NUMERO
DE FOLIO

277

INICIATIVA POR LA QUE SE SE DEROGA LA FRACCIÓN IV DEL ARTÍCULO 89 Y SE ADICIONAN LA FRACCIÓN XXIX BIS AL ARTÍCULO 3, LA FRACCIÓN IX AL ARTÍCULO 85, EL ARTÍCULO 97 BIS Y EL ARTÍCULO 97 TER TODOS DE LA LEY DE SEGURIDAD CIUDADANA DEL ESTADO DE QUINTANA ROO, EN MATERIA DE POLICÍA CIBERNÉTICA.

HONORABLE XVIII LEGISLATURA DEL ESTADO LIBRE Y SOBERANO DE QUINTANA ROO.

El suscrito **Diputado Filiberto Martínez Méndez**, Presidente de la Comisión de Defensa de los Límites de Quintana Roo y Asuntos Fronterizos de la Honorable XVIII Legislatura del Estado de Quintana Roo, con fundamento en la fracción II del artículo 68 de la Constitución Política del Estado Libre y Soberano de Quintana Roo, los artículos 140 y 141 de la Ley Orgánica del Poder Legislativo y el artículo 36 del Reglamento para el Gobierno Interior del Poder Legislativo del Estado de Quintana Roo, me permito someter a la consideración de este Honorable Pleno Legislativo, la siguiente **INICIATIVA POR LA QUE SE REFORMAN Y ADICIONAN DIVERSOS ARTÍCULOS DE LA LEY DE SEGURIDAD CIUDADANA DEL ESTADO DE QUINTANA ROO.** Lo anterior al tenor de la siguiente:

RECIBIDO
21 OCT 2025

EXPOSICION DE MOTIVOS

Nuestro marco normativo desde el nivel federal hasta el municipal no debe permanecer estático, pues las condiciones sociales y la propia sociedad cambia a pasos vertiginosos, los motivos son múltiples tal es el caso de las costumbres o los avances tecnológicos, como el surgimiento de nuevas herramientas digitales, en el que desafortunadamente dicho avance trae aparejado tanto cosas buenas como problemáticas socialmente dañinas; por ello empecemos por saber que son las TIC´s, *"El concepto de Tecnologías de la Información y la Comunicación (TICs) se refiere al conjunto de herramientas que permiten la transmisión, el procesamiento y el almacenamiento de información. En este concepto se encuentran las computadoras*

y los elementos que la integran como los programas de cómputo (software) y el hardware; los teléfonos inteligentes; las tabletas; las redes como Internet; sistemas informáticos y otros."[1]

Como puede destacarse del concepto de *Tecnologías de la Información y la Comunicación (TICs)* resaltan dos aspectos importantes que requieren una definición completa y amplia, nos referimos al *software y al hardware,* para ello la Real Academia Española establece lo siguiente:

software: *"Voz inglesa que se usa, en informática, con el sentido de 'conjunto de programas, instrucciones y reglas para ejecutar ciertas tareas en una computadora u ordenador."*

hardware: *"Voz inglesa que se usa, en informática, para designar el conjunto de los componentes que integran la parte material de una computadora u ordenador."*

Una vez establecido que son y como se integran las tecnologías de la información, debemos precisar donde se emplean estas, pues se les dan diversos usos y sirven para *"... ejecutar actividades cotidianas de trabajo, educación, entretenimiento, transacciones comerciales, financieras, etcétera, y son usadas por un gran número de individuos, desde menores de edad hasta personas de la tercera edad, así como por las empresas y el gobierno. ..."*[1]

Ahora bien, sabiendo que son las TIC´s y como se usan, lo consiguientes es que el propio avance de la misma tecnología representa riesgos para las y los usuarios en todas sus modalidades, es por ello que el Instituto Universal de Capacitación Policial a través de su artículo denominado "NUEVAS TECNOLOGÍAS Y SU IMPACTO EN LA

---

[1] https://mexico.justia.com/derecho-penal/delitos-informaticos/#:~:text=Por ejemplo, un programa de cómputo será,delictiva, como cuando se insertan virus para

PREVENCIÓN DE CIBERDELINCUENCIA" refiere aspectos importantes del tema, tal como se cita a continuación:

"Las nuevas tecnologías están transformando la manera en que se enfrenta la ciberdelincuencia. Desde la inteligencia artificial hasta el análisis predictivo, estas herramientas permiten a las organizaciones anticiparse a los ataques, fortalecer sus sistemas y crear una red de seguridad digital más eficaz. La inteligencia artificial (IA) y el aprendizaje automático han cambiado el enfoque de la ciberseguridad al ofrecer capacidades avanzadas para detectar patrones y predecir comportamientos maliciosos. Estas tecnologías son capaces de analizar grandes volúmenes de datos y reconocer patrones que indican posibles ciberamenazas, como intentos de acceso no autorizados o comportamientos inusuales en la red."[2]

En la actualidad, la interacción humana, el desarrollo económico, la educación, la salud, el acceso a los servicios tanto públicos como privados, e incluso el ejercicio de derechos fundamentales como lo son la libertad de expresión, el derecho al acceso a la información o bien la interposición de demandas de acceso a la justicia, las notificaciones de acuerdos o de diversos asuntos administrativos o jurisdiccionales, pues inclusive audiencias judiciales, sesiones del pleno de la Suprema Corte de Justicia o de congresos locales, todas estas acciones ocurren en entornos digitales, otro aspecto que ya migró al avance tecnológico es la forma en que se realizan actividades económicas, como son las transacciones bancarias que antes se realizaban desde casa rigurosamente a través de una computadora de escritorio (PC´s), sin embargo hoy en día desde cualquier lugar es posible hacer estas transacciones ya sea por medio de una laptop, tableta electrónica o inclusive desde un teléfono inteligente a través de la denominada banca móvil, esto es posible gracias a diversos factores como lo son la disponibilidad de internet que se tiene en la actualidad y el desarrollo tecnológico que hizo posible que los equipos electrónicos referidos anteriormente, puedan funcionar a través de conexiones inalámbricas, sin embargo esta transformación ha traído consigo no solo estar a la vanguardia en cuanto a la tecnología, sino que también ha generado diversas amenazas y conductas

---

2 https://iucpol.com/nuevas-tecnologias-ciberdelincuencia/?srsltid=AfmBOooPyRtioHy79Vu7RHq2ztmPP36PnPtdYC40-IWhYzuLyRjgNzI3

constitutivas de delitos de los denominados "cibernéticos", ya que al estar navegando en el ciberespacio todo usuario debe contar con las medidas de seguridad digital idóneas, de lo contrario pueden ser víctimas de aquellas personas que con habilidades o conocimientos informáticos se dedican a cometer delitos cibernéticos, ya que al accesar a la información personal que se encuentra almacenada en la red, pueden suplantar cualquier identidad o inclusive sustraer los recursos económicos de sus cuentas bancarias.

En ese sentido es de mencionarse que, *"los delitos informáticos se definen como aquellos actos ilícitos en los que se usan las tecnologías de la información, como las computadoras, los programas informáticos, los medios electrónicos, el internet, entre otros, como medio o como fin. Por ejemplo, un programa de cómputo será un medio para cometer un delito cuando es utilizado para acceder sin autorización a información confidencial; ahora bien, un programa de cómputo será el fin en un delito informático cuando recaiga sobre ese programa la conducta delictiva, como cuando se insertan virus para destruir el programa."*[1]

"Aunado a ello se tiene que, las estadísticas de delitos cibernéticos a nivel mundial se muestran que un mínimo de 422 millones de personas se vieron afectadas, según los registros de delitos en Internet del FBI, con 800.944 denuncias registradas en 2022. En 2023, se violaron 33 mil millones de cuentas , lo que equivale a 2328 al día y 97 víctimas de ciberdelitos por hora. Se registraron un total de 800 000 ciberataques y, en promedio, se produce un ataque cada 39 segundos, lo que representa un aumento considerable en 2025."[3]

"Asimismo, la Organización de las Naciones Unidas ha considerado que los delitos informáticos implican grandes retos para todos los Estados, toda vez que tienen lugar en el ciberespacio, y los delincuentes y las víctimas pueden encontrarse en cualquier parte del mundo."[4]

---

[3] https://www.getastra.com/blog/security-audit/cyber-crime-statistics/

[4] https://mexico.justia.com/derecho-penal/delitos-informaticos/

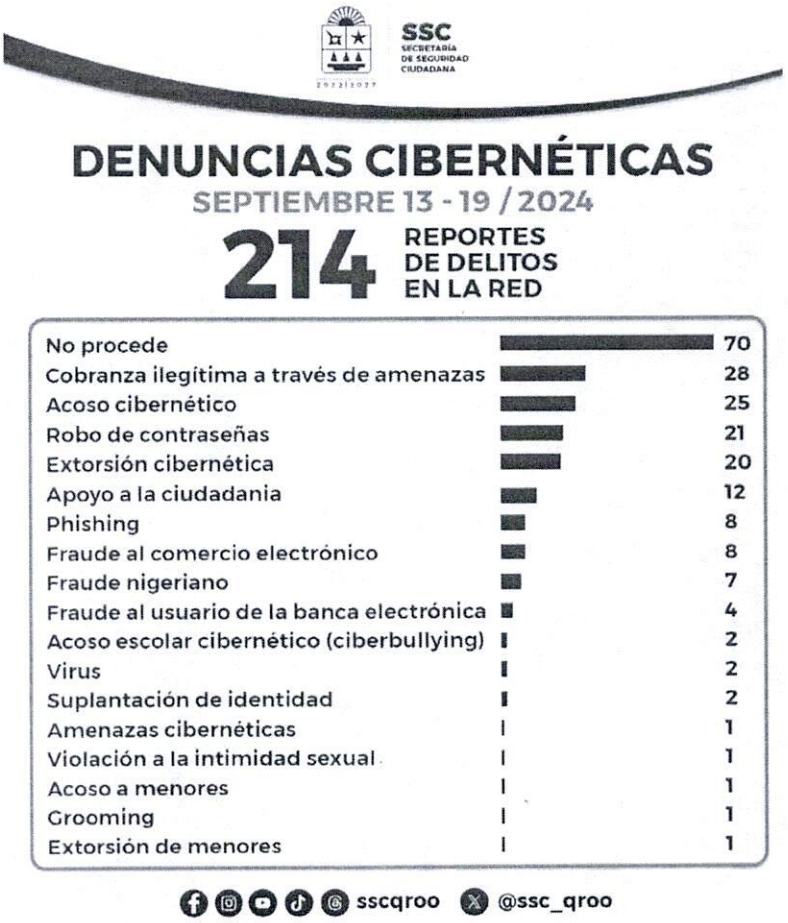
El Estado Mexicano ha sido uno de esos países que ha incluido en su legislación a los delitos informativos a través del Código Penal Federal en especifico en el capitulo II denominado Acceso ilícito a sistemas y equipos de informática, sin embargo además de lo anterior, resulta importante diseñar políticas públicas eficaces para combatir la ciberdelincuencia, ello requiere no solo la voluntad política, sino también adecuaciones legislativas que permitan dotar a las instituciones sobre todo a las policiales de herramientas jurídicas que sean acordes a esta nueva realidad y así priorizar la seguridad ciudadana de las personas.

Son múltiples y contundentes los esfuerzos que se llevan a cabo a nivel mundial, para combatir los peligros, riesgos y daños ocasionados por los delitos cometidos mediante el uso de las tecnologías de la información y comunicación, por ello en la Asamblea General de la Organización de las Naciones Unidas, de fecha 24 de diciembre de 2024, aprobó la Resolución 79/243 *"Convención de las Naciones Unidas contra la Ciberdelincuencia; Fortalecimiento de la Cooperación Internacional para la Lucha contra Determinados Delitos Cometidos mediante Sistemas de Tecnología de la Información y las Comunicaciones y para la Transmisión de Pruebas en Forma Electrónica de Delitos Graves."*

El Estado mexicano participó activamente en la conformación y redacción del texto definitivo del documento mencionado líneas arriba, por lo que el interés de ser parte y adoptar su contenido es notable, con estas acciones se busca que sin importar en qué lugar del mundo se haya cometido el o los delitos del tipo informático o cibernético, si sus efectos se producen en el territorio de nuestro país, las autoridades mexicanas serán competentes para sancionarlo o viceversa, en el supuesto que el delito haya tenido origen en México y sus consecuencias repercutan en uno o más países, la referida convención, prevé que los estados parte podrán establecer la cooperación entre ellos a fin de investigar, perseguir y en su caso, castigar a quienes comentan este tipo de acciones que tanto daño le hacen a las personas que lo padecen; en ese mismo sentido, la presente propuesta legislativa busca establecer las facultades que tendrá la autoridad en nuestro Estado que se dedique a investigar los delitos

cibernéticos, a efecto que la policía cuente con los elementos necesarios para hacer frente a las múltiples conductas delictivas que se cometen en nuestra Entidad y que como se ha mencionado anteriormente, no distinguen entre personas o instituciones, pudiendo afectar a todos por igual.

Ahora bien, en el Estado de Quintana Roo de acuerdo con la Ley de Seguridad Ciudadana existe la Policía de Proximidad Social que tiene entre sus facultades la *prevención, detección, atención y combate* de las conductas antijurídicas y/o delictivas que se cometen a través de las tecnologías de la información y las comunicaciones, medios informáticos, electrónicos e *internet;* y esta reportó que en la semana del 13 al 19 de septiembre de 2024 atendieron 214 denuncias cibernéticas conforme a la siguiente gráfica: [5]



[5] https://saberpolitico.com/portada/toma-precauciones-aumentan-delitos-ciberneticos-en-quintana-roo/

En ese sentido, si bien es cierto como se mencionó líneas arriba, en el Estado de Quintana Roo se cuenta con una policía que tiene como una de sus atribuciones la de prevenir, investigar y combatir los delitos cibernéticos que puedan afectar a los ciudadanos y la seguridad del Estado. Esto incluye fraudes, robo de información, ciberacoso, entre otros delitos cometidos a través de las tecnologías de la información y comunicación, pudiendo ser por el uso de la internet o de las distintas redes sociales existentes, también es cierto que no existe una policía especializada con facultades definidas a través de las cuales se establezcan con claridad las funciones que deberían realizar, por ello a través de la presente acción legislativa, se propone la creación de la Dirección de la Policía Cibernética, así como se propone el establecimiento de su competencia, los protocolos que deben regir el actuar de sus integrantes y su coadyuvancia con otras instancias de seguridad y procuración de justicia.

Como podemos observar esta omisión legislativa genera un vacío enorme en el marco jurídico del Estado, el cual impide la operatividad y el actuar efectivo y legítimo de la policía frente a delitos digitales, toda vez que el cuerpo de seguridad pública que actualmente atiende estas exigencias sociales, se ha visto rebasado por las personas que se dedican a delinquir valiéndose del uso indebido de las tecnologías de la información y la comunicación, por eso es necesario que exista un cuerpo policial especializado y que la ley lo dote de las facultades necesarias para llevar a cabo las investigaciones correspondientes en materia de ciberdelitos y con ello atender a la población Quintanarroense que requiere de sus servicios en virtud de ser víctima de algún delito cibernético, en ese sentido de aprobarse la presente iniciativa se le daría vida jurídica a lo que sería la Policía Cibernética y desaparecería el vacío legal existente.

Por último, se propone que, para el cumplimiento de sus funciones la policía cibernética cuente con personal especializado, así como con la infraestructura tecnológica, las herramientas digitales y una base de datos segura conforme a los

principios de legalidad, proporcionalidad, transparencia y protección de datos personales.

Por lo anteriormente expuesto y fundado en el cuerpo de la presente iniciativa de decreto, me permito someter a la consideración de este Alto Pleno Deliberativo la siguiente **INICIATIVA POR LA QUE SE DEROGA LA FRACCIÓN IV DEL ARTÍCULO 89 Y SE ADICIONAN LA FRACCIÓN XXIX BIS AL ARTÍCULO 3, LA FRACCIÓN IX AL ARTÍCULO 85, EL ARTÍCULO 97 BIS Y EL ARTÍCULO 97 TER TODOS DE LA LEY DE SEGURIDAD CIUDADANA DEL ESTADO DE QUINTANA ROO, EN MATERIA DE POLICÍA CIBERNÉTICA.**

ÚNICO. SE DEROGA LA FRACCIÓN IV DEL ARTÍCULO 89 Y SE ADICIONAN LA FRACCIÓN XXIX BIS AL ARTÍCULO 3, LA FRACCIÓN IX AL ARTÍCULO 85, EL ARTÍCULO 97 BIS Y EL ARTÍCULO 97 TER TODOS DE LA LEY DE SEGURIDAD CIUDADANA DEL ESTADO DE QUINTANA ROO, para quedar como sigue:

Artículo 3. ...

I. a XXIX. ...

XXIX Bis. Policía cibernética: La Policía Cibernética del Estado de Quintana Roo es la unidad especializada de la Secretaría de Seguridad Ciudadana encargada de la prevención, detección, análisis, contención, mitigación, atención e investigación de delitos digitales o cibernéticos, así como de incidentes de seguridad informática que puedan afectar la integridad, privacidad, patrimonio o derechos fundamentales de las personas en entornos digitales;

XXX. a la XXXIX. ...

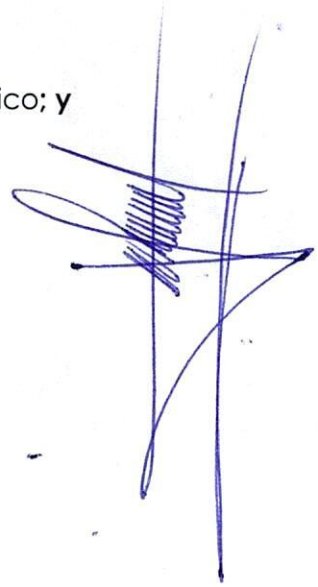
Artículo 85. ...

I. a VI. ...

VII. Reacción;

VIII. Unidad de Servicios Especiales de Vigilancia y de Servicio Público; **y**

IX. Policía cibernética.



Artículo 89. A la Policía de Proximidad Social, le corresponde:

I. a la III. ...

IV. *SE DEROGA.*

V. a la VI. ...

Artículo 97 bis. A la policía cibernética, le corresponde:

I. Monitorear la red pública y redes sociales para identificar conductas que puedan constituir delitos o infracciones administrativas en el entorno digital;

II. Atender reportes y denuncias ciudadanas de las víctimas que son objeto de delitos digitales o que se haya detectado actividad sospechosa en línea;

III. Coadyuvar con el Ministerio Público en investigaciones cibernéticas, conforme a los protocolos establecidos;

IV. Emitir alertas preventivas y recomendaciones sobre amenazas digitales a la ciudadanía;

V. Actuar conforme a protocolos homologados de seguridad informática, ciber inteligencia, cadena de custodia digital, análisis forense de evidencias electrónicas;

VI. Coordinarse con la Fiscalía del Estado y con unidades cibernéticas federales y de otros estados para investigar y atender los delitos cibernéticos;

VII. Impulsar campañas de concientización en ciberseguridad para niñas, niños y adolescentes, y a todos los sectores que se encuentren en situación de vulnerabilidad;

VIII. Efectuar campañas de concientización a la población del uso responsable de las nuevas tecnologías de la información y la comunicación;

IX. Participar en el diseño e implementación de estrategias y programas que buscan fortalecer la ciberseguridad en el estado y proteger la información de la ciudadanía; y

X. Las demás que le confiera esta ley y otros ordenamientos aplicables.

Artículo 97 Ter. Para el cumplimiento de sus funciones la Policía Cibernética contará con personal especializado, así como con la infraestructura tecnológica, las herramientas digitales y la base de datos segura, conforme a los principios de legalidad, proporcionalidad, transparencia y protección de datos personales.

Transitorios

Primero. El presente Decreto entrara en vigor al día siguiente de su publicación en el Periódico Oficial del Estado de Quintana Roo.

Segundo. Se derogan todas las disposiciones que se opongan al presente Decreto.

Dado en la Ciudad de Chetumal, Quintana Roo, a los veinte días del mes de octubre del año dos mil veinticinco.

ATENTAMENTE

DIPUTADO FILIBERTO MARTÍNEZ MÉNDEZ
Presidente de la Comisión de Defensa
de los Límites de Quintana Roo y Asuntos Fronterizos.

RECIBIDO
21 OCT 2025
PODER LEGISLATIVO DEL ESTADO DE QUINTANA ROO
XVIII LEGISLATURA
CONSTITUCIONAL
OFICIALIA DE PARTES