESTRATÉGICA

a. Facultades del Consejo Ciudadano de Seguridad

Como órgano de análisis, opinión y consulta, y derivado de sus facultades de emitir opiniones en materia de prevención, investigación y persecución del delito; así como de proponer normas y procedimientos a las instituciones de seguridad y procuración de justicia, este órgano de representación ciudadana se enfocará en el análisis situacional de los ciberdelitos en el estado de Jalisco para promover una mayor sensibilización y prevención. (Seguridad, Consejo Ciudadano de Seguridad, 2025)

b. Programa Anual de Trabajo 2025

Entre las facultades del Consejo Ciudadano de Seguridad, se encuentra la fracción I artículo 220 de la Ley del Sistema de Seguridad del Estado de Jalisco: “Emitir opiniones respecto al sistema de seguridad pública, así como en materia de prevención investigación y persecución del delito”.

(Seguridad, Consejo Ciudadano de Seguridad, 2025). Con base en este fundamento, el Consejo estableció como objetivo la elaboración de tres ejercicios consultivos a lo largo del año, centrados en las siguientes temáticas:

- Tema 1: “Ciberdelitos”
- Tema 2: “Evolución de la Violencia Digital en Adolescentes y el camino a seguir por las autoridades en Jalisco”
- Tema 3: “Prevención de la Violencia Familiar en el Área Metropolitana de Guadalajara”

A través de ellos, el Consejo Ciudadano emite recomendaciones en los temas abordados y propuestas tendentes a atender o solucionar las problemáticas identificadas. (Seguridad, Plan Estatal Jalisco, s.f.)

4. APARTADOS Y CONTENIDOS TEMÁTICOS

4.1 Introducción

El crecimiento exponencial de las tecnologías de la información y comunicación ha transformado profundamente la vida social, económica y política. En el Estado de Jalisco, el aumento de estas conductas delictivas representa un reto para las autoridades, instituciones educativas y sociedad en general. Este ejercicio consultivo tiene como objetivo identificar las principales problemáticas relacionadas con los ciberdelitos en la entidad, así como los actores involucrados y las estrategias posibles para su prevención y control. La transformación digital exige, por tanto, una respuesta institucional y social que reconozca la complejidad del ciberespacio como nuevo campo de batalla para el crimen.

La revolución digital ha reconfigurado de manera vertiginosa las dinámicas sociales, económicas y políticas, dando lugar a nuevos escenarios de interacción tanto a nivel personal como institucional. Las tecnologías de la información y comunicación (TIC) han permitido la conectividad global y el intercambio instantáneo de información, facilitando el acceso al conocimiento y el desarrollo de nuevas oportunidades. Sin embargo, este avance tecnológico también ha dado paso a la proliferación de actividades ilícitas en el ciberespacio, originando un fenómeno creciente: los ciberdelitos. Estos delitos abarcan una variedad de actos

criminales, desde el fraude cibernético y el robo de identidad, hasta los ataques informáticos que buscan dañar sistemas críticos, como servicios bancarios, sanitarios o gubernamentales.

En México, la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2023 reveló que el 92.4 % de los hogares en zonas urbanas cuentan con conexión a internet, lo que ha intensificado la exposición a riesgos cibernéticos. Los delitos cibernéticos son cada vez más comunes en Jalisco y representan una amenaza diaria. Compartir datos personales en redes sociales, plataformas digitales o aplicaciones sin revisar puede derivar en suplantación, extorsión o incluso en la exposición de información íntima sin consentimiento. (Nuño, 2025)

El Estado de Jalisco no ha sido ajeno a este fenómeno global, los ciberdelitos han experimentado un incremento notable en los últimos años. Aunque estos delitos afectan a todos los estados de la República Mexicana, Jalisco presenta características particulares que lo convierten en un foco de atención para los expertos en seguridad digital. Factores como el crecimiento acelerado de la digitalización en la región, la expansión de servicios bancarios y comerciales en línea, y la alta penetración de tecnologías móviles en la vida cotidiana de los ciudadanos, han generado un ecosistema propicio para la acción de los ciberdelincuentes. Sin embargo, también existen retos estructurales en la capacidad de respuesta de las autoridades y en la formación de la población en temas de ciberseguridad.

Es fundamental abordar este fenómeno no solo desde una perspectiva tecnológica, sino también desde un enfoque multidisciplinario que considere las dimensiones jurídicas, sociales, psicológicas y económicas del problema. Para ello, se requiere de un ejercicio consultivo preciso que permita identificar las causas subyacentes que propician la proliferación de los ciberdelitos, los actores involucrados, los sectores más vulnerables y las consecuencias que este fenómeno genera tanto a nivel individual como colectivo.

El objetivo principal de este trabajo es llevar a cabo un ejercicio consultivo sobre la incidencia de ciberdelitos en el estado de Jalisco. Para identificar cuáles son las principales problemáticas relacionadas con estos delitos, reconocer las áreas que presentan mayor

vulnerabilidad y comprender las causas que propician su comisión. Además, es importante detectar quiénes son los actores involucrados en este fenómeno, tanto desde el ámbito delictivo como institucional. Todo esto con el propósito de generar información que nos permita aportar elementos sólidos para el diseño de estrategias efectivas en el ámbito estatal, orientadas a la prevención, atención y reducción de los ciberdelitos

Además, se explorarán los factores sociales y estructurales que facilitan la comisión de estos delitos, como la brecha digital existente entre diversos sectores de la población, la falta de educación en ciberseguridad y los vacíos en la legislación vigente. Con ello, se busca una comprensión profunda y contextualizada de los ciberdelitos en Jalisco, orientada a la formulación de políticas públicas y estrategias de prevención e intervención.
El crecimiento de las tecnologías digitales ha modificado no solo el comportamiento humano, sino también las estructuras de poder, dejando al ciberespacio como un terreno nuevo en el que se deben redefinir las normas sociales, legales y éticas.

Este estudio no solo se limita a ofrecer una descripción de la situación actual, sino que también busca contribuir con recomendaciones estratégicas para mejorar la respuesta ante los ciberdelitos, tanto a nivel gubernamental como en el sector privado y en la sociedad civil.

La creciente incidencia de los ciberdelitos exige una respuesta integral, coherente y proactiva, que no solo se limite a la persecución de los delincuentes, sino que también impulse la educación y concientización de los ciudadanos y el fortalecimiento institucional. Solo de esta manera se podrá generar un entorno digital más seguro, donde la tecnología sea una herramienta de desarrollo y no una amenaza constante. (INEGI, Estudio sobre los hábitos de usuarios de Internet en México 2024 y Perspectiva de la IA, s.f.).

4.2 Objetivos

Objetivo General:

Realizar un ejercicio consultivo sobre la incidencia de ciberdelitos en el Estado de Jalisco, con el fin de identificar las principales problemáticas, las áreas de vulnerabilidad, las causas

que propician la comisión de estos delitos y los actores involucrados, para aportar elementos para el diseño de estrategias en el ámbito estatal.

Objetivos Específicos:

1. Se enuncia marco normativo vigente a nivel internacional, nacional y estatal.
2. Recabar e interpretar datos estadísticos sobre la incidencia de ciberdelitos en Jalisco.
3. Identificar causas estructurales y actores relevantes en la comisión de ciberdelitos.
4. Proponer estrategias de prevención.
5. Fomentar la participación ciudadana en la cultura de la denuncia y ciberseguridad.
6. Evaluar la efectividad de las políticas de ciberseguridad y propuestas de acción estatal.

4.3 Alcances y limitaciones

Este documento se enfoca en el análisis de la ciberdelincuencia en el Estado de Jalisco entre los años 2020 y 2024. Incluye revisión documental, análisis estadístico, entrevistas con actores clave, y revisión normativa en tres niveles (internacional, nacional y estatal). (INAI, s.f.) El documento también plantea propuestas de mejora específicas para fortalecer la capacidad de prevención, atención e investigación de los delitos informáticos en la entidad. (AMECI, 2023).

En cuanto a limitaciones podemos enumerar las siguientes:

- El subregistro de ciberdelitos debido a la baja cultura de denuncia afecta la precisión de las estadísticas.
- No toda la información está desagregada por municipio o tipo de delito.
- La naturaleza cambiante de los métodos delictivos en el entorno digital limita la vigencia del análisis a mediano plazo.
- Algunas dependencias estatales y federales no cuentan con sistemas de datos abiertos sobre incidentes cibernéticos.

5. MARCO NORMATIVO

El marco normativo relacionado con los ciberdelitos es fundamental para comprender las medidas legales que regulan y sancionan las conductas ilícitas en el ciberespacio. A medida que los ciberdelitos se diversifican y se sofistican, el marco jurídico también debe evolucionar para abordar estos nuevos desafíos. Este apartado está dividido en tres secciones: el marco normativo internacional, nacional y estatal, con el objetivo de ofrecer una visión integral sobre las leyes que regulan el uso de las tecnologías de la información y la comunicación (TIC) y la persecución de los ciberdelitos.

5.1 Internacional

A nivel internacional, la regulación de los ciberdelitos ha sido un desafío debido a la naturaleza transnacional de los mismos. La globalización de las tecnologías ha generado un espacio donde las leyes de un país no siempre son suficientes para abordar los delitos cometidos a través de internet. Sin embargo, existen tratados, convenciones, recomendaciones y acuerdos internacionales que promueven la cooperación entre Estados y que buscan establecer un marco común para la cooperación entre países en la lucha contra los ciberdelitos.

Convención sobre Ciberdelincuencia del Consejo de Europa (Convención de Budapest)
Primer tratado internacional que busca armonizar legislaciones nacionales y establecer mecanismos de cooperación internacional para combatir los delitos informáticos. La Convención de Budapest es uno de los principales acuerdos internacionales que aborda los ciberdelitos. Adoptada en 2001, establece normas legales y procesos de cooperación entre países para combatir el crimen en línea. Esta convención fue diseñada para proporcionar un marco legal común que permita a los países cooperar en la persecución de ciberdelitos transnacionales, y regula delitos como la accesibilidad no autorizada a sistemas informáticos, la interceptación ilegal de comunicaciones y la producción y distribución de material ilícito en línea.

Actualmente más de 60 países son miembros del ***Convenio de Budapest***, Aunque México no es parte firmante, se encuentra como observador y ha adoptado varias de sus recomendaciones en su marco jurídico interno, pero no se ha adherido. (OAS, 2001)

Directiva de la Unión Europea sobre Ciberseguridad (Directiva NIS)

La Directiva de Seguridad de Redes y Sistemas de Información (NIS, por sus siglas en inglés) fue adoptada por la Unión Europea en 2016 y es uno de los principales esfuerzos para fortalecer la ciberseguridad dentro del bloque europeo. Aunque está dirigida principalmente a la protección de infraestructuras críticas y a la mejora de la seguridad de redes y sistemas informáticos, también establece un marco para la cooperación en la prevención y respuesta a incidentes cibernéticos. Aunque esta directiva no es directamente aplicable a México, su modelo ha influido en la legislación de muchos países, incluyendo aquellos en América Latina, como un modelo de buenas prácticas en la ciberseguridad. (NIS, 2016)

Convenio de la ONU contra el Crimen Organizado Transnacional

La Asamblea General de las Naciones Unidas aprobó en 2000 el Convenio de las Naciones Unidas contra la Delincuencia Organizada Transnacional, también conocido como la Convención de Palermo. Aunque no se enfoca exclusivamente en ciberdelitos, este tratado establece principios para la cooperación internacional en la lucha contra el crimen organizado, que a menudo emplea ciberespacio para actividades ilícitas como el tráfico de personas, el narcotráfico, y el lavado de dinero. La cooperación internacional en los ciberdelitos, especialmente cuando están vinculados al crimen organizado, es un principio central de este convenio. (ONU, 2000).

Declaración Universal de los Derechos Humanos (1948):

Garantiza el derecho a la privacidad, la libertad de expresión y el acceso a la información, pilares fundamentales para un uso seguro y libre del entorno digital.

Agenda 2030 para el Desarrollo Sostenible (ONU):

En su Objetivo 16, promueve el acceso a la justicia y el fortalecimiento de las instituciones para reducir todas las formas de violencia, incluyendo la digital.

Reglamento General de Protección de Datos (GDPR) – Unión Europea:

Aunque no tiene aplicación directa en México, ha servido como referencia internacional para legislar sobre el tratamiento de datos personales y la protección de la privacidad digital. (Nader, 2021).

5.2 Nacional

En México, el marco normativo que regula los ciberdelitos ha evolucionado en respuesta a las crecientes amenazas cibernéticas y a la necesidad de mejorar la protección de los derechos de los ciudadanos en el ámbito digital, los ciberdelitos están regulados por un conjunto disperso de normas que abordan tanto los aspectos penales como los derechos digitales. Algunos de los principales instrumentos normativos son:

Constitución Política de los Estados Unidos Mexicanos

Artículo 6°: Reconoce el derecho al acceso al internet y las tecnologías de la información.

Artículo 16°: Garantiza la protección de los datos personales.

Código Penal Federal

El Código Penal Federal de México, en sus reformas recientes, ha incorporado disposiciones relacionadas con los delitos informáticos. Aunque las reformas comenzaron a integrarse en 2007, ha sido en los últimos años cuando las leyes han sido modificadas para hacer frente a la sofisticación de los ciberdelitos. Algunos de los delitos contemplados en el Código Penal son:

- Acceso ilegal a sistemas y redes informáticas.
- Robo de identidad y fraude cibernético.
- Difusión de virus informáticos y malware.
- Suplantación de identidad en plataformas digitales.

Se han agregado artículos (como el 211 bis 1 al 211 bis 7) que definen y sancionan diversas conductas delictivas relacionadas con el uso de tecnologías de la información. Las reformas

a este código buscan garantizar que las sanciones sean proporcionales a la gravedad del ciberdelito y que las víctimas puedan obtener justicia. (Dr. Caritino Morales, s.f.)

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

La Ley General de Protección de Datos Personales, promulgada en 2010, establece principios para la protección de datos personales en el ámbito digital. Esta ley se refiere a la protección de los derechos de los individuos en cuanto a la recolección, almacenamiento y uso de sus datos personales por parte de entidades públicas y privadas, lo cual es crucial en un contexto donde los ciberdelincuentes buscan acceder a estos datos con fines fraudulentos. La Ley establece sanciones para aquellos que violen los derechos de los titulares de los datos personales, fortaleciendo la seguridad cibernética y la confianza de los usuarios en el uso de plataformas digitales. (UNIÓN, LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS , 2025).

Ley Olimpia (Reforma Federal de 2021)

Tipifica la violencia digital y el delito de difusión no consentida de contenido íntimo. Ha sido adoptada por todas las entidades federativas, con sanciones de 3 a 6 años de prisión (dependiendo del daño y difusión). (Olimpia, 2021).

Ley Nacional de Ejecución Penal y Ley Nacional del Sistema Integral de Justicia Penal para Adolescentes:

Incluyen consideraciones sobre el uso de medios digitales en la comisión de delitos y sanciones aplicables. (UNIÓN, LNSIJPA, 2022) (UNIÓN, LNEP, 2024).

5.3 Estatal

A nivel estatal, el marco normativo de Jalisco también ha adoptado diversas iniciativas para combatir los ciberdelitos. Sin embargo, la legislación estatal aún depende en gran medida de las leyes federales, aunque existen leyes locales que promueven la ciberseguridad y la protección de los datos personales.

Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco:

Adapta las disposiciones federales al contexto estatal, garantizando la privacidad digital en la gestión pública. (Congreso, s.f.).

Ley de Acceso a una Vida Libre de Violencia para las Mujeres del Estado de Jalisco:

Reconoce la violencia digital como una forma de agresión y establece obligaciones para su prevención, atención y sanción. (ESTADO, s.f.).

6. METODOLOGÍA

La presente investigación se enmarca dentro de un enfoque cualitativo, documental y participativo, en congruencia con las facultades y atribuciones del Consejo Ciudadano de Seguridad, el cual no cuenta con funciones operativas ni presupuestales, pero sí con la capacidad de incidir, analizar y articular procesos de consulta e interlocución. Esta estrategia permitió obtener una visión integral y multidimensional del fenómeno, integrando tanto datos duros como interpretaciones sociales y estructurales del contexto delictivo digital.

a. Fuentes y técnicas utilizadas:

a) Revisión documental:

Se realizó un análisis exhaustivo de la legislación vigente a nivel internacional, nacional y estatal, incluyendo códigos penales, leyes especializadas y reglamentos municipales. Se recopilaron documentos oficiales, informes institucionales y publicaciones académicas para contextualizar el marco normativo y las políticas públicas relacionadas con la ciberdelincuencia.

b) Solicitud formal de información:

Se recabaron datos estadísticos de fuentes oficiales y confiables, tales como:

- Instituto Nacional de Estadística y Geografía (INEGI), Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH).
- Instituto de Información Estadística y Geográfica de Jalisco (IIEG).
- Se enviaron oficios de solicitud de información a:
    - Fiscalía del Estado de Jalisco;
    - Secretaría de Seguridad Jalisco;
    - Comisaría de Guadalajara
    - Comisaría de Zapopan
    - Comisaría de Tonalá
    - Comisaría de San Pedro Tlaquepaque
    - Comisaría de Tlajomulco de Zúñiga
    - Comisaría de El Salto
    - Comisaría de Juanacatlán
    - Comisaría de Ixtlahuacan de los Membrillos
    - Comisaría de Acatlán de Juárez
- Organismos no gubernamentales y asociaciones especializadas en ciberseguridad.

c) Mesas de trabajo interinstitucionales:

Se llevaron a cabo dos mesas de trabajo en los meses de mayo y julio para la discusión de hallazgos preliminares y fomentar la colaboración interinstitucional con actores clave, incluyendo autoridades de seguridad pública, especialistas en ciberseguridad y tecnología, representantes de organizaciones civiles y académicas.

e) Limitaciones metodológicas

Entre las principales limitaciones encontradas se destacan:

- La cifra negra en los registros oficiales, debido a la baja cultura de denuncia en delitos cibernéticos.
- La rápida evolución tecnológica impone un desafío constante para mantener la vigencia del análisis.

Pese a estas limitaciones, la metodología empleada permite construir un ejercicio consultivo sólido y representativo, con base en la evidencia disponible, que aporte insumos valiosos para la formulación de políticas públicas, estrategias preventivas y mejoras en la coordinación institucional.

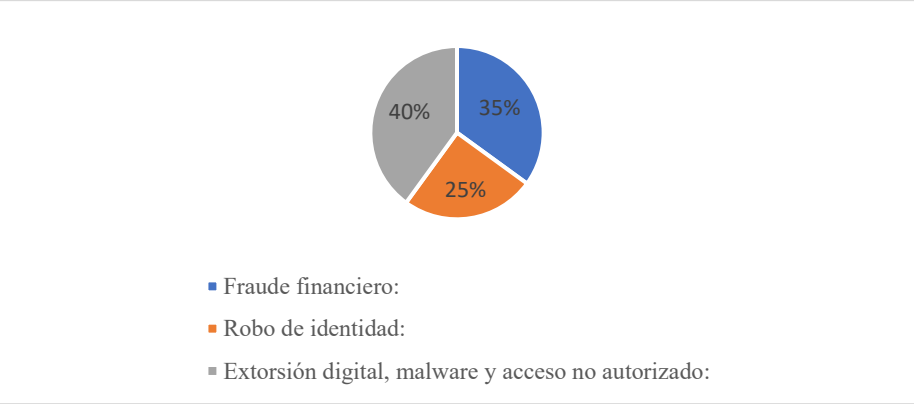
7. INTERPRETACIÓN DE LOS DATOS OBTENIDOS EN EL ANÁLISIS

La interpretación de los datos obtenidos durante la investigación sobre la incidencia de ciberdelitos en el Estado de Jalisco se basa en un enfoque multidimensional que abarca no sólo el análisis numérico y estadístico, sino también un marco contextual que permita comprender las causas subyacentes de estos delitos en el ciberespacio. A través del análisis de las fuentes de información, los patrones observados y la correlación entre los datos, se busca obtener una visión integral de la situación.

Durante el periodo 2020–2024, la incidencia de ciberdelitos en Jalisco ha experimentado un aumento notable, acorde con la creciente digitalización de la vida cotidiana y la expansión del acceso a internet. Datos oficiales del Instituto de Información Estadística y Geográfica de Jalisco (IIEG) muestran que las denuncias relacionadas con delitos informáticos se incrementaron en un 45 % en este lapso, lo que indica una tendencia creciente preocupante.

Este crecimiento está asociado, en parte, a factores externos como la pandemia de COVD-19 que aceleró la adopción de herramientas digitales para trabajo, educación y comercio, exponiendo a un mayor número de personas a riesgos en línea.

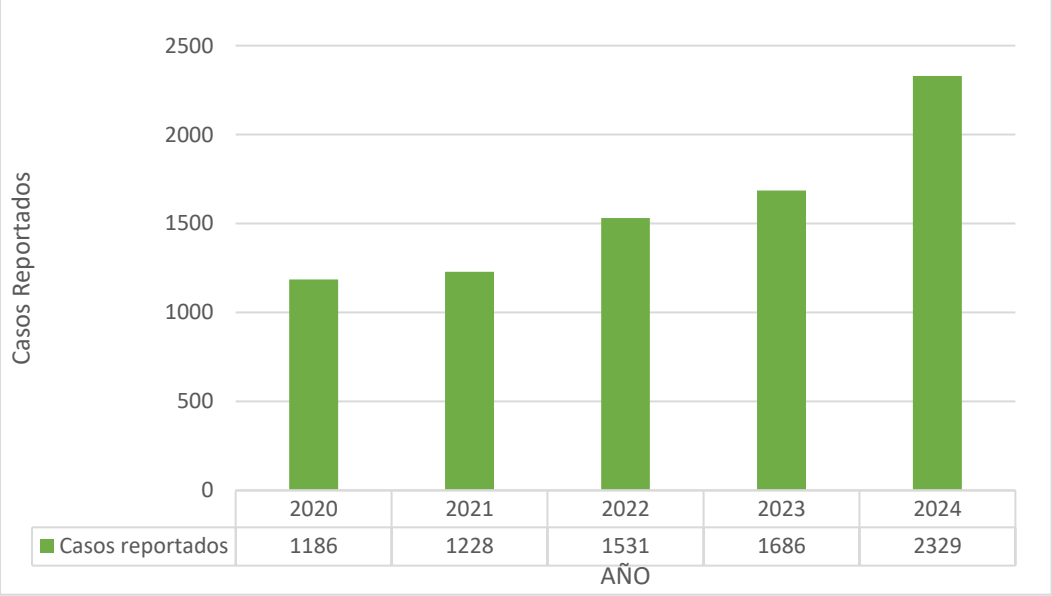
Gráfico 1. Tipos de Ciberdelitos Reportados en Jalisco (2024)



Fuente: Elaboración propia con datos obtenidos mediante investigación y correspondencia oficial

Este gráfico muestra la distribución porcentual de los tipos de ciberdelitos reportados, con el fraude financiero representando el 35% de los casos, seguido por el robo de identidad con un 25%. Otros delitos incluyen extorsión digital, acceso no autorizado a sistemas y ataques de malware, que representan el 40%.

Gráfico 2. Casos reportados de Ciberdelitos en Jalisco (2020–2024)

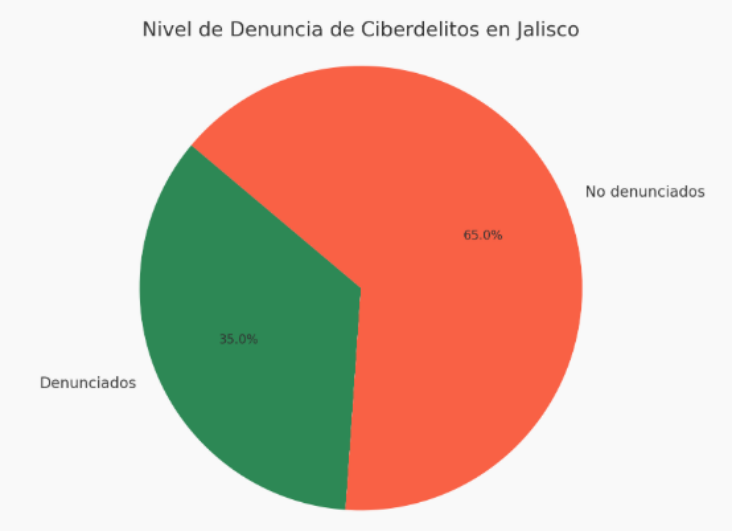


Fuente: Elaboración propia con datos obtenidos mediante investigación y correspondencia oficial

Según datos proporcionados por la Fiscalía del Estado en el oficio FE.10.01/63/2025/DGI/DPE, la evolución temporal revela un crecimiento constante de los ciberdelitos en el estado. En 2020 se reportaron 1186 casos y en 2024 reportan 2329, lo que

representa un incremento de más del 96.4%. Este aumento refleja tanto una mayor incidencia como un posible incremento en la conciencia social para reportar los casos.

Gráfico 3. Nivel de Denuncia de Ciberdelitos en Jalisco



Fuente: Elaboración propia con datos obtenidos mediante investigación y correspondencia oficial

Los ciberdelitos denunciados en el estado representan un porcentaje cada vez mayor de las denuncias totales, aunque aún se percibe una gran disparidad entre los delitos ocurridos y los reportados. Se estima que solo el 35% de los ciberdelitos son efectivamente denunciados, mientras que el 65% restante permanece en la cifra negra, lo cual genera una subestimación de la magnitud real del problema. Esta cifra pone de manifiesto uno de los principales obstáculos para una respuesta efectiva: la falta de confianza en las instituciones y el desconocimiento generalizado sobre cómo proceder ante un ciberdelito.

Dentro de los ciberdelitos más comunes en Jalisco, el Coordinador de Ciberprevención de la Fiscalía de Jalisco, Alejandro Tavera Ramírez, señaló que los ciberdelitos más comunes en el estado son el phishing, el fraude, el ciberacoso y la violación a la intimidad sexual, afectando principalmente a menores de edad y usuarios comunes. (Nuño, 2025)

El robo de identidad sigue de cerca, siendo utilizado por los ciberdelincuentes para realizar transacciones fraudulentas, adquirir créditos a nombre de las víctimas y, en algunos casos, para suplantación en redes sociales con el fin de extorsionar o manipular a otras personas.

Este tipo de delito ha mostrado un crecimiento progresivo en los últimos años, especialmente en el contexto de la creciente digitalización de servicios gubernamentales y privados.

Otro patrón importante es el ciberacoso, que ha afectado a jóvenes en su mayoría. Este delito está vinculado con el uso de redes sociales y plataformas de mensajería instantánea para acosar, difamar o amenazar a las víctimas. Según la Secretaría de Seguridad Pública de Jalisco (2024), alrededor del 25% de los casos de ciberacoso tienen relación con adolescentes que son víctimas de acosos sexuales o psicológicos a través de internet.

Existen múltiples factores que favorecen la proliferación de los ciberdelitos en Jalisco, siendo uno de los más relevantes la brecha en educación digital, la falta de conocimientos básicos sobre ciberseguridad, tanto en la población general como en las pequeñas y medianas empresas, crea amplias oportunidades para los ciberdelincuentes. La incapacidad de los usuarios para identificar correos electrónicos de phishing, contraseñas débiles y la falta de medidas preventivas son factores que contribuyen a un aumento de los delitos cibernéticos.

Además, la escasez de recursos destinados a la ciberseguridad y la falta de capacitación de los funcionarios encargados de investigar estos delitos también son factores que han contribuido al desbordamiento de la situación, muchos de los cuerpos de seguridad en Jalisco carecen de formación especializada en delitos informáticos, lo que reduce la capacidad de respuesta ante estos crímenes.

Desde una perspectiva socioeconómica, el impacto de los ciberdelitos en Jalisco es significativo, los fraudes cibernéticos, por ejemplo, han afectado principalmente a sectores vulnerables como los adultos mayores y personas de bajos recursos que, debido a su falta de familiaridad con la tecnología, son más susceptibles a caer en engaños digitales. Esto refuerza la necesidad urgente de generar campañas de concientización y programas de capacitación para prevenir estos delitos.

Por otro lado, las empresas locales también enfrentan pérdidas millonarias debido a los ciberataques, virus que no solo afectan su economía, sino que también dañan su reputación

y confianza del cliente. Un análisis de la unidad de investigación de SILIKN advirtió que, entre 2024 y 2030, el aumento del cibercrimen podría provocar la desaparición de tres de cada cinco micro, pequeñas y medianas empresas (MiPyMEs) en México. El cibercrimen ha pasado a ser un factor adicional que empeora la situación de las MiPyMEs acelerando su extinción, pues su desaparición es un fenómeno preocupante que refleja los retos económicos y estructurales a los que se enfrentan en el país. La alta tasa de cierres, con un 83.5% de las MiPyMEs que no superan los dos años de operación, pone de manifiesto la necesidad urgente de políticas efectivas y apoyo integral para asegurar su sostenibilidad y crecimiento. (Ruiz, 2024)

El avance constante de tecnologías como la inteligencia artificial, el internet de las cosas y las criptomonedas presenta nuevos desafíos para la prevención y detección de ciberdelitos. Los delincuentes aprovechan estas herramientas para crear ataques más sofisticados y difíciles de rastrear.

Por ello, la actualización continua de capacidades técnicas, normativas y de capacitación institucional es indispensable para hacer frente a esta realidad en constante transformación.

A lo largo de los últimos cinco años, el análisis de las estadísticas de ciberdelitos en Jalisco revela que hay tendencias preocupantes relacionadas con el aumento de ciertos tipos de delitos. A continuación, se desglosan las principales tendencias observadas:

Fraude Electrónico y Estafas en Línea:

La incidencia de fraudes electrónicos ha aumentado significativamente, especialmente en plataformas de comercio electrónico, transacciones bancarias en línea y pagos móviles. Las víctimas suelen ser personas que no están completamente familiarizadas con las herramientas digitales, lo que facilita que los ciberdelincuentes exploten sus vulnerabilidades

Ciberacoso y Delitos de *Sexting*:

Otra tendencia alarmante es el aumento de los casos de ciberacoso, en particular aquellos que involucran la difusión de material íntimo no consentido (conocido como "*sexting*") y la

extorsión digital. En Jalisco, las víctimas de estos delitos son mayormente adolescentes y mujeres jóvenes.

Ataques a Infraestructuras Críticas:

Los ciberataques dirigidos a infraestructuras críticas, como hospitales, servicios públicos y bancos, también han mostrado un aumento. Estos ataques, que incluyen el ransomware, tienen como objetivo secuestrar información sensible para exigir pagos a cambio de su liberación.

Ciberterrorismo y Activismo Digital:

Aunque en menor medida, se ha detectado un aumento de ciberactivismo, con grupos de hackers realizando actos de hacktivismo para promover agendas políticas. Estos incidentes son más difíciles de medir y clasificar como ciberdelitos convencionales, pero se han incrementado en Jalisco durante las elecciones y en momentos de tensiones políticas.

Causas Estructurales y Socioeconómicas que Contribuyen a la Ciberdelincuencia

La ciberdelincuencia no surge de manera aislada ni es un fenómeno producto solo de las acciones de los delincuentes. Diversos factores estructurales contribuyen a la proliferación de estos delitos. A continuación, se detallan algunas de las principales causas observadas en Jalisco:

Brecha Digital:

Un factor clave en el aumento de los ciberdelitos es la brecha digital existente en muchas partes del Estado de Jalisco. La falta de alfabetización digital entre amplios sectores de la población genera un caldo de cultivo para los ciberdelincuentes, quienes explotan la vulnerabilidad de los usuarios menos experimentados en el uso de tecnologías. La falta de educación sobre cómo protegerse en línea y reconocer estafas virtuales sigue siendo una de las principales barreras para una mayor prevención. Según datos del INEGI (2023), solo el 55% de los habitantes de Jalisco tiene conocimientos básicos sobre ciberseguridad, lo que deja a una gran parte de la población expuesta a riesgos.

Desajustes en la Legislación Local:

En el estado de Jalisco no existe un marco normativo suficientemente robusto para abordar el incremento de ciberdelitos.

Falta de Capacitación en Instituciones Públicas y Privadas:

Otra causa importante es la falta de capacitación en ciberseguridad tanto en los organismos gubernamentales como en las empresas privadas. Muchas instituciones públicas, especialmente a nivel municipal, no tienen personal especializado en ciberseguridad, lo que dificulta la detección y respuesta rápida ante un ciberataque. Las empresas, por otro lado, no siempre implementan medidas adecuadas de protección de datos, lo que las convierte en blancos fáciles para los cibercriminales.

Cultura de Impunidad y Desconfianza en las Autoridades:

El desconocimiento sobre las herramientas y procedimientos legales para denunciar ciberdelitos genera una cultura de impunidad. La desconfianza en las autoridades también juega un papel importante en la baja tasa de denuncias. Muchos ciudadanos no creen que la denuncia de un ciberdelito conducirá a una acción efectiva, lo que contribuye a la falta de datos exactos sobre la magnitud del problema.

Una barrera crítica identificada es la baja cultura de denuncia, con solo un 35 % de los ciberdelitos reportados formalmente. Las principales razones que inhiben la denuncia son:

- Desconfianza en las autoridades: La percepción de falta de eficacia o lentitud en la investigación genera desmotivación.
- Temor a represalias: Especialmente en casos de violencia digital o amenazas.
- Desconocimiento sobre el proceso de denuncia: Muchas víctimas no saben cómo o dónde denunciar.

7.1 Mesas de Trabajo 2025 sobre Ciberdelitos y Violencia Digital en Jalisco

Durante el 2025 se llevaron a cabo dos mesas de trabajo interinstitucionales para abordar la problemática emergente y multidimensional de los ciberdelitos y la violencia digital en el estado de Jalisco.

- Primera Mesa: 27 de mayo de 2025.
- Segunda Mesa: 03 de julio de 2025.

Ambas sesiones se desarrollaron en El Colegio de Jalisco, reuniendo a representantes de instituciones públicas, organismos autónomos, academia y sociedad civil para reflexionar, diagnosticar y proponer estrategias frente a este fenómeno, con especial atención en la protección de niñas, niños y adolescentes (NNA).

La primera sesión de la Mesa de Ciberdelitos y Violencia Digital marcó un punto de partida estratégico para abordar una problemática creciente y altamente sensible: la violencia digital y los ciberdelitos que afectan de manera desproporcionada a niñas, niños, adolescentes y otros sectores vulnerables en el estado de Jalisco. Esta reunión permitió establecer un primer panorama sobre los retos normativos, institucionales, culturales y tecnológicos que enfrenta el estado frente a este fenómeno.

Uno de los aportes más significativos de la sesión fue el marco conceptual compartido, que permitió distinguir entre ciberdelitos (conductas tipificadas penalmente con uso de tecnología) y violencia digital (formas de agresión no siempre tipificadas, pero que causan daño y requieren atención). Esta distinción es fundamental para evitar la confusión en la intervención institucional y para diseñar políticas diferenciadas y efectivas, tanto desde lo preventivo como desde lo punitivo.

La Policía Cibernética de la Fiscalía del Estado habló sobre las conductas delictivas: desde el ciberacoso, la extorsión y la corrupción de menores, hasta la pornografía infantil y la suplantación de identidad. A su vez, se destacó que no todos los eventos digitales alcanzan el umbral penal, pero sí pueden representar riesgos importantes para la salud emocional, la

privacidad y la dignidad de las personas, especialmente cuando se perpetúan sin reconocimiento institucional o social.

En cuanto a los obstáculos estructurales, se identificaron tres grandes retos:

- El retraso normativo para reconocer y sancionar adecuadamente la violencia digital, lo cual dificulta la protección efectiva de las víctimas.
- La escasa capacidad técnica de las autoridades para recolectar, preservar y analizar evidencia digital en tiempo real, lo cual favorece la impunidad.
- La invisibilización de las víctimas, quienes frecuentemente no reconocen que han sido agredidas, lo que retrasa la denuncia y limita la intervención oportuna.

Los datos estadísticos presentados refuerzan la gravedad de la situación: el ciberacoso continúa siendo el delito más reportado entre adolescentes; la corrupción de menores ha incrementado significativamente; y el sexting, grooming y distribución de contenido sexual sin consentimiento persisten como amenazas constantes. Además, se evidenció que Jalisco se encuentra por encima de la media nacional en conectividad y uso de internet, lo que, si bien es un avance tecnológico, también expone a una mayor proporción de la población a posibles riesgos en entornos digitales.

En ese contexto, las y los participantes coincidieron en que la violencia digital es una extensión de las violencias estructurales ya existentes, y que, por tanto, su abordaje debe contemplar un enfoque de derechos humanos, perspectiva de género y protección integral de la infancia y adolescencia. Se reconoció también que la tecnología no es el enemigo, sino una herramienta que debe ser utilizada responsablemente, regulada inteligentemente y acompañada de alfabetización digital crítica desde edades tempranas.

Los acuerdos de esta primera mesa apuntaron a generar condiciones estructurales para la prevención y atención:

- Impulsar reformas legislativas a favor de NNA.
- Fortalecer el rol de las familias y escuelas como núcleos protectores.
- Mejorar los canales de denuncia y reducir la revictimización.

- Consolidar bases de datos confiables y alertas tempranas.

La Segunda Mesa de Trabajo sobre Ciberdelitos y Violencia Digital permitió identificar con claridad que esta problemática no solo está creciendo en términos cuantitativos, sino también en complejidad y sofisticación. La violencia digital, especialmente la dirigida a niñas, niños y adolescentes (NNA), está dejando de ser una amenaza marginal para convertirse en un riesgo estructural en los entornos educativos, familiares y comunitarios, muchas veces sin que sus víctimas o agresores reconozcan sus implicaciones legales, emocionales y sociales.
Uno de los hallazgos más importantes de esta sesión fue la desarticulación entre las capacidades institucionales, los marcos normativos y las necesidades sociales actuales. Si bien existen esfuerzos relevantes desde el sector educativo, judicial, de seguridad pública y desde la sociedad civil, la ausencia de una política integral de prevención y atención de los ciberdelitos impide respuestas efectivas, coordinadas y sostenibles. La duplicidad de acciones, la falta de protocolos unificados, y el subregistro de casos limitan el diseño de intervenciones pertinentes y oportunas.

Asimismo, se reconoció que la tecnología por sí sola no es el problema, sino el uso que se le da. La formación de madres, padres, docentes y personas cuidadoras, así como el empoderamiento de las infancias y juventudes para navegar de manera segura en internet, son pilares fundamentales para transformar el entorno digital en un espacio de cuidado y no de vulnerabilidad.

La Policía Cibernética enfrenta limitaciones operativas por la falta de herramientas especializadas y de cooperación con plataformas digitales, lo que impacta negativamente en la capacidad de investigación, judicialización y sanción de los delitos. Esta situación, sumada a la creciente demanda de apoyo por parte de las víctimas, como evidencian los más de 800 casos diarios que llega a recibir el Colectivo DLR, revela la urgencia de fortalecer las capacidades institucionales, tanto en lo técnico como en lo humano.

Por otro lado, la sesión puso sobre la mesa la necesidad de repensar la legislación vigente, no necesariamente para crear más leyes, sino para armonizar y actualizar las ya existentes,

cerrando brechas, eliminando ambigüedades y garantizando que sean aplicables en un entorno digital en constante cambio.

Finalmente, se reafirmó que la violencia digital no puede abordarse desde un solo frente. Se necesita una estrategia estatal basada en cuatro pilares fundamentales: la prevención, la atención integral, la generación de datos confiables y la formación ciudadana. Solo a través del trabajo conjunto entre gobierno, sociedad civil, academia y sector privado se podrán diseñar políticas públicas efectivas, basadas en evidencia, sensibles al contexto local y centradas en los derechos humanos.

Este ejercicio interinstitucional representa un paso clave hacia la construcción de un análisis sólido sobre ciberdelitos, que dé sustento a futuras acciones normativas, preventivas y de atención, con el fin de construir un entorno digital más seguro, justo e incluyente para todas las personas, especialmente para las infancias y adolescencias de Jalisco.

Acuerdos clave

- Armonización normativa sin sobrelegislar, con enfoque en derechos digitales.
- Fortalecimiento institucional en tecnología, capacitación y especialización.
- Prevención comunitaria y escolar con enfoque de derechos y género.
- Campañas para desnaturalizar la violencia digital**.**
- Documentación confiable y mecanismos de alerta temprana**.**
- Coordinación interinstitucional efectiva y sostenida**.**

7.2 Buenas Prácticas Internacionales:

1. Legislación Específica sobre Ciberdelitos y Tecnologías Emergentes

- ***Australia*** **– Online Safety Act 2021**
  Ley que impone obligaciones claras a plataformas para eliminar contenido dañino, incluyendo violencia digital, ciberacoso, y pornografía no consensuada. Crea la figura del *eSafety Commissioner* con autoridad para emitir sanciones.

- ***Alemania* – NetzDG (Ley de Aplicación de la Red)**
  Exige que las plataformas eliminen contenido ilegal (odio, amenazas, etc.) en menos de 24 horas. Multas de hasta €50 millones por incumplimiento.

2. Agencias Especializadas y Coordinación Institucional

- ***Reino Unido* – National Cyber Security Centre (NCSC)**
  Agencia técnica del gobierno para prevención, manejo de incidentes y ciberprotección de infraestructuras críticas.
- ***Singapur* – Cyber Security Agency (CSA)**
  Agencia nacional con funciones regulatorias, educativas y de monitoreo de infraestructuras.

3. Educación Digital y Campañas de Concientización

- ***Estonia* – Formación en ciberseguridad desde la educación primaria**
  Plan de estudios escolar con contenidos en ciberhigiene, privacidad, y defensa digital.
- ***Canadá* – Campaña Nacional "Get Cyber Safe"**
  Plataforma educativa del gobierno con herramientas y guías para protegerse en línea.

4. Protección Legal Contra la Violencia Digital y Uso Ilegítimo de IA

- ***Francia* – Ley contra el odio en línea (Loi Avia)**
  Obliga a retirar contenido violento o de odio en 24 horas. Algunas disposiciones fueron moderadas por el Consejo Constitucional.
- ***Corea del Sur* – Criminalización de deepfakes sexuales**
  Criminaliza la creación, difusión o simple tenencia de contenido sexual falso sin consentimiento.

5. Transparencia y Datos Abiertos sobre Ciberdelitos

- ***Estados Unidos* – Plataforma IC3 (FBI)**

Portal para denuncias de ciberdelitos y publicación anual de estadísticas detalladas. Permite identificar tendencias, tipo de fraude y pérdidas económicas.

A continuación, se presenta una tabla comparativa que ilustra los vacíos actuales en México frente a iniciativas destacadas a nivel internacional en materia de prevención, legislación y combate al ciberdelito:

Tabla 1. Buenas prácticas internacionales y la situación en México (2024)

Eje Estratégico	*Buenas Prácticas Internacionales*	*Situación Actual en México*
Legislación	Leyes que obligan a plataformas a retirar contenido ilegal en plazos definidos (Australia, Alemania). Regulación sobre el uso de IA y deepfakes (Corea del Sur).	La legislación mexicana no contempla plazos obligatorios de remoción ni marcos específicos para IA o contenido manipulado digitalmente.
Institucionalidad	Agencias especializadas en ciberseguridad con capacidad operativa y técnica (NCSC - Reino Unido, CSA - Singapur).	Las funciones están dispersas entre varias dependencias (Guardia Nacional, SICT, SRE, etc.), sin una entidad única técnica y autónoma.
Educación y Cultura Digital	Incorporación de educación digital desde la infancia (Estonia), campañas nacionales permanentes de alfabetización digital (Canadá).	La educación digital no forma parte del currículo obligatorio nacional. Las campañas son esporádicas y sin continuidad.
Derechos Digitales y Violencia	Penalización específica de deepfakes sexuales y contenido no consensuado (Corea del Sur). Legislación sobre discurso de odio y violencia digital (Francia).	Existen leyes parciales como la "Ley Olimpia", pero no hay una regulación federal integral sobre uso ilegítimo de IA ni violencia digital sistematizada.
Datos y Transparencia	Sistemas de denuncia accesibles, con datos abiertos y estadísticas anuales (EE.UU. - IC3).	No hay un portal nacional para denuncias cibernéticas con datos abiertos. Las cifras son escasas y desarticuladas.

Fuente: Elaboración propia con datos obtenidos mediante investigación documental

Dinamarca, la identidad digital y deepfakes

Dinamarca se posiciona a la vanguardia de la regulación digital al proponer una reforma pionera que otorgaría derechos de autor a las personas sobre su propia identidad física (rostro, voz y cuerpo) como respuesta al creciente uso de deepfakes generados por inteligencia

artificial. Esta iniciativa, representa un hito en la defensa de los derechos personales frente a la manipulación tecnológica y el uso no autorizado de la imagen.

La propuesta pretende que cualquier persona pueda reclamar legalmente la eliminación de contenido manipulado en el que se le represente sin consentimiento, además de solicitar compensaciones económicas. Este marco se convierte en una herramienta legal robusta contra contenidos que, aunque generados digitalmente, afectan la integridad, reputación o incluso la seguridad de las personas. En esencia, se reconoce el rostro y la voz como propiedad intelectual y, por tanto, sujetos de protección bajo el régimen de copyright.

Este enfoque responde a una necesidad urgente. El crecimiento exponencial de los contenidos deepfake, que combinan hiperrealismo con facilidad de distribución viral, ha generado un terreno fértil para la desinformación, el fraude digital, la extorsión, el daño reputacional y la violencia simbólica, particularmente hacia figuras públicas, activistas, periodistas y, en muchos casos, mujeres víctimas de pornografía no consensuada.

La experiencia danesa representa un referente clave para países latinoamericanos, como México, que actualmente carecen de normativas específicas para proteger la identidad digital ante la generación y difusión de contenido manipulado por inteligencia artificial.

8. POSIBLES EFECTOS DE LAS CIRCUNSTANCIAS Y ESCENARIOS

8.1 Contexto a nivel internacional

A nivel global, la ciberdelincuencia se ha consolidado como una amenaza multidimensional que afecta no solo la seguridad individual, sino también la estabilidad económica y política de los países. Según el **Informe de Seguridad Cibernética Global 2024** de la firma IBM, el costo global del cibercrimen alcanzó los 4.88 millones de dólares en 2024, con un aumento del 15% anual desde 2020. Esta tendencia refleja la sofisticación y expansión constante de

las técnicas utilizadas por los actores maliciosos, desde ataques de ransomware hasta campañas de desinformación digital.

Además, organismos internacionales como la **Interpol** y la **ONU** han alertado sobre el riesgo creciente de que grupos criminales y actores estatales utilicen el ciberespacio para la interferencia política, el espionaje económico y el terrorismo digital, lo que requiere una cooperación internacional más estrecha y marcos legales armonizados.

8.2 Contexto a nivel nacional

En México, el aumento de la conectividad y la digitalización de servicios públicos y privados han propiciado un entorno favorable para la proliferación de ciberdelitos.

Entre los efectos más relevantes se encuentra la afectación a la confianza ciudadana en las plataformas digitales, la pérdida económica y el impacto psicológico en las víctimas, especialmente en casos de violencia digital contra mujeres, niñas, niños y adolescentes.

El sector empresarial también reporta pérdidas considerables debido a ataques cibernéticos, afectando la competitividad y la inversión extranjera.

8.3 Contexto a nivel estatal

En Jalisco, la expansión de las tecnologías digitales ha ido acompañada de un incremento en la incidencia de ciberdelitos. Las autoridades locales reconocen que, aunque las denuncias han aumentado, la capacidad para atender, investigar y sancionar estos delitos todavía presenta deficiencias, derivadas de limitaciones técnicas, humanas y normativas.

El impacto social se refleja en la vulnerabilidad de grupos específicos, como adolescentes, mujeres y pequeños comerciantes, que sufren consecuencias directas como pérdida económica, daño a la reputación, y afectaciones psicológicas.

Además, el entorno digital propicia nuevas formas de violencia y discriminación que afectan la cohesión social y requieren respuestas integrales desde los ámbitos educativo, legal y comunitario.

- En 2020, cuando ya estaba vigente la Ley Olimpia en Jalisco, se registraron 66 denuncias por ciberacoso y 41 por violación a la intimidad sexual. En 2021, sumaban ya 10 y 17 respectivamente, para esos delitos. A pesar del volumen de denuncias, ningún caso había sido judicializado durante ese periodo. (TELEDIARIO, 2021)
- En 2022, la Fiscalía del Estado recibió 1,211 denuncias por violación a la intimidad sexual y ciberacoso, pero solo 46 carpetas de investigación judicializadas. Lo que indica una impunidad del orden del 96 % según medios locales. (DIPUTADOSMORENA.ORG.MX, 2023)
- Medios locales documentan un aumento de estafas dirigidas a comerciantes que venden en plataformas (Marketplace, redes sociales): perfiles falsos, capturas de pago fraudulentas, presiones para enviar producto sin confirmación y poca ayuda de administradores de las plataformas. (Informador, 2025)

Esto muestra que, aunque hay reconocimiento del problema (las denuncias van en aumento), existe falta de capacidad institucional de llevar estas denuncias hasta sanción judicial, lo que refuerza la idea de deficiencias técnicas, humanas o normativas. Así mismo existe un alto riesgo para los comerciantes que operan en plataformas digitales ya que pueden ser víctimas de estafas mediante perfiles falsos, suplantación o manipulación de confianza.

En septiembre de 2025, la Vicefiscalía Especializada en Delitos de Género, Mujeres, Niñas, Niños y Adolescentes de Jalisco vinculó a proceso a 194 personas por hechos relacionados con violencia contra mujere,s incluyendo ciberacoso, violación a la intimidad, amenazas, entre otros

. (informador, 2025) Esto nos muestra que hay cierta respuesta institucional: no solo denuncias, sino que en algunos casos se llega a procesar. Este tipo de dato sirve para

contrastar con los periodos anteriores, evidenciar mejoras, pero también para ver la escala aún insuficiente frente al problema.

8.4 Causas del problema

La evaluación de los escenarios actuales en torno a los ciberdelitos en Jalisco evidencia una serie de efectos negativos de corto, mediano y largo plazo que amenazan la estabilidad digital, la confianza ciudadana y la integridad institucional. Estos efectos no solo comprometen la seguridad individual, sino que también inciden en la gobernanza, la economía y la cohesión social.

Uno de los efectos más inmediatos es el aumento de la percepción de inseguridad digital, especialmente entre los jóvenes y usuarios frecuentes de plataformas en línea. Esta percepción afecta negativamente la confianza en las instituciones encargadas de la ciberseguridad, incluyendo la policía cibernética y las fiscalías especializadas.

Otro efecto relevante es la afectación económica, tanto para personas como para empresas. Los fraudes electrónicos, el ransomware y el robo de identidad generan pérdidas millonarias, especialmente para pequeñas y medianas empresas que no cuentan con infraestructura de seguridad robusta.

En términos sociales, se observa una creciente vulnerabilidad de sectores específicos, como niñas, niños y adolescentes, frente a delitos como el grooming, la explotación sexual y el ciberacoso. Esta problemática genera efectos psicológicos profundos y afecta el desarrollo integral de las víctimas.

Asimismo, se han identificado déficits institucionales en la respuesta ante los ciberdelitos, incluyendo la falta de personal capacitado, carencia de protocolos homologados, y escasa coordinación entre niveles de gobierno. Estos vacíos limitan la capacidad de prevención y judicialización efectiva de los casos.

A mediano plazo, estos escenarios podrían traducirse en una erosión del estado de derecho digital, debilitando la capacidad del Estado para garantizar derechos y libertades en el entorno virtual. Esto se acompaña de un debilitamiento de la cultura de la denuncia, propiciando un entorno de impunidad.

Desde una perspectiva más amplia, se corre el riesgo de que Jalisco se convierta en un nodo vulnerable en redes delictivas transnacionales, especialmente en actividades como el phishing, el tráfico de datos personales y la ciberdelincuencia financiera organizada. Este tipo de dinámicas refuerzan la necesidad de cooperación internacional y desarrollo de capacidades técnicas locales.

Finalmente, el impacto educativo también es significativo. La normalización de prácticas como la suplantación de identidad, el acceso no autorizado a información y el uso indebido de redes sociales, plantea un reto ético y formativo que debe ser abordado desde las instituciones educativas.

En resumen, los efectos de los escenarios identificados van más allá del ámbito técnico o policial, y demandan una respuesta multisectorial, articulada desde el Estado, el sector privado, la academia y la sociedad civil.

8.5 Causas estructurales

Macro-estructurales (nivel estatal y nacional)

- Brechas en el marco normativo: Leyes desactualizadas o insuficientes frente a nuevas modalidades de ciberdelitos, como deepfakes o ransomware como servicio.
- Desigualdad socioeconómica: Acceso limitado a educación digital y tecnologías de seguridad en zonas rurales o marginales.
- Políticas públicas insuficientes: Falta de estrategias integrales de ciberseguridad y prevención que involucren a todos los sectores de la sociedad.
- Baja coordinación interinstitucional: Escasa integración entre autoridades

estatales, municipales y federales, lo que reduce la eficacia en prevención y persecución.

Meso-estructurales (nivel institucional o comunitario)

- Capacidad limitada de instituciones: Recursos humanos y tecnológicos insuficientes en cuerpos policiales, fiscalías y ministerios públicos especializados en delitos cibernéticos.
- Falta de protocolos estandarizados: Ausencia de lineamientos claros para la investigación, atención a víctimas y seguimiento de casos.
- Redes de cooperación débiles: Pocas alianzas entre gobierno, sector privado, academia y sociedad civil para intercambio de información y prevención.

Micro-estructurales (nivel individual o familiar)

- Baja cultura de ciberseguridad: Usuarios con conocimientos limitados sobre protección de datos, contraseñas seguras o reconocimiento de fraudes.
- Exposición a riesgos cotidianos: Uso frecuente de dispositivos móviles, redes sociales y servicios de banca digital sin prácticas de seguridad.
- Vulnerabilidad social y emocional: Jóvenes y adultos mayores con menor supervisión o acompañamiento en entornos digitales, lo que los hace más susceptibles a engaños o extorsiones.

8.6 Posibles efectos por grupos etarios vulnerables

Niños y adolescentes

- Exposición a grooming, ciberacoso y contenido inapropiado, con impactos en la salud mental y emocional.
- Riesgo de phishing educativo o fraude en aplicaciones de juegos.
- Efectos a largo plazo en la confianza digital y hábitos de seguridad online.

Jóvenes (18-29 años)

- Alta incidencia en fraudes financieros, robo de identidad y estafas en

comercio electrónico.

- Vulnerabilidad ante campañas de desinformación y manipulación en redes sociales, afectando la percepción política y social.
- Impacto potencial en economía personal y reputación digital, con consecuencias en oportunidades académicas o laborales.

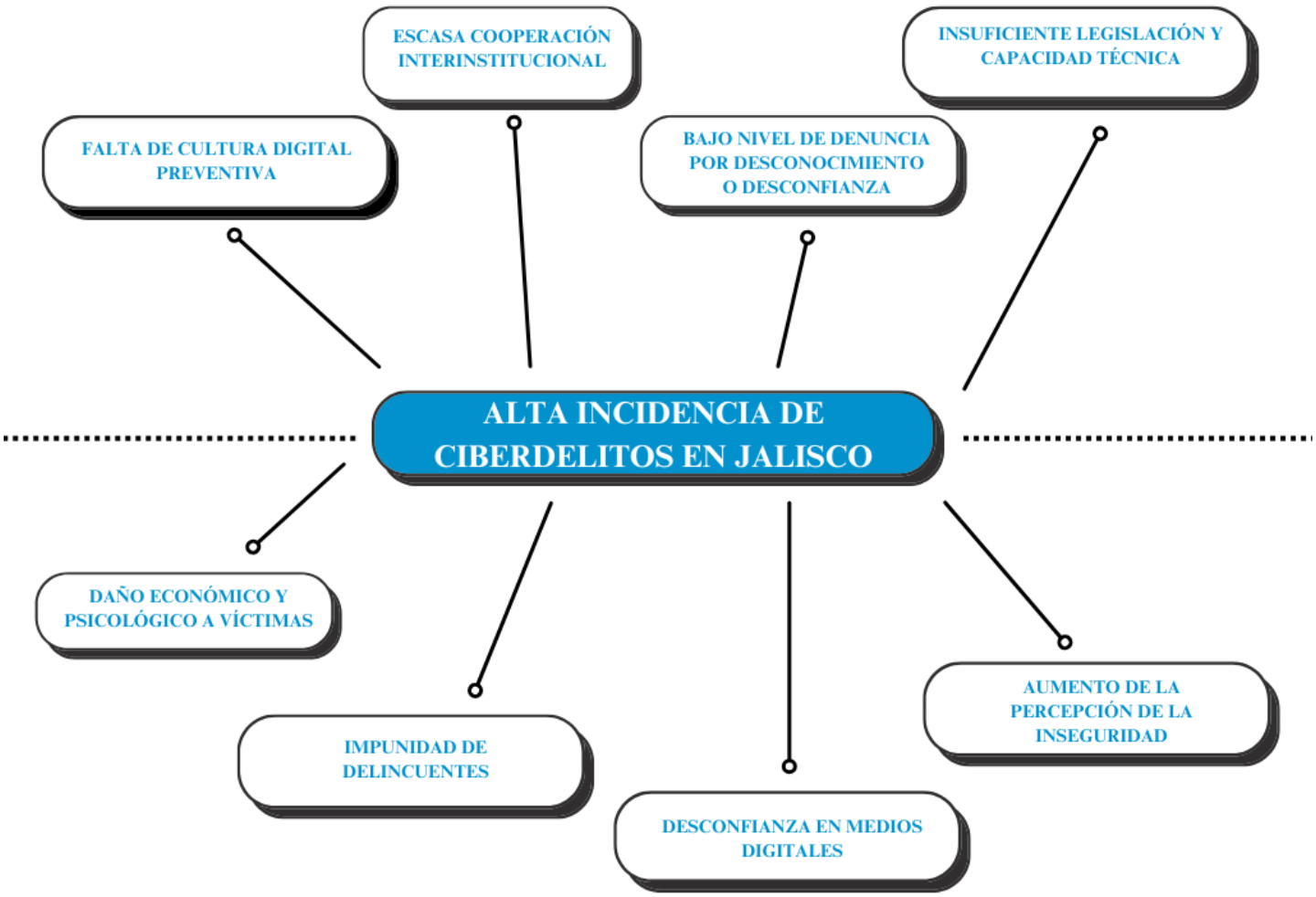
Adultos (30-59 años)

- Mayor exposición a fraudes financieros y extorsiones vía correo electrónico o mensajería instantánea, especialmente durante períodos de pago o compras en línea.
- Riesgo de afectación económica significativa debido a inversiones fraudulentas o suplantación de identidad.
- Estrés y pérdida de confianza en instituciones financieras y gubernamentales.

Adultos mayores (60+ años)

- Vulnerabilidad a fraudes telefónicos y ciberestafas de suplantación de identidad, por menor familiaridad tecnológica.
- Posibles efectos psicológicos graves, incluyendo ansiedad, miedo o aislamiento social.
- Dependencia de familiares o instituciones para restaurar su seguridad digital y financiera

9. ÁRBOL DE PROBLEMAS



Fuente: Elaboración propia por personal de la Secretaría Ejecutiva del Consejo Ciudadano, con los datos obtenidos mediante investigación documental e información obtenida por correspondencia oficial.

10. CONCLUSIONES Y RECOMENDACIONES

10.1 Conclusiones

El análisis del fenómeno de los ciberdelitos en el Estado de Jalisco permite reconocer una problemática compleja, dinámica y en constante transformación. La creciente conectividad, el acceso generalizado a internet y el uso cotidiano de dispositivos digitales han generado nuevas oportunidades de desarrollo, pero también un entorno vulnerable donde se incrementan las conductas ilícitas en línea.

Entre los delitos más frecuentes se identifican el fraude electrónico, la suplantación de identidad, el ciberacoso y la difusión no consentida de contenido íntimo. Estas conductas afectan principalmente a niñas, niños, adolescentes y personas usuarias comunes, lo que evidencia la necesidad de fortalecer las habilidades digitales, promover la educación en seguridad cibernética y fomentar una cultura de autoprotección en el entorno digital.

Este documento también muestra que, aunque las instituciones estatales han avanzado en la atención de estos casos y en la promoción de la ciberprevención, aún existen retos importantes. Entre ellos destacan la falta de recursos tecnológicos, la necesidad de capacitación constante del personal especializado y la importancia de una mejor coordinación interinstitucional para la investigación y sanción de los ciberdelitos.

Asimismo, se identificó que gran parte de la población aún desconoce los mecanismos disponibles para denunciar o bien, no los utiliza por miedo, desconfianza o falta de información. Esta situación reafirma la importancia de fortalecer la cultura de la denuncia y de seguir impulsando campañas de sensibilización que acerquen a la ciudadanía a los canales de atención y acompañamiento.

El fenómeno de los ciberdelitos trasciende el ámbito tecnológico, ya que impacta directamente en la seguridad, la privacidad y la confianza de las personas en el entorno digital. Por ello, se requiere una respuesta integral que combine prevención, educación, atención oportuna.

Solo mediante una acción coordinada, sostenida y con enfoque de derechos humanos será posible reducir la incidencia de los ciberdelitos y avanzar hacia un entorno digital más seguro, ético y confiable para todas las personas en Jalisco.

10.2 Recomendaciones

A partir del análisis realizado, se proponen las siguientes líneas de acción:

1. **Fortalecimiento normativo y jurídico**

   Es indispensable actualizar el marco normativo estatal en materia de ciberdelitos, armonizándolo con los estándares nacionales e internacionales, incorporando figuras delictivas emergentes y mecanismos para la persecución penal eficaz y regulando plataformas digitales.

   Orientación de política pública: Establecer reformas legislativas y protocolos claros de actuación para autoridades competentes.

   Actores a los que va dirigida:

   Congreso del Estado de Jalisco.

   Fiscalía del Estado (área de delitos cibernéticos).

   Poder Judicial y autoridades regulatorias.

2. **Capacitación y profesionalización**

   Incrementar la capacidad técnica de las instituciones encargadas de la investigación, persecución y atención de ciberdelitos mediante programas de

formación continua en ciberseguridad, análisis forense digital, inteligencia artificial y normatividad aplicable.

Orientación de política pública: Diseñar programas estatales de profesionalización con recursos específicos y alianzas con instituciones académicas y tecnológicas.

Actores a los que va dirigida:

Policía Cibernética

Fiscalía Especializada en Delitos Electrónicos.

Comisarías municipales.

Instituciones académicas y centros de investigación.

3. Educación y cultura digital

Implementar campañas permanentes para la ciudadanía orientadas a la prevención de riesgos en entornos digitales, la protección de datos personales y la denuncia segura de ciberdelitos.

Orientación de política pública: Establecer estrategias transversales de alfabetización digital que involucren a los sectores educativo, empresarial y social.

Actores a los que va dirigida:

Secretaría de Educación Jalisco.

Instituciones educativas públicas y privadas.

Organizaciones de la sociedad civil especializadas en derechos digitales.

Medios de comunicación y plataformas digitales.

4. Mejora en la atención a víctimas

Garantizar un servicio eficiente, especializado y sensible para la atención integral de víctimas de ciberdelitos, que incluya orientación jurídica, psicológica y tecnológica.

Orientación de política pública: Crear protocolos estandarizados y unidades especializadas en atención a víctimas en delitos cibernéticos, incorporando mecanismos de denuncia accesibles y seguros.

Actores a los que va dirigida:

Fiscalía del Estado.

Unidades de Atención a Víctimas.

Organismos de derechos humanos.

Instituciones de apoyo psicológico y social.

5. Cooperación interinstitucional y con el sector privado

Establecer mecanismos permanentes de colaboración entre instituciones gubernamentales, sector privado, academia y organizaciones sociales, con el fin de intercambiar información, recursos tecnológicos y buenas prácticas para prevenir y combatir los ciberdelitos.

Orientación de política pública: Crear mesas de trabajo y convenios de colaboración que fortalezcan la inteligencia compartida y la respuesta coordinada ante incidentes cibernéticos.

Actores a los que va dirigida:

Fiscalía del Estado.

Policía Cibernética.

Empresas de tecnología y telecomunicaciones.

Instituciones académicas y de investigación.

Organizaciones de la sociedad civil.

10.3 Hallazgos

Del análisis realizado se identificaron tendencias y patrones que reflejan la evolución de los ciberdelitos en el Estado de Jalisco. Estos hallazgos permiten comprender mejor el comportamiento delictivo en entornos digitales, así como los factores contextuales que influyen en su incidencia.

1. Ciberdelitos Emergentes

Se observa la aparición y consolidación de nuevas modalidades delictivas asociadas al uso intensivo de tecnologías:

Deepfakes y manipulación audiovisual: Uso de IA para crear videos o audios falsos con fines de extorsión, difamación o fraude.

Phishing avanzado mediante IA: Correos y mensajes altamente personalizados que imitan patrones lingüísticos del destinatario.

Fraudes en plataformas de comercio electrónico y redes sociales: Venta de productos inexistentes, clonación de cuentas y estafas en marketplace.

Ransomware como servicio (RaaS): Criminales que arriendan herramientas para secuestro de datos sin conocimientos técnicos avanzados.

Estafas relacionadas con criptomonedas y trading falso: Ofertas fraudulentas de inversión y robo de wallets.

Suplantación mediante aplicaciones de mensajería: Uso de WhatsApp, Telegram y otras apps para fraudes y extorsión.

2. Factores de riesgo específicos por contexto geográfico.

Existen diferencias significativas según la ubicación y características socioeconómicas:

Zonas urbanas: Mayor exposición a fraudes financieros, phishing y robo de identidad por alto uso de servicios digitales y bancarización.

Zonas rurales y semiurbanas: Vulnerabilidad en programas sociales y becas, fraudes relacionados con apoyos gubernamentales, y falta de alfabetización digital.

Regiones con alta actividad turística: Incremento en fraudes relacionados con reservaciones falsas y alquileres temporales fraudulentos.

3. Factores de riesgo por temporalidad

El análisis revela que la incidencia de ciberdelitos aumenta en ciertos periodos:

Días de pago (quincenas): Mayor número de intentos de phishing, fraudes financieros y clonación de tarjetas.

Temporada navideña y Buen Fin: Incremento en fraudes por comercio electrónico y promociones falsas.

Períodos electorales: Campañas de desinformación, ataques a sitios web institucionales y robo de datos personales con fines políticos.

Regreso a clases: Fraudes relacionados con la venta de útiles escolares y cursos falsos.

11. RESULTADOS Y ACCIONES ESPERADAS

A través de la implementación de estas propuestas, se espera alcanzar los siguientes resultados:

11.1 Corto plazo

Este apartado establece los escenarios deseables (resultados) y las acciones concretas que permitirían alcanzarlos. Se considera que estos logros solo son posibles mediante la participación activa y coordinada de las instancias competentes, con un enfoque progresivo en corto, mediano y largo plazo.

Resultados esperados:

- Contar con un ejercicio consultivo integral formalizado y difundido, que sirva como base para la toma de decisiones.
- Mayor sensibilización de autoridades y ciudadanía sobre la importancia de la ciberseguridad.
- Funcionarios públicos con conocimientos básicos en prevención y atención de ciberdelitos.
- Canales de denuncia más accesibles y confiables para la población.

Acciones esperadas:

- Consolidación de un documento integral: Formalizar y difundir los resultados del ejercicio consultivo acerca de ciberdelitos.
- Implementación de campañas de concientización: Desarrollar campañas educativas para fomentar la cultura de la denuncia y el uso seguro de tecnologías digitales.
- Capacitación inicial a funcionarios públicos: Impartir cursos básicos en ciberseguridad a personal de seguridad pública, procuración de justicia y áreas administrativas.
- Establecimiento de canales de denuncia accesibles: Crear o mejorar plataformas digitales para la denuncia anónima y segura.

11.2 Mediano plazo

Resultados esperados:

- Marco normativo actualizado y alineado con estándares nacionales e internacionales.
- Instituciones fortalecidas en recursos humanos y tecnológicos para combatir ciberdelitos.
- Alianzas consolidadas entre gobierno, sector privado, academia y sociedad

civil.

- Inclusión de la ciberseguridad en programas educativos y capacitación ciudadana.
- Protocolos claros para atención integral a víctimas, con enfoque sensible y especializado.

Acciones esperadas:

- Revisión y adecuación del marco normativo: Proponer reformas legales para cerrar vacíos y armonizar la legislación.
- Fortalecimiento institucional: Dotar a las unidades de ciberseguridad con personal especializado y equipamiento tecnológico.
- Alianzas multisectoriales: Formalizar convenios de colaboración para intercambio de información y recursos.
- Desarrollo de programas educativos: Incorporar contenidos de ciberseguridad en planes escolares y cursos de capacitación para adultos.
- Implementación de protocolos de atención a víctimas: Establecer lineamientos para asistencia legal y apoyo psicológico.

11.3 Largo Plazo

Resultados esperados:

- Consolidación de un sistema estatal de ciberseguridad robusto y eficiente.
- Ciudadanía con cultura digital fortalecida y mayor confianza en las instituciones.
- Innovación tecnológica permanente para anticipar nuevas amenazas.
- Políticas y estrategias dinámicas gracias a mecanismos de evaluación y mejora continua.

Acciones esperadas:

- Consolidación de un sistema estatal de ciberseguridad: Integrar esfuerzos

técnicos, normativos y sociales en una estructura coordinada.

- Cultura ciudadana consolidada: Desarrollar campañas permanentes y programas comunitarios para prevención y denuncia.
- Innovación tecnológica constante: Mantener inversiones en infraestructura tecnológica y herramientas avanzadas.
- Evaluación y mejora continua: Implementar sistemas de monitoreo para ajustar políticas y estrategias conforme evolucionen los ciberdelitos.

12. REFERENCIAS BIBLIOGRÁFICAS

- AMECI. (2023). *Asociación Mexicana de Ciberseguridad*. Obtenido de https://www.ameci.org/blog/alertan-por-presencia-de-la-delincuencia-en-el-ambito-digital
- Congreso. (s.f.). *LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DEL ESTADO DE JALISCO Y SUS MUNICIPIOS*. Obtenido de https://info.jalisco.gob.mx/sites/default/files/leyes/leydep2.pdf
- Dr. Caritino Morales, D. P. (s.f.). *Ciencia Latina*. Obtenido de Delitos informaticos un tema de atencion legislativa en el estado de Guerrero: https://dialnet.unirioja.es/descarga/articulo/10070457.pdf
- ESTADO, C. D. (s.f.). *LEY DE ACCESO DE LAS MUJERES A UNA VIDA LIBRE DE VIOLENCIA DEL ESTADO DE JALISCO*. Obtenido de https://igualdad.jalisco.gob.mx/wp-content/uploads/2021/12/Ley_de_Acceso_de_las_Mujeres_a_una_Vida_Libre_de_Violencia_del_Estado.pdf
- IMSS. (s.f.). *imss.gob.mx*. Obtenido de https://www.imss.gob.mx/salud-en-linea/salud-mental#:~:text=%C2%BFQu%C3%A9%20es%20la%20salud%20mental,persona%20ante%20momentos%20de%20estr%C3%A9s.
- INAI. (s.f.). *Informe sobre ciberseguridad y proteccion de datos*. Obtenido de https://home.inai.org.mx/
- INEGI. (2023). *ENDUTIH*. Obtenido de https://www.inegi.org.mx/programas/dutih/2023/
- INEGI. (s.f.). *Estudio sobre los hábitos de usuarios de Internet en México 2024 y Perspectiva de la IA*. Obtenido de https://www.inegi.org.mx/contenidos/inegi/ccu/2024/segunda_sesion/presentaciones/habitos_internet.pdf
- Nader, H. &. (2021). *El Reglamento General de Protección de Datos (GDPR) de la Unión Europea y sus implicaciones en México*. Obtenido de https://www.nhg.mx/es/el-reglamento-general-de-proteccion-de-datos-gdpr-de-la-union-europea-y-sus-implicaciones-en-mexico/
- NIS, D. (2016). *Directiva SRI 2*. Obtenido de https://digital-strategy.ec.europa.eu/es/policies/nis2-directive

- OAS. (2001). *Convenio de Budapest*. Obtenido de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
- Olimpia, L. (2021). *Gobierno de Mexico*. Obtenido de https://www.gob.mx/profeco/es/articulos/la-ley-olimpia-y-el-combate-a-la-violencia-digital?idiom=es
- OMS. (17 de JUNIO de 2022). *OMS*. Obtenido de OMS: https://www.who.int/es/news-room/fact-sheets/detail/mental-health-strengthening-our-response#:~:text=La%20salud%20mental%20es%20un,la%20mejora%20de%20su%20comunidad.
- ONU. (2000). *CONVENCIÓN DE LAS NACIONES UNIDAS CONTRALADELINCUENCIAORGANIZADA TRANSNACIONALYSUS PROTOCOLOS*. Obtenido de https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf
- Organization, A. H. (2021). *paho*. Obtenido de paho: https://www.paho.org/es/enlace/causas-principales-mortalidad-discapacidad
- Roa, M. M. (6 de octubre de 2023). *statista*. Obtenido de statista: https://es.statista.com/grafico/25428/encuestados-que-afirman-haber-tenido-problemas-de-salud-mental-en-los-ultimos-12-meses/
- Secretaría Ejecutiva, C. C. (2021). *Diagnóstico del Sistema Penitenciario y Reinserción Social.* Guadalajara Jalisco.
- Seguridad, C. C. (2023). *consejociudadano*. Obtenido de consejociudadano: https://consejociudadano.org.mx/tecnologias-del-centro-de-coordinacion-comando-control-comunicaciones-y-computo/
- Seguridad, C. C. (2025). *Consejo Ciudadano de Seguridad*. Obtenido de Consejo Ciudadano de Seguridad: https://consejociudadanojalisco.org/transparencia
- Seguridad, C. C. (s.f.). *Plan Estatal Jalisco*. Obtenido de https://plan.jalisco.gob.mx/wp-content/uploads/2024/11/1-Consejo-Ciudadano-de-Seguridad.pdf
- UNIÓN, C. D. (20 de 12 de 2022). *LNSIJPA*. Obtenido de https://www.diputados.gob.mx/LeyesBiblio/pdf/LNSIJPA.pdf
- UNIÓN, C. D. (01 de 04 de 2024). *LNEP*. Obtenido de https://www.diputados.gob.mx/LeyesBiblio/pdf/LNEP.pdf

- UNIÓN, C. D. (20 de marzo de 2025). *LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS* . Obtenido de https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf
- UNODOC. (enero de 2011). *Oficina de las Naciones Unidas contra la Drga y el delito.* Recuperado el 08 de 11 de 2022, de https://www.unodc.org/pdf/criminal_justice/UN_Justice_Section_Brochure_Spanish.pdf

- Gobierno de Jalisco. (2024). Informe sobre ciberdelitos en Jalisco. Fiscalía General del Estado de Jalisco.
- López, A., & García, M. (2022). Impacto del robo de identidad en el Estado de Jalisco: Un estudio sobre fraudes digitales. Revista de Seguridad Digital, 8(2), 45-60.
- Pérez, J., & Rodríguez, F. (2023). Análisis de fraudes cibernéticos y sus tendencias en Jalisco. Universidad de Guadalajara.
- Rodríguez, P., Sánchez, L., & Torres, V. (2023). Capacitación en ciberseguridad en Jalisco: Barreras y soluciones. Centro de Investigación en Ciberseguridad de Jalisco.
- Gobierno de Jalisco. (2024). Informe sobre ciberdelitos en Jalisco. Fiscalía General del Estado de Jalisco.
- González, R., & Hernández, M. (2023). Ciberterrorismo y hacktivismo: Nuevas formas de conflicto digital en Jalisco. Revista de Seguridad Digital, 9(1), 33-47.
- López, A., & Ramírez, P. (2023). Retos legislativos en ciberseguridad en Jalisco: Un análisis crítico. Universidad Autónoma de Jalisco.
- Pérez, J., & Rodríguez, F. (2023). Análisis de fraudes cibernéticos y sus tendencias en Jalisco. Universidad de Guadalajara.
- Secretaría de Innovación, Ciencia y Tecnología de Jalisco. (2024). Ciberseguridad y su impacto en el sector empresarial de Jalisco.
- Universidad de Guadalajara. (2023). Estudio sobre la brecha digital en Jalisco. Reporte del Centro de Investigación en Tecnologías de la Información.
- Consejo Ciudadano para la Seguridad y Justicia de la Ciudad de México (2023). Informe sobre ciberdelitos en México.

- INEGI (2023). Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información.
- Policía Cibernética de Jalisco (2024). Informe anual de actividades.
- ONU (2019). Directrices sobre Ciberseguridad.
- Budapest Convention on Cybercrime (2001).
- Secretaría de Seguridad Pública del Estado de Jalisco (2023). Diagnóstico de criminalidad digital.
- López, J. (2022). "El delito en línea: una mirada desde la criminología digital". Revista Mexicana de Derecho Penal.
- Asociación Mexicana de Ciberseguridad (2023). Reporte Nacional de Riesgos Digitales.
- Comisión Nacional de Seguridad (2022). Estrategia Nacional de Ciberseguridad.