PODER LEGISLATIVO DEL ESTADO DE BAJA CALIFORNIA
XXV LEGISLATURA

DIP. JORGE RAMOS HERNÁNDEZ

Presidente de la Comisión de Seguridad Ciudadana y Protección Civil de la H. XXV Legislatura del Estado de Baja California

2354

"2025, Año del Turismo Sostenible como Impulsor del Bienestar Social y Progreso"

DEPENDENCIA	CONGRESO DEL ESTADO
SECCIÓN	DIPUTADOS
No. DE OFICIO	**CSCyPC/JRH/ST151/2025**

PODER LEGISLATIVO DEL ESTADO DE BAJA CALIFORNIA XXV LEGISLATURA
RECIBIDO
02 SEP 2025
14:59 hrs
OFICIALIA DE PARTES

DIP. JAIME EDUARDO CANTÓN ROCHA
PRESIDENTE DE LA MESA DIRECTIVA
DEL CONGRESO DEL ESTADO.
Presente:

Por medio del presente y anteponiendo un cordial saludo, le solicito atentamente se giren las instrucciones necesarias al personal de la dirección a su digno cargo, para que sea incluido en el orden del día de la Sesión Ordinaria de Pleno, a realizarse el día jueves veintiocho de mayo del año en curso, una **INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE REFORMA Y SE ADICIONA EL CÓDIGO PENAL PARA EL ESTADOS DE BAJA CALIFORNIA EN MATERIA DE DELITOS CIBERNÉTICOS TECNOLÓGICOS,** El objetivo es establecer un marco jurídico integral para la prevención, investigación y sanción de delitos cibernéticos.

Sin más por el momento y agradeciendo de antemano la atención que brinde al presente, me despido de Usted reiterándole mi distinguida consideración y respeto.

A T E N T A M E N T E
Mexicali, B.C. a 19 de agosto de 2025

DIP. JORGE RAMOS HERNÁNDEZ
Diputado Local de la H. XXV Legislatura
de Baja California

PODER LEGISLATIVO DEL ESTADO DE BAJA CALIFORNIA XXV LEGISLATURA
DESPACHADO
02 SEP 2025
DIP. JORGE RAMOS HERNÁNDEZ
DIPUTADO LOCAL DE LA XV LEGISLATURA
DEL ESTADO DE BAJA CALIFORNIA

DIP. JAIME EDUARDO CANTÓN ROCHA
PRESIDENTE DE LA MESA DIRECTIVA
DEL CONGRESO DEL ESTADO.
HONORABLE ASAMBLEA:

El suscrito **DIPUTADO JORGE RAMOS HERNÁNDEZ**, Presidente de la Comisión de Seguridad Ciudadana y Protección Civil, con fundamento en los Artículos 27 y 28, ambos en su fracción I, de la Constitución Política del Estado Libre y Soberano de Baja California, así como por los Artículos 110 fracción II, 115 fracción I, 116, 117 y 118 de la Ley Orgánica del Poder Legislativo del Estado de Baja California, comparecemos ante esta Soberanía para presentar **INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE REFORMA Y ADICIONA EL CÓDIGO PENAL PARA EL ESTADO DE BAJA CALIFORNIA EN MATERIA DE DELITOS CIBERNÉTICOS Y TECNOLÓGICOS** al tenor de la siguiente

EXPOSICIÓN DE MOTIVOS

I. PLANTEAMIENTO DEL PROBLEMA

El desarrollo exponencial de las tecnologías de la información y comunicación (TICs) ha transformado radicalmente la sociedad bajacaliforniana, generando nuevas formas de interacción social, económica y gubernamental. Sin embargo, este avance tecnológico ha traído consigo la aparición de modalidades delictivas que aprovechan el ciberespacio para vulnerar bienes jurídicos fundamentales como la privacidad, el patrimonio, la seguridad pública y la integridad de las personas.

Según el diagnóstico sobre delitos cibernéticos presentado por la Secretaría de Gobernación en 2024, México registra uno de cada dos ataques cibernéticos dirigidos a Latinoamérica, con millones de intentos de intrusión mensualmente. El Instituto Nacional de Estadística y Geografía (INEGI) reporta que el 79.5% de la población mexicana mayor

de 12 años utiliza internet, y de este universo, 20.8% ha sido víctima de ciberacoso, equivalente a 17.4 millones de personas, siendo las mujeres las más afectadas con 9.8 millones de víctimas.

En Baja California, la alta conectividad digital y la proximidad con Estados Unidos intensifican estos riesgos. La entidad se posiciona como uno de los estados con mayor penetración tecnológica del país, lo que la convierte en un objetivo atractivo para la ciberdelincuencia transnacional.

II. MARCO NORMATIVO ACTUAL Y SUS LIMITACIONES

El Código Penal vigente para el Estado de Baja California, publicado en 1989 y reformado por última vez en julio de 2025, carece de un marco integral para la tipificación y sanción de delitos cibernéticos. Esta omisión legislativa genera lagunas normativas que permiten la impunidad de conductas delictivas que utilizan medios tecnológicos para su comisión.

Actualmente, la persecución de estos ilícitos se basa en la aplicación analógica de tipos penales tradicionales, lo que contraviene el principio de legalidad establecido en el artículo 1° del propio código, que establece: "Nadie podrá ser sancionado por acciones u omisiones, si no están expresamente previstas como delito por las leyes vigentes."

III. DERECHO COMPARADO

A. Marco Federal Mexicano

El Código Penal Federal incorporó desde 1999 disposiciones específicas sobre delitos informáticos, estableciendo en el Título Noveno, Capítulo II, los delitos de "Acceso Ilícito a Sistemas y Equipos de Informática" (artículos 211 bis 1 al 211 bis 7). Estas disposiciones sancionan conductas como:

- Acceso no autorizado a sistemas informáticos
- Modificación, destrucción o pérdida de información

- Interceptación de comunicaciones privadas
- Ataques a sistemas del Estado

B. Convenio de Budapest sobre Ciberdelincuencia

El Convenio sobre Ciberdelincuencia de Budapest, adoptado en 2001 y vigente desde 2004, constituye el primer tratado internacional específico para combatir delitos informáticos. Este instrumento establece estándares internacionales para la tipificación de diez categorías fundamentales de ciberdelitos: acceso ilícito, interceptación ilícita, ataque a la integridad de datos, ataques a la integridad del sistema, abuso de dispositivos, falsificación informática, fraude informático, delitos relacionados con pornografía infantil e infracciones a la propiedad intelectual.

Actualmente 65 estados son partes del Convenio, incluyendo países latinoamericanos como Colombia, Costa Rica, Panamá, República Dominicana, Perú, Paraguay, Chile y Argentina. México mantiene estatus de observador pero no se ha adherido formalmente.

C. Experiencias Estatales en México

Catorce entidades federativas han incorporado delitos informáticos en sus códigos penales: Aguascalientes, Baja California Sur, Chiapas, Ciudad de México, Coahuila, Durango, Guerrero, Estado de México, Michoacán, Nuevo León, Oaxaca, Puebla, Querétaro y Veracruz.

La Ciudad de México destaca por su marco integral, que incluye disposiciones sobre espionaje cibernético, ataques a comunicaciones, violación de correspondencia digital y violencia digital de género.

IV. SUSTENTO ACADÉMICO

La doctrina penal contemporánea reconoce la necesidad imperiosa de adaptar los sistemas normativos a las realidades tecnológicas. El profesor Carlos Romeo Casabona, autoridad en derecho penal informático, señala que "la especificidad del medio cibernético requiere de tipos penales específicos que consideren las particularidades técnicas y la naturaleza transnacional de estas conductas."

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) define los delitos informáticos como "cualquier conducta ilegal, no ética o no autorizada, que involucra el procesamiento automatizado de datos y/o la transmisión de datos."

V. BIENES JURÍDICOS PROTEGIDOS

La presente reforma busca proteger los siguientes bienes jurídicos fundamentales:

1. **Confidencialidad de la información**: Protección contra accesos no autorizados
2. **Integridad de datos**: Preservación contra alteraciones maliciosas
3. **Disponibilidad de sistemas**: Garantía de funcionamiento de infraestructuras críticas
4. **Privacidad digital**: Protección de datos personales y comunicaciones
5. **Patrimonio**: Defensa contra fraudes y estafas cibernéticas
6. **Dignidad humana**: Prevención de violencia digital y ciberacoso
7. **Seguridad pública**: Protección de infraestructuras críticas estatales

VI. PRINCIPIOS RECTORES DE LA REFORMA

La iniciativa se fundamenta en los siguientes principios:

1. **Principio de Legalidad**: Tipificación expresa y detallada de las conductas
2. **Principio de Proporcionalidad**: Sanciones acordes a la lesividad social
3. **Principio de Especialidad**: Regulación específica para medios tecnológicos
4. **Principio de Tecnología Neutral**: Normas aplicables independientemente del tipo de tecnología
5. **Principio de Protección de Derechos Fundamentales**: Equilibrio entre seguridad y derechos humanos

VII. OBJETIVOS DE LA REFORMA

1. Establecer un marco jurídico integral para la prevención, investigación y sanción de delitos cibernéticos
2. Armonizar la legislación estatal con estándares federales e internacionales
3. Proporcionar herramientas jurídicas efectivas para la procuración de justicia
4. Proteger a la ciudadanía bajacaliforniana contra nuevas formas de criminalidad
5. Fortalecer la cooperación interinstitucional en materia de ciberseguridad

VIII. IMPACTO SOCIAL Y ECONÓMICO

La implementación de esta reforma generará beneficios significativos:

- **Seguridad Jurídica**: Claridad normativa para ciudadanos, empresas y autoridades
- **Confianza Digital**: Fortalecimiento del ecosistema digital estatal
- **Atracción de Inversiones**: Mejora del clima de negocios tecnológicos
- **Protección de Derechos**: Salvaguarda efectiva de derechos fundamentales
- **Competitividad Regional**: Posicionamiento como estado líder en marco jurídico tecnológico

Se presenta un cuadro comparativo entre el texto vigente y el que se propone:

TEXTO VIGENTE	TEXTO PROPUESTO
ARTÍCULO 6.- Principio de territorialidad y extraterritorialidad de la Ley penal. - Este Código se aplicará por los delitos que se cometan en el Estado de Baja California y sean de la competencia de sus Tribunales. Asimismo, por los que se inicien, preparen o cometan en otra	ARTÍCULO 6.- ...

Entidad Federativa cuando sus efectos se produzcan en el territorio del Estado; y por los delitos continuados o permanentes, cuando en un momento cualquiera de su ejecución éstos se realicen dentro del citado territorio.	
Las conductas previstas en el capítulo II de la Ley General para Prevenir y Sancionar los Delitos en materia de Secuestro, reglamentaria de la fracción XXI del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, tendrán el carácter de delitos para los efectos de este Código, siempre que se colme el supuesto del artículo 23, párrafo segundo de dicha ley general.	...
	Para los delitos cibernéticos y tecnológicos, se aplicará este Código cuando: **I. El sujeto activo se encuentre en territorio del Estado al momento de la comisión del delito;** **II. El sujeto pasivo sea residente del Estado y el delito afecte sus derechos o intereses;** **III. Los sistemas, equipos o datos informáticos objeto del delito se**

	encuentren total o parcialmente en el Estado; **IV. Los efectos del delito se produzcan en territorio estatal; o** **V. Se utilicen sistemas o infraestructuras ubicadas en el Estado para la comisión del delito, aun cuando los sujetos se encuentren en otro lugar.**
ARTÍCULO 97.- Causas de Extinción. - Son causas de Extinción de la acción penal y de la potestad de ejecutar las penas y medidas de seguridad impuestas, las siguientes:	ARTÍCULO 97.- …
I.- Cumplimiento de la pena o medida de seguridad; II.- Muerte del imputado o sentenciado; III.- Amnistía; IV.- Reconocimiento de la inocencia del sentenciado; V.- Perdón del ofendido en los delitos de querella; VI.- Rehabilitación; VII.- Indulto;	I.- a VII.- …
VIII.- Prescripción; y	VIII.- Prescripción;
IX.- El cumplimiento del criterio de oportunidad, así como el debido	IX.- El cumplimiento del criterio de oportunidad, así como el debido

cumplimiento de la solución alterna correspondiente; y,	cumplimiento de la solución alterna correspondiente;
X.- Las demás que se establezcan en la ley.	**X.- En delitos cibernéticos, la reparación integral del daño, el otorgamiento de garantías de no repetición y la implementación de medidas de seguridad tecnológica cuando así lo determine la autoridad judicial; y**
	XI.- Las demás que se establezcan en la ley.
Sin correlativo	**TÍTULO OCTAVO** **DELITOS CIBERNÉTICOS Y TECNOLÓGICOS** **CAPÍTULO I** **DISPOSICIONES GENERALES** **ARTÍCULO 359.- Definiciones. - Para efectos de este Título se entenderá por:** **I. Sistema informático: Dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, que mediante un programa realizan el tratamiento automatizado de datos digitales;** **II. Datos informáticos: Cualquier representación de hechos, información o conceptos expresados de manera**

	que puedan ser procesados por un sistema informático, incluidos programas destinados a que un sistema informático ejecute una función; **III. Proveedor de servicios: Entidad pública o privada que ofrece a los usuarios de sus servicios la posibilidad de comunicarse por medio de un sistema informático;** **IV. Datos de tráfico: Datos informáticos relacionados con una comunicación efectuada por medio de un sistema informático, generados por este último como elemento de la cadena de comunicación, que indican el origen, destino, ruta, hora, fecha, tamaño, duración o tipo de servicio subyacente;** **V. Dispositivos: Programas informáticos, contraseñas, códigos de acceso o datos similares por medio de los cuales puede accederse total o parcialmente a un sistema informático;** **VI. Ciberacoso: Uso de medios electrónicos para molestar, humillar, avergonzar, amenazar o intimidar a una persona de manera reiterada;**

	VII. Violencia digital: Actos de acoso, hostigamiento, amenazas, vulneración de datos e información privada, así como la publicación de información, datos, imágenes reales o simuladas de contenido íntimo sexual sin consentimiento; **VIII. Inteligencia artificial: Sistema tecnológico que utiliza algoritmos avanzados para simular procesos de inteligencia humana como aprendizaje, razonamiento y autocorrección.** **ARTÍCULO 360.- Querella necesaria. - Los delitos previstos en este Título se perseguirán por querella, salvo que la víctima sea menor de edad, carezca de capacidad para comprender el significado del hecho o no tenga capacidad para resistirlo.** **CAPÍTULO II** **ACCESO ILÍCITO Y ATAQUES A SISTEMAS** **ARTÍCULO 361.- Acceso ilícito a sistemas informáticos. - Al que sin autorización acceda de manera intencional a un sistema informático protegido por medidas de seguridad, se le impondrán de seis meses a dos**

	años de prisión y de cien a trescientos días multa. **Las penas se aumentarán hasta en una mitad cuando:** **I. Se obtenga información del sistema;** **II. El acceso se realice a sistema informático de carácter gubernamental, financiero, de salud o de seguridad pública;** **III. Se ponga en riesgo la seguridad nacional, la seguridad pública o la economía del Estado; o** **IV. Se cometa el delito con fines lucrativos.** **ARTÍCULO 362.- Interceptación ilícita. - Al que de manera intencional e ilegítima intercepte transmisiones no públicas de datos informáticos dirigidos a un sistema informático, que procedan de él o que se den dentro del mismo, incluidas las emisiones electromagnéticas de un sistema informático que contengan tales datos, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.**

	ARTÍCULO 363.- Ataque a la integridad de datos. - Al que de manera intencional e ilegítima dañe, borre, deteriore, altere o suprima datos informáticos, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. **Las penas se aumentarán hasta en una mitad cuando los datos correspondan a sistemas gubernamentales, de seguridad pública, financieros o de salud.** **ARTÍCULO 364.- Ataque a la integridad del sistema. - Al que de manera intencional e ilegítima obstaculice gravemente, sin derecho, el funcionamiento de un sistema informático introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando o suprimiendo datos informáticos, se le impondrán de uno a cuatro años de prisión y de trescientos a novecientos días multa.** **CAPÍTULO III** **DELITOS PATRIMONIALES CIBERNÉTICOS**

	ARTÍCULO 365.- Fraude informático. - Al que con ánimo de lucro y para causar un perjuicio patrimonial a otro, influya en el procesamiento o funcionamiento de un sistema informático mediante la introducción, alteración, borrado o supresión de datos informáticos o por cualquier interferencia en el funcionamiento de un sistema informático, consiguiendo así una transferencia no autorizada de bienes, se le impondrán de tres a diez años de prisión y multa de quinientos a mil días. **ARTÍCULO 366.- Falsificación informática. - Al que introduzca, altere, borre o suprima de manera ilegítima datos informáticos que den lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, independientemente de si los datos son directamente legibles e inteligibles o no, se le impondrán de seis meses a cinco años de prisión y de ciento cincuenta a setecientos cincuenta días multa.**

	ARTÍCULO 367.- Estafa mediante comercio electrónico. - Al que, por medio de sistemas de comercio electrónico, páginas web o plataformas digitales simule la venta de bienes o servicios inexistentes o diferentes a los ofrecidos, con el propósito de obtener un beneficio económico ilícito, se le impondrán de dos a ocho años de prisión y multa de trescientos a mil días. **CAPÍTULO IV** **DELITOS CONTRA LA PRIVACIDAD Y DATOS PERSONALES** **ARTÍCULO 368.- Acceso no autorizado a datos personales.- Al que sin consentimiento de su titular y de manera ilegítima obtenga, copie, use, modifique o divulgue información clasificada como datos personales, se le impondrán de uno a cinco años de prisión y de doscientos a setecientos días multa.** **Las penas se aumentarán hasta en una mitad cuando se trate de datos personales sensibles.** **ARTÍCULO 369.- Revelación de secretos informáticos.- Al que teniendo**

	conocimiento de secretos o información confidencial de una persona por razón de su actividad profesional o laboral, los divulgue sin consentimiento mediante sistemas informáticos, se le impondrán de dos a cinco años de prisión, multa de trescientos a setecientos días y suspensión para ejercer su profesión hasta por tres años. **ARTÍCULO 370.- Violación de comunicaciones privadas digitales.- Al que de manera dolosa intercepte, grabe, reproduzca, divulgue o aproveche sin consentimiento comunicaciones privadas realizadas por medios electrónicos, digitales o telemáticos, se le impondrán de tres a ocho años de prisión y de quinientos a mil días multa.** **CAPÍTULO V** **VIOLENCIA DIGITAL Y CIBERACOSO** **ARTÍCULO 371.- Ciberacoso.- Al que utilizando medios electrónicos, digitales o cualquier tecnología de la información y comunicación, de manera reiterada contacte, persiga, vigile, amenace o moleste a una**

	persona sin su consentimiento, afectando su tranquilidad, libertad o seguridad, se le impondrán de dos a cuatro años de prisión y de trescientos a ochocientos días multa. **ARTÍCULO 372.- Violación a la intimidad sexual digital.- Al que sin consentimiento divulgue, distribuya, publique, reproduzca, transmita, comercialice o ponga a disposición de terceros imágenes, audios o videos con contenido sexual íntimo de una persona identificable por cualquier medio tecnológico, se le impondrán de tres a seis años de prisión y de quinientos a mil días multa.** **Las penas se aumentarán hasta en una mitad cuando:** **I. Las imágenes o videos hayan sido obtenidos en una relación de confianza;** **II. Exista o haya existido una relación de pareja, matrimonio, concubinato o de parentesco entre el activo y la víctima;** **III. Se obtenga un beneficio económico; o**

	IV. La víctima sea menor de edad. **ARTÍCULO 373.- Sextorsión.- Al que amenace con difundir material de contenido sexual íntimo de una persona para obtener dinero, información, contacto sexual, material sexual adicional o cualquier beneficio, se le impondrán de cuatro a ocho años de prisión y de seiscientos a mil doscientos días multa.** **CAPÍTULO VI** **DELITOS CONTRA MENORES EN ENTORNOS DIGITALES** **ARTÍCULO 374.- Contacto sexual con menor mediante tecnología.- Al mayor de edad que por cualquier medio tecnológico contacte a una persona menor de dieciocho años de edad y le solicite realizar conductas sexuales, se le impondrán de tres a seis años de prisión y de quinientos a mil días multa.** **ARTÍCULO 375.- Pornografía infantil digital.- Al que produzca, distribuya, promueva, publicite, transmita, importe, exporte, comercialice, posea o almacene por cualquier medio material que represente a menores de dieciocho años en conductas sexuales explícitas,**

	reales o simuladas, se le impondrán de siete a doce años de prisión y de mil a dos mil días multa. **ARTÍCULO 376.- Grooming.- Al que por cualquier medio tecnológico contacte a un menor de edad con el propósito de ganar su confianza para posteriormente obtener material sexual, concertar encuentros o realizar conductas de naturaleza sexual, se le impondrán de cinco a diez años de prisión y de ochocientos a mil quinientos días multa.** **CAPÍTULO VII** **DELITOS CONTRA LA SEGURIDAD PÚBLICA DIGITAL** **ARTÍCULO 377.- Ataques a infraestructura crítica.- Al que dañe, destruya, altere o inutilice sistemas informáticos de infraestructura crítica del Estado, se le impondrán de cinco a quince años de prisión y de mil a tres mil días multa.** **ARTÍCULO 378.- Terrorismo cibernético.- Al que utilice sistemas informáticos para realizar actos destinados a perturbar la paz pública, atemorizar a la población o presionar a**

	las autoridades para que tomen una determinación, se le impondrán de diez a cuarenta años de prisión y de dos mil a cinco mil días multa. **ARTÍCULO 379.- Sabotaje informático.- Al que de manera intencional cause interrupción o entorpecimiento de un sistema informático introduciendo, transmitiendo o activando virus, programas maliciosos o cualquier código destinado a causar daños, se le impondrán de dos a seis años de prisión y de cuatrocientos a mil días multa.** **CAPÍTULO VIII** **DELITOS EMERGENTES CON INTELIGENCIA ARTIFICIAL** **ARTÍCULO 380.- Deepfakes maliciosos.- Al que utilice inteligencia artificial para crear, distribuir o poseer material audiovisual falso que simule la participación de una persona identificable en actos que no realizó, con propósito de dañar su reputación, obtener beneficio ilícito o causar perjuicio, se le impondrán de uno a cinco años de prisión y de doscientos a ochocientos días multa.**

	Las penas se aumentarán hasta en una mitad cuando el material simule contenido sexual. **ARTÍCULO 381.- Uso ilícito de sistemas de inteligencia artificial. - Al que utilice sistemas de inteligencia artificial para cometer cualquier delito previsto en este Código, las penas correspondientes se aumentarán hasta en una tercera parte.** **CAPÍTULO IX** **DISPOSICIONES COMUNES** **ARTÍCULO 382.- Agravantes generales.- Las penas previstas en este Título se aumentarán hasta en una mitad cuando:** **I. El sujeto activo sea servidor público y cometa el delito en ejercicio de sus funciones, o cuente con título profesional en materias relacionadas con las tecnologías de la información y las comunicaciones;** **II. Se trate de delincuencia organizada;** **III. La víctima sea menor de edad, adulto mayor, persona con discapacidad o pertenezca a un grupo en situación de vulnerabilidad;**

	IV. Se cause daño patrimonial superior a mil veces la Unidad de Medida y Actualización; o **V. Se ponga en riesgo la seguridad nacional o la seguridad pública.** **ARTÍCULO 383.- Equipos y programas.- Al que produzca, comercialice, importe, distribuya o ponga de cualquier modo a disposición de terceros dispositivos, programas informáticos, contraseñas, códigos de acceso o cualquier dato similar diseñados o adaptados principalmente para permitir la comisión de los delitos previstos en este Título, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.** **ARTÍCULO 384.- Tentativa.- La tentativa de los delitos previstos en este Título será sancionada conforme a las reglas generales establecidas en los artículos 80 y 81 de este Código.** **ARTÍCULO 385.- Medidas de seguridad.- Además de las penas previstas, el juzgador podrá imponer al sentenciado:**

	I. Decomiso de los equipos e instrumentos utilizados para la comisión del delito; **II. Prohibición de acceso o uso de sistemas informáticos, redes sociales o tecnologías específicas hasta por el tiempo de duración de la pena;** **III. Tratamiento especializado en el uso responsable de tecnologías;** **IV. Prestación de servicios comunitarios relacionados con la promoción del uso seguro de tecnologías;** **y V. Reparación integral del daño que incluya medidas de rehabilitación, restitución, compensación, satisfacción y garantías de no repetición.**

Por lo anteriormente expuesto y con fundamento en lo dispuesto por los artículos 27 y 28 ambos en su fracción I de la Constitución Política del Estado Libre y Soberano de Baja California, así como por los artículos 110 fracción II, 115 fracción I, 116, 117 y 118 y demás relativos y aplicables de la Ley Orgánica del Poder Legislativo del Estado de Baja California, me permito someter a consideración de esta H. Legislatura del Congreso del Estado de Baja California la presente iniciativa con proyecto de:

DECRETO

ARTÍCULO PRIMERO. Se reforman los artículos 6 y 97 del Código Penal para el Estado de Baja California para quedar como sigue:

ARTÍCULO 6.- ...

...

Para los delitos cibernéticos y tecnológicos, se aplicará este Código cuando:

I. El sujeto activo se encuentre en territorio del Estado al momento de la comisión del delito;

II. El sujeto pasivo sea residente del Estado y el delito afecte sus derechos o intereses;

III. Los sistemas, equipos o datos informáticos objeto del delito se encuentren total o parcialmente en el Estado;

IV. Los efectos del delito se produzcan en territorio estatal; o

V. Se utilicen sistemas o infraestructuras ubicadas en el Estado para la comisión del delito, aun cuando los sujetos se encuentren en otro lugar.

ARTÍCULO 97.- ...

I.- a VII.- ...

VIII.- Prescripción;

IX.- El cumplimiento del criterio de oportunidad, así como el debido cumplimiento de la solución alterna correspondiente;

X.- En delitos cibernéticos, la reparación integral del daño, el otorgamiento de garantías de no repetición y la implementación de medidas de seguridad tecnológica cuando así lo determine la autoridad judicial; y

XI.- Las demás que se establezcan en la ley.

ARTÍCULO SEGUNDO. Se adicionan un Título Octavo con diez Capítulos y los artículos 359 a 385 al Código Penal para el Estado de Baja California para quedar como sigue:

TÍTULO OCTAVO

DELITOS CIBERNÉTICOS Y TECNOLÓGICOS

CAPÍTULO I

DISPOSICIONES GENERALES

ARTÍCULO 359.- Definiciones.- Para efectos de este Título se entenderá por:

I. Sistema informático: Dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, que mediante un programa realizan el tratamiento automatizado de datos digitales;

II. Datos informáticos: Cualquier representación de hechos, información o conceptos expresados de manera que puedan ser procesados por un sistema informático, incluidos programas destinados a que un sistema informático ejecute una función;

III. Proveedor de servicios: Entidad pública o privada que ofrece a los usuarios de sus servicios la posibilidad de comunicarse por medio de un sistema informático;

IV. Datos de tráfico: Datos informáticos relacionados con una comunicación efectuada por medio de un sistema informático, generados por este último como elemento de la cadena de comunicación, que indican el origen, destino, ruta, hora, fecha, tamaño, duración o tipo de servicio subyacente;

V. Dispositivos: Programas informáticos, contraseñas, códigos de acceso o datos similares por medio de los cuales puede accederse total o parcialmente a un sistema informático;

VI. Ciberacoso: Uso de medios electrónicos para molestar, humillar, avergonzar, amenazar o intimidar a una persona de manera reiterada;

VII. Violencia digital: Actos de acoso, hostigamiento, amenazas, vulneración de datos e información privada, así como la publicación de información, datos, imágenes reales o simuladas de contenido íntimo sexual sin consentimiento;

VIII. Inteligencia artificial: Sistema tecnológico que utiliza algoritmos avanzados para simular procesos de inteligencia humana como aprendizaje, razonamiento y autocorrección.

ARTÍCULO 360.- Querella necesaria.- Los delitos previstos en este Título se perseguirán por querella, salvo que la víctima sea menor de edad, carezca de capacidad para comprender el significado del hecho o no tenga capacidad para resistirlo.

CAPÍTULO II

ACCESO ILÍCITO Y ATAQUES A SISTEMAS

ARTÍCULO 361.- Acceso ilícito a sistemas informáticos.- Al que sin autorización acceda de manera intencional a un sistema informático protegido por medidas de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Las penas se aumentarán hasta en una mitad cuando:

I. Se obtenga información del sistema;

II. El acceso se realice a sistema informático de carácter gubernamental, financiero, de salud o de seguridad pública;

III. Se ponga en riesgo la seguridad nacional, la seguridad pública o la economía del Estado; o

IV. Se cometa el delito con fines lucrativos.

ARTÍCULO 362.- Interceptación ilícita.- Al que de manera intencional e ilegítima intercepte transmisiones no públicas de datos informáticos dirigidos a un sistema informático, que procedan de él o que se den dentro del mismo, incluidas las emisiones electromagnéticas de un sistema informático que contengan tales datos, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

ARTÍCULO 363.- Ataque a la integridad de datos.- Al que de manera intencional e ilegítima dañe, borre, deteriore, altere o suprima datos informáticos, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Las penas se aumentarán hasta en una mitad cuando los datos correspondan a sistemas gubernamentales, de seguridad pública, financieros o de salud.

ARTÍCULO 364.- Ataque a la integridad del sistema.- Al que de manera intencional e ilegítima obstaculice gravemente, sin derecho, el funcionamiento de un sistema informático introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando o suprimiendo datos informáticos, se le impondrán de uno a cuatro años de prisión y de trescientos a novecientos días multa.

CAPÍTULO III

DELITOS PATRIMONIALES CIBERNÉTICOS

ARTÍCULO 365.- Fraude informático.- Al que con ánimo de lucro y para causar un perjuicio patrimonial a otro, influya en el procesamiento o funcionamiento de un sistema informático mediante la introducción, alteración, borrado o supresión de datos informáticos o por cualquier interferencia en el funcionamiento de un sistema informático, consiguiendo así una transferencia no autorizada de bienes, se le impondrán de tres a diez años de prisión y multa de quinientos a mil días.

ARTÍCULO 366.- Falsificación informática.- Al que introduzca, altere, borre o suprima de manera ilegítima datos informáticos que den lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, independientemente de si los datos son directamente legibles e inteligibles o no, se le impondrán de seis meses a cinco años de prisión y de ciento cincuenta a setecientos cincuenta días multa.

ARTÍCULO 367.- Estafa mediante comercio electrónico.- Al que por medio de sistemas de comercio electrónico, páginas web o plataformas digitales simule la venta de bienes o servicios inexistentes o diferentes a los ofrecidos, con el propósito de obtener un beneficio económico ilícito, se le impondrán de dos a ocho años de prisión y multa de trescientos a mil días.

CAPÍTULO IV

DELITOS CONTRA LA PRIVACIDAD Y DATOS PERSONALES

ARTÍCULO 368.- Acceso no autorizado a datos personales.- Al que sin consentimiento de su titular y de manera ilegítima obtenga, copie, use, modifique o divulgue información clasificada como datos personales, se le impondrán de uno a cinco años de prisión y de doscientos a setecientos días multa.

Las penas se aumentarán hasta en una mitad cuando se trate de datos personales sensibles.

ARTÍCULO 369.- Revelación de secretos informáticos.- Al que teniendo conocimiento de secretos o información confidencial de una persona por razón de su actividad profesional o laboral, los divulgue sin consentimiento mediante sistemas informáticos, se le impondrán de dos a cinco años de prisión, multa de trescientos a setecientos días y suspensión para ejercer su profesión hasta por tres años.

ARTÍCULO 370.- Violación de comunicaciones privadas digitales.- Al que de manera dolosa intercepte, grabe, reproduzca, divulgue o aproveche sin consentimiento comunicaciones privadas realizadas por medios electrónicos, digitales o telemáticos, se le impondrán de tres a ocho años de prisión y de quinientos a mil días multa.

CAPÍTULO V

VIOLENCIA DIGITAL Y CIBERACOSO

ARTÍCULO 371.- Ciberacoso.- Al que utilizando medios electrónicos, digitales o cualquier tecnología de la información y comunicación, de manera reiterada contacte, persiga, vigile, amenace o moleste a una persona sin su consentimiento, afectando su tranquilidad, libertad o seguridad, se le impondrán de dos a cuatro años de prisión y de trescientos a ochocientos días multa.

ARTÍCULO 372.- Violación a la intimidad sexual digital.- Al que sin consentimiento divulgue, distribuya, publique, reproduzca, transmita, comercialice o ponga a disposición de terceros imágenes, audios o videos con contenido sexual íntimo de una persona

identificable por cualquier medio tecnológico, se le impondrán de tres a seis años de prisión y de quinientos a mil días multa.

Las penas se aumentarán hasta en una mitad cuando:

I. Las imágenes o videos hayan sido obtenidos en una relación de confianza;

II. Exista o haya existido una relación de pareja, matrimonio, concubinato o de parentesco entre el activo y la víctima;

III. Se obtenga un beneficio económico; o

IV. La víctima sea menor de edad.

ARTÍCULO 373.- Sextorsión.- Al que amenace con difundir material de contenido sexual íntimo de una persona para obtener dinero, información, contacto sexual, material sexual adicional o cualquier beneficio, se le impondrán de cuatro a ocho años de prisión y de seiscientos a mil doscientos días multa.

CAPÍTULO VI

DELITOS CONTRA MENORES EN ENTORNOS DIGITALES

ARTÍCULO 374.- Contacto sexual con menor mediante tecnología.- Al mayor de edad que por cualquier medio tecnológico contacte a una persona menor de dieciocho años de edad y le solicite realizar conductas sexuales, se le impondrán de tres a seis años de prisión y de quinientos a mil días multa.

ARTÍCULO 375.- Pornografía infantil digital.- Al que produzca, distribuya, promueva, publicite, transmita, importe, exporte, comercialice, posea o almacene por cualquier medio material que represente a menores de dieciocho años en conductas sexuales explícitas, reales o simuladas, se le impondrán de siete a doce años de prisión y de mil a dos mil días multa.

ARTÍCULO 376.- Grooming.- Al que por cualquier medio tecnológico contacte a un menor de edad con el propósito de ganar su confianza para posteriormente obtener material

sexual, concertar encuentros o realizar conductas de naturaleza sexual, se le impondrán de cinco a diez años de prisión y de ochocientos a mil quinientos días multa.

CAPÍTULO VII

DELITOS CONTRA LA SEGURIDAD PÚBLICA DIGITAL

ARTÍCULO 377.- Ataques a infraestructura crítica.- Al que dañe, destruya, altere o inutilice sistemas informáticos de infraestructura crítica del Estado, se le impondrán de cinco a quince años de prisión y de mil a tres mil días multa.

ARTÍCULO 378.- Terrorismo cibernético.- Al que utilice sistemas informáticos para realizar actos destinados a perturbar la paz pública, atemorizar a la población o presionar a las autoridades para que tomen una determinación, se le impondrán de diez a cuarenta años de prisión y de dos mil a cinco mil días multa.

ARTÍCULO 379.- Sabotaje informático.- Al que de manera intencional cause interrupción o entorpecimiento de un sistema informático introduciendo, transmitiendo o activando virus, programas maliciosos o cualquier código destinado a causar daños, se le impondrán de dos a seis años de prisión y de cuatrocientos a mil días multa.

CAPÍTULO VIII

DELITOS EMERGENTES CON INTELIGENCIA ARTIFICIAL

ARTÍCULO 380.- Deepfakes maliciosos.- Al que utilice inteligencia artificial para crear, distribuir o poseer material audiovisual falso que simule la participación de una persona identificable en actos que no realizó, con propósito de dañar su reputación, obtener beneficio ilícito o causar perjuicio, se le impondrán de uno a cinco años de prisión y de doscientos a ochocientos días multa.

Las penas se aumentarán hasta en una mitad cuando el material simule contenido sexual.

ARTÍCULO 381.- Uso ilícito de sistemas de inteligencia artificial.- Al que utilice sistemas de inteligencia artificial para cometer cualquier delito previsto en este Código, las penas correspondientes se aumentarán hasta en una tercera parte.

CAPÍTULO IX

DISPOSICIONES COMUNES

ARTÍCULO 382.- Agravantes generales.- Las penas previstas en este Título se aumentarán hasta en una mitad cuando:

I. El sujeto activo sea servidor público y cometa el delito en ejercicio de sus funciones, o cuente con título profesional en materias relacionadas con las tecnologías de la información y las comunicaciones;

II. Se trate de delincuencia organizada;

III. La víctima sea menor de edad, adulto mayor, persona con discapacidad o pertenezca a un grupo en situación de vulnerabilidad;

IV. Se cause daño patrimonial superior a mil veces la Unidad de Medida y Actualización; o

V. Se ponga en riesgo la seguridad nacional o la seguridad pública.

ARTÍCULO 383.- Equipos y programas. - Al que produzca, comercialice, importe, distribuya o ponga de cualquier modo a disposición de terceros dispositivos, programas informáticos, contraseñas, códigos de acceso o cualquier dato similar diseñados o adaptados principalmente para permitir la comisión de los delitos previstos en este Título, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

ARTÍCULO 384.- Tentativa. - La tentativa de los delitos previstos en este Título será sancionada conforme a las reglas generales establecidas en los artículos 80 y 81 de este Código.

ARTÍCULO 385.- Medidas de seguridad. - Además de las penas previstas, el juzgador podrá imponer al sentenciado:

I. Decomiso de los equipos e instrumentos utilizados para la comisión del delito;

II. Prohibición de acceso o uso de sistemas informáticos, redes sociales o tecnologías específicas hasta por el tiempo de duración de la pena;

III. Tratamiento especializado en el uso responsable de tecnologías;

IV. Prestación de servicios comunitarios relacionados con la promoción del uso seguro de tecnologías;

y V. Reparación integral del daño que incluya medidas de rehabilitación, restitución, compensación, satisfacción y garantías de no repetición.

ARTÍCULOS TRANSITORIAS

PRIMERO. El presente Decreto entrará en vigor al día siguiente de su publicación en el Periódico Oficial del Estado de Baja California.

SEGUNDO. La Fiscalía General del Estado de Baja California contará con un plazo de ciento ochenta días naturales a partir de la entrada en vigor del presente Decreto para establecer las unidades especializadas necesarias para la investigación y persecución de los delitos previstos en el Título Octavo del Código Penal.

TERCERO. El Poder Judicial del Estado implementará los programas de capacitación necesarios para jueces y magistrados en materia de delitos cibernéticos dentro de los noventa días naturales siguientes a la entrada en vigor del presente Decreto.

DADO en el Salón de Sesiones "Lic. Benito Juárez García" del H. Poder Legislativo del Estado de Baja California, en la ciudad de Mexicali, Baja California, a la fecha de su presentación.

ATENTAMENTE

DIPUTADO JORGE RAMOS HERNÁNDEZ