

De la senadora Cora Cecilia Pinedo Alonso a nombre propio y de las senadoras Geovanna del Carmen Bañuelos de la Torre, Nancy de la Sierra Arámburo, Alejandra del Carmen León Gastélum y de los senadores Joel Padilla Peña y Miguel Ángel Lucero Olivas integrantes del Grupo Parlamentario del Partido del Trabajo de la LXIV Legislatura del Honorable Congreso de la Unión, con fundamento en lo dispuesto por los Artículos 71, Fracción II y 135 de la Constitución Política de los Estados Unidos Mexicanos, y 8 fracción I, 164, 169, 171 fracción I, y 172 del Reglamento del Senado de la República, sometemos a la consideración de esta Honorable Asamblea, la siguiente **iniciativa con proyecto de decreto por el que se reforman el artículo 11, la fracción VII del artículo 14, recorriéndose las subsecuentes, y se adiciona un artículo 30 bis de la Ley Orgánica de la Fiscalía General de la República, para crear la Fiscalía Especializada en Delitos Informáticos, conforme a la siguiente:**

Exposición de Motivos

Introducción

Los delitos informáticos han tomado una gran relevancia no solo en México, sino en todo el mundo como consecuencia de los grandes avances tecnológicos.

La delincuencia organizada ha aprovechado el avance tecnológico para la comisión de este tipo de delitos que afectan gravemente el patrimonio de las personas, de las empresas e, incluso, del Estado mexicano.

De acuerdo con la Organización de las Naciones Unidas (ONU), cada día un millón de personas son víctimas de delitos informáticos, siendo una de las modalidades más recurrentes los relacionados con la identidad de las personas; y los ataques de hackers a sistemas informáticos con ochenta millones de víctimas al día.

La comisión de los delitos informáticos se ha incrementado de una manera muy rápida, la tecnología avanza aceleradamente, sin embargo, la forma y herramientas jurídicas y tecnológicas para combatir y neutralizar su comisión en ocasiones no avanza con la misma rapidez dificultando el combate efectivo de la ciberdelincuencia.

Por la complejidad que representa la investigación, la ejecución y acreditación de este tipo de ilícitos penales, así como por el impacto negativo que representa en la economía de las personas, empresas y del Estado mexicano, consideramos necesario la creación de una fiscalía especializada en delitos informáticos, que cuente con el personal capacitado para realizar una adecuada procuración de justicia en esta materia.

El *iter criminis* o camino de los delitos

El *iter criminis* es una alocución latina que significa *camino del delito*. El derecho penal utiliza esta expresión para referirse al proceso de desarrollo del delito, es decir, a las etapas que posee, desde el momento en que se idea la comisión de un delito hasta que se consuma.

El *iter criminis* es el “conjunto de actos sucesivos que sigue el delito en su realización. Antes de producirse el resultado, partimos de la simple idea de cometer un delito, idea que surge en la mente del delincuente o agresor, y que termina con la consumación de ese ilícito penal. Todos los actos que van desde la ideación del delito, hasta su consumación es el camino del delito.”

En consecuencia, desde la ideación del delito hasta su consumación se pasa por diferentes etapas. En México, nuestro sistema jurídico adopta el modelo de derecho penal de acto, el cual asume que las personas son sujetos de derechos y obligaciones, y en ese sentido presupone que pueden y deben hacerse responsable por sus actos. Por ello, sólo son sancionables penalmente las conductas que la persona exterioriza y son perceptibles a través de los sentidos.

El *iter criminis* se compone de dos fases: la interna, que está formada por el conjunto de actos voluntarios del fuero interno de la persona que no son punibles, es decir, no están sancionados por el Código Penal. Por seguir el modelo de derecho penal de acto, esta fase no se castiga ya que se encuentra dentro del pensamiento de la persona. Aquí nos encontramos con tres momentos diferenciados: ideación, deliberación y decisión.

Por su parte, la fase externa es en la que se materializa la voluntad del o de los delincuentes. Va desde la simple manifestación de que el delito se realizará, hasta la consumación del mismo. Es en esta fase el delito cobra vida, deja de ser pensamiento para convertirse en acción.

Son parte de esta fase, la manifestación de la idea delictiva, los actos preparatorios y los actos de ejecución.

Resulta importante que se tengan presentes las fases del *iter criminis* a efecto de tener conciencia y claridad de que el derecho penal, y en particular la teoría del delito, son cuestiones técnicas que en sí mismas requieren de un conocimiento especializado y de un detallado estudio y análisis a efecto de que el agente del ministerio público integre sólida y adecuadamente la correspondiente carpeta de investigación de los delitos informáticos.

Los delitos informáticos pasan por distintas etapas durante el *iter criminis* y utilizan instrumentos tecnológicos sofisticados y plataformas informáticas que hacen complicado detectar a los autores y partícipes de tales delitos, así como su *modus operandi* durante el *iter criminis* de los delitos informáticos.

Atentos a la complejidad que se da durante la fase externa del *iter* y atendiendo al principio de taxatividad que rige en materia penal, el cual establece que en la ley penal se describan con la mayor exactitud posible las conductas que están prohibidas y que constituyen delitos, es que se advierte la necesidad de que el personal de la Fiscalía General de la República cuente con una preparación, especialización y dedicación exclusiva a la atención de este tipo de ilícitos penales en materia informática.

Lo anterior redundará en una mayor eficacia en la procuración de justicia y en un combate efectivo a la delincuencia organizada.

Delitos informáticos

Los delitos informáticos, también llamados cibernéticos, son aquellos realizados por el autor con el auxilio o utilizando la capacidad de los sistemas informáticos para garantizar su anonimato o impunidad territorial, pero que pueden tener tipos penales específicos en algunas legislaciones, definidos con anterioridad a la aparición de los nuevos sistemas de información y telecomunicaciones.¹

Gabriel Andrés Cámpolli menciona que los delitos informáticos son aquellos realizados por el autor con el auxilio o utilizando la capacidad de los sistemas informáticos para garantizar su anonimato o impunidad territorial, pero que pueden tener tipos penales específicos en algunas legislaciones, definidos con

¹ *Delitos Informáticos en la Legislación Mexicana*, Instituto Nacional de Ciencias Penales, México, 2009, p. 17.

anterioridad a la aparición de los nuevos sistemas de información y telecomunicaciones.²

Finalmente, se afirma que delito informático es toda acción u omisión culpable realizada por un ser humano, que cause perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, tipificado por la ley, que se realiza en el entorno informático y está sancionado con una pena.³

Los delitos informáticos se clasifican⁴ como delitos de instrumento o medio, o delitos como fin u objetivo.

En la primera clasificación, como instrumento o medio se encuentran aquellas conductas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito. Como ejemplos el autor cita los siguientes: a) falsificación de documentos por la vía computarizada (tarjetas de crédito, cheques); b) variación de los activos y pasivos en la situación contable de las empresas; c) planeación o simulación de delitos convencionales (robo, fraude); d) intervención en las líneas de comunicación de datos o teleproceso.

Por su parte, en la clasificación como fin u objetivo se encuadran las conductas dirigidas en contra de la computadora, accesorios o programas como entidad física. Entre los ejemplos que al respecto mencionan se encuentran: a) programación de instrucciones que producen un bloqueo total al sistema; b) destrucción de programas por cualquier medio; c) atentado físico contra la máquina o sus accesorios; d) sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados; e) daño a las memorias de las computadoras.

De igual manera, se afirma que en términos generales hay dos tipos de delitos informáticos: aquellos que tienen como finalidad destruir, alterar, modificar o extraer información de manera no autorizada de los sistemas informáticos y los delitos del orden común que se cometen a través de nuevas tecnologías.

² *Delitos Informáticos en la Legislación Mexicana*, Instituto Nacional de Ciencias Penales, México, 2009, p. 17.

³ Flores Salgado, Lucerito. *Derecho Informático*, Grupo Editorial Patria, 2009, p.132.

⁴ Téllez Valdés, Op. Cit. P. 190.

Política criminal y combate a los delitos informáticos

Dentro de la criminología siempre se habla del *factor criminógeno* cuando se analizan las circunstancias en las que se cometen los delitos. El factor criminógeno, son los elementos que contribuyen para facilitar la comisión u omisión de una conducta de resultado antisocial. Está constituido por los factores endógenos y exógenos.

Los factores endógenos, conocidos también como factores somáticos, son aquellos de cualidad innata a la persona, como los factores psicológicos (trastornos de la personalidad; patologías), biológicos (adn, enfermedades corporales, herencia genética) etcétera, donde existe relación entre la actividad del organismo con las conductas antisociales de la persona. Los factores exógenos, son factores sociales que influyen en el comportamiento de las personas.

En el caso de los delitos informáticos, el Doctor Alberto Nava⁵ sostiene que la informática y, en general el tratamiento automatizado de datos son el factor criminógeno que influye en el delincuente para realizar ese tipo de conductas ilícitas.

En muchas ocasiones no se crean conductas delictivas nuevas sino que se cometen conductas ilícitas ya conocidas que aprovechan para su comisión de nuevos medios para alcanzar sus objetivos, lesionando o poniendo en riesgo bienes jurídicos tutelados por el derecho penal.

Entre la diversidad de crímenes informáticos existentes, encontramos aquellos que buscan por medio del software especializado lograr un beneficio económico ilegal, a través del chantaje y la extorsión. Ejemplo de ello es el *ransomware*, el cual es un programa de software malicioso que infecta los equipos informativos y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema.

Este tipo de *malware* es un sistema criminal, de secuestro informático, para ganar dinero que se puede instalar a través de enlaces engañosos incluidos en un mensaje de correo electrónico, mensaje instantáneo o sitio web. El *ransomware* tiene la capacidad de bloquear la pantalla de una computadora o cifrar archivos importantes predeterminados con una contraseña que en el mejor de los casos cesa con la aplicación de otras herramientas informáticas de seguridad o bien tras el pago por el rescate de la información.

⁵ Nava Garcés, Alberto E. *Delitos Informáticos*, México, Porrúa, 2007, p. 33-36.

El uso de ordenadores, computadoras, dispositivos móviles como celulares o tabletas, han servido a las personas a mantenerse informado, pero también el uso de estos dispositivos ha sido utilizado para la comisión de actos ilícitos catalogados como delitos informáticos o cibernéticos.

Los delitos informáticos afectan diversos bienes jurídicos que el derecho penal pretende tutelar como son el patrimonio, la reserva o la confidencialidad de los datos, la seguridad y el derecho de propiedad, la identidad, el honor, etc.

La delincuencia organizada ha hecho más efectivas su capacidad y forma de operación al momento de realizar los delitos que comúnmente realizan dentro de éstos sin duda alguna los delitos informáticos han alcanzado un nivel de sofisticación que hacen cada día más difícil su comprobación.

A continuación se mencionan algunos de los delitos cibernéticos más comunes en internet:

Tipos de delitos según la Policía Cibernética	Descripción
Tipo 1	Es el robo o manipulación de datos o servicios por medio de piratería o virus, el robo de identidad y fraudes en el sector bancario o del comercio electrónico.
TIPO 2	Son actividades como el acoso en Internet, turismo sexual, extorsión, chantaje, espionaje, terrorismo, abuso de menores, explotación sexual comercial infantil, robo o sustracción de menores, etc.
Principales delitos cometidos en internet	
TIPO 1	Robo de identidad
	Phreaking (mecanismos que vulneran la seguridad de los sistemas telefónicos)
	Amenazas
	Fraudes en e-commerce (portales de subasta)
	Fraudes online (compras en tiendas virtuales)
	Clonación de tarjetas de crédito
	Robo de información
	Carding (utilización ilegal de tarjetas de crédito)
	Trasposos ilegítimos
	Phishing (correos falsos para robar datos del usuario) Extorsiones, secuestros o localización de objetivos
TIPO 2	Pornografía infantil

	Explotación sexual comercial infantil
	Lenocinio infantil en Internet
	Abuso de menores
	Turismo sexual en Internet
	Robo y sustracción de menores
	Fuente: Policía Cibernética.

La política criminal de combate a la comisión de delitos informáticos implementada por el gobierno federal ha logrado contenerlos, sin embargo, consideramos que dado el impacto negativo que tiene en términos sociales, de seguridad y en las finanzas y patrimonio de las personas y del Estado, es necesario crear una Fiscalía Especializada en Delitos Informáticos que cuente con el presupuesto y el personal calificado que permita que las personas que realizan esta conducta delictiva realmente sean procesados y sancionados penalmente.

Los tres Poderes de la Unión deben de trabajar en unidad para poder combatir con total eficacia este delito. El Ejecutivo manteniendo y reforzando la política criminal que ha implementado desde el inicio de su gobierno; el Judicial resolviendo con prontitud y apegado a la ley los casos penales que lleguen a los juzgados, y el poder Legislativo realizando los cambios normativos que permitan dar sustento legal a la política criminal y creando los órganos que hagan más eficiente el combate a los delitos informáticos en cualquiera de sus modalidades.

De acuerdo con la Organización de las Naciones Unidas (ONU), cada día, un millón de personas son víctimas de delitos informáticos, siendo una de las modalidades más recurrentes los relacionados con la identidad de las personas; y los ataques de hackers que generan ochenta millones de víctimas al día.

México es el tercer país a nivel mundial con el mayor número de delitos cibernéticos, se encuentra solo por debajo de países como China y Sudáfrica. En América Latina ocupa el primer lugar en la comisión de este tipo de delitos.

De acuerdo con la Secretaría de Hacienda y Crédito Público, el fraude cibernético durante el primer trimestre del año 2019, incrementó en quejas en un 35 por ciento en comparación con el año 2018. En tanto que el robo de identidad durante el primer trimestre del 2019 aumentó en un 217 por ciento respecto al mismo periodo del 2018.

Como ya hemos mencionado, los delitos informáticos pueden afectar los derechos e integridad de una persona física como también los de las empresas o el Estado mexicano.

Un caso reciente donde se vio afectado el Estado mexicano se presentó el pasado domingo 10 de noviembre de este año cuando la red interna de Petróleos Mexicanos fue víctima de ataques cibernéticos y los agresores solicitaron a la petrolera un pago de cinco millones de dólares.

El ataque obligó a Pemex a apagar sus equipos de cómputo en todo el país, inhabilitando, entre otros, los sistemas de pagos.

De acuerdo a diferentes notas periodísticas, los hackers introdujeron un *ransomware*. Mediante una nota de rescate que apareció en los equipos de cómputo de Pemex, se daba instrucciones para acceder a un sitio de internet anónimo ligado a "DoppelPaymer", y en él se pedían 565 bitcoins, equivalente a cinco millones de dólares, dando un plazo de 48 horas para realizar el pago.

Tras vencerse el plazo otorgado por los presuntos delincuentes, éstos anunciaron que la empresa productiva del Estado aún contaba con tiempo para entregar los 565 bitcoins y que les pudieran restablecer el funcionamiento del sistema.

Diversas áreas de Pemex se vieron afectadas en su operación cotidiana. Durante horas fueron apagados y desconectados equipos de cómputo de para darles mantenimiento y desinfectarlas. Hubo necesidad de comunicarse con los empleados a través del servicio de mensajería móvil WhatsApp porque los empleados no podían abrir sus correos electrónicos. "En Finanzas, todas las computadoras están apagadas, eventualmente podría haber problemas con los pagos", dijeron a los medios algunos trabajadores que solicitaron el anonimato.⁶

Por todo lo expuesto, es urgente crear la Fiscalía Especializada en Delitos Informáticos, que cuente con el presupuesto y el personal calificado que permita un combate eficaz desde el ámbito de la procuración de justicia.

⁶ <https://www.milenio.com/negocios/hackeo-pemex-robo-datos-afirma-sener>

La Fiscalía Especializada en Delitos Informáticos que proponemos, presentará anualmente ante el Senado de la República y el Comité Coordinador del Sistema Nacional Anticorrupción, este último sólo en los casos en que exista correlación entre los delitos informáticos y posibles actos de corrupción cometidos desde la función pública, un informe sobre actividades sustantivas y sus resultados, el cual será público, en términos de lo previsto en la Ley General de Transparencia y Acceso a la Información Pública y demás disposiciones aplicables en la materia.

Finalmente, para explicar el sentido y alcance de las reformas propuestas, se presenta un cuadro comparativo entre la legislación vigente y la presente propuesta de reforma a los artículos 11, fracción VII del artículo 14, recorriéndose las subsecuentes, y se adiciona un artículo 30 Bis de la ley Orgánica de la Fiscalía General de la República:

TEXTO VIGENTE	TEXTO PROPUESTO
<p>Artículo 11. Órganos a cargo de la función fiscal</p> <p>La representación de la Fiscalía General de la República corresponde a los siguientes órganos: I. Titular de la Fiscalía General de la República; II. Titulares de la Fiscalía Especializada en Materia de Derechos Humanos, de la Fiscalía Especializada de Delitos Electorales, de la Fiscalía Especializada en Combate a la Corrupción y de la Fiscalía Especializada de Asuntos Internos;</p> <p>III. Titulares de las Fiscalías Especializadas;</p> <p>(...)</p>	<p>Artículo 11. Órganos a cargo de la función fiscal</p> <p>La representación de la Fiscalía General de la República corresponde a los siguientes órganos:</p> <p>I. Titular de la Fiscalía General de la República;</p> <p>II. Titulares de la Fiscalía Especializada en Materia de Derechos Humanos, de la Fiscalía Especializada de Delitos Electorales, de la Fiscalía Especializada en Combate a la Corrupción, de la Fiscalía Especializada de Asuntos Internos y Fiscalía Especializada en Delitos Informáticos.</p> <p>III. Titulares de las Fiscalías Especializadas;</p> <p>(...)</p>
<p>Artículo 14. De la Estructura de la Fiscalía General de la República</p> <p>La Fiscalía General de la República tendrá la siguiente estructura:</p> <p>I. Fiscal General;</p> <p>II. Coordinación General;</p>	<p>Artículo 14. De la Estructura de la Fiscalía General de la República</p> <p>La Fiscalía General de la República tendrá la siguiente estructura:</p> <p>I. Fiscal General;</p> <p>II. Coordinación General;</p>

<p>III. Fiscalía Especializada en Materia de Derechos Humanos;</p> <p>IV. Fiscalía Especializada en Delitos Electorales;</p> <p>V. Fiscalía Especializada en Combate a la Corrupción;</p> <p>VI. Fiscalía Especializada de Asuntos Internos;</p> <p>VII. Coordinación de Investigación y Persecución Penal;</p> <p>VIII. Coordinación de Métodos de Investigación;</p> <p>IX. Coordinación de Planeación y Administración;</p> <p>X. Órgano Interno de Control;</p> <p>XI. Centro de Formación y Servicio Profesional de Carrera;</p> <p>XII. Órgano de Mecanismos Alternativos de Solución de Controversias, y</p> <p>XIII. Las Fiscalías, órganos o unidades que determine la persona titular de la Fiscalía General, a través de acuerdos generales, de conformidad con la presente Ley y su Reglamento, y acorde con el Plan de Persecución Penal.</p> <p>(...)</p> <p>(...)</p> <p>(...)</p> <p>(...)</p> <p>(...)</p> <p>(...)</p> <p>(...)</p> <p>(...)</p> <p>(...)</p>	<p>III. Fiscalía Especializada en Materia de Derechos Humanos;</p> <p>IV. Fiscalía Especializada en Delitos Electorales;</p> <p>V. Fiscalía Especializada en Combate a la Corrupción;</p> <p>VI. Fiscalía Especializada de Asuntos Internos;</p> <p>VII. Fiscalía Especializada en Delitos Informáticos;</p> <p>VIII. Coordinación de Investigación y Persecución Penal;</p> <p>IX. Coordinación de Métodos de Investigación;</p> <p>X. Coordinación de Planeación y Administración;</p> <p>XI. Órgano Interno de Control;</p> <p>XII. Centro de Formación y Servicio Profesional de Carrera;</p> <p>XIII. Órgano de Mecanismos Alternativos de Solución de Controversias, y</p> <p>XIV. Las Fiscalías, órganos o unidades que determine la persona titular de la Fiscalía General, a través de acuerdos generales, de conformidad con la presente Ley y su Reglamento, y acorde con el Plan de Persecución Penal.</p> <p>(...)</p> <p>(...)</p> <p>(...)</p> <p>(...)</p> <p>(...)</p> <p>(...)</p> <p>(...)</p> <p>(...)</p> <p>(...)</p>
<p>Artículo 30 Bis. (Sin correlativo)</p>	<p>Artículo 30 Bis. Funciones de la Fiscalía Especializada en Delitos</p>

Informáticos

La Fiscalía Especializada en Delitos Informáticos tendrá bajo su cargo la investigación, prevención y persecución de los delitos contenidos en el Capítulo II del Título Noveno del Libro Segundo del Código Penal Federal, y en cualquier otro ordenamiento legal en la materia. Deberá informar mensualmente al titular de la Fiscalía General de la República sobre la cantidad y naturaleza de las denuncias recibidas, el estado de las investigaciones, así como las determinaciones o procesos según sea el caso.

Igualmente, de forma anual, presentará ante el Senado de la República y al Comité Coordinador del Sistema Nacional Anticorrupción, este último sólo en los casos en que exista correlación entre los delitos informáticos y posibles actos de corrupción cometidos desde la función pública, un informe sobre actividades sustantivas y sus resultados, el cual será público, en términos de lo previsto en la Ley General de Transparencia y Acceso a la Información Pública y demás disposiciones aplicables en la materia.

Por los motivos antes expuestos, someto a esta Soberanía la presente iniciativa con proyecto de:

DECRETO POR EL QUE SE REFORMA EL ARTÍCULO 11, SE REFORMA LA FRACCIÓN VII DEL ARTÍCULO 14, RECORRIÉNDOSE LAS SUBSECUENTES, Y SE ADICIONA UN ARTÍCULO 30 BIS DE LA LEY ORGÁNICA DE LA FISCALÍA GENERAL DE LA REPÚBLICA, PARA CREAR LA FISCALÍA ESPECIALIZADA EN MATERIA DE HIDROCARBUROS.

ARTÍCULO ÚNICO.- Se reforma el artículo 11, se reforma la fracción VII del artículo 14, recorriéndose las subsecuentes, y se adiciona un artículo 30 Bis de la ley Orgánica de la Fiscalía General de la República, para quedar como sigue:

Artículo 11. Órganos a cargo de la función fiscal

La representación de la Fiscalía General de la República corresponde a los siguientes órganos:

- I. Titular de la Fiscalía General de la República;
- II. Titulares de la Fiscalía Especializada en Materia de Derechos Humanos, de la Fiscalía Especializada de Delitos Electorales, de la Fiscalía Especializada en Combate a la Corrupción, de la Fiscalía Especializada de Asuntos Internos y Fiscalía Especializada en Delitos Informáticos.
- III. Titulares de las Fiscalías Especializadas;
- (...)

Artículo 14. De la Estructura de la Fiscalía General de la República

La Fiscalía General de la República tendrá la siguiente estructura:

- I. Fiscal General;
- II. Coordinación General;
- III. Fiscalía Especializada en Materia de Derechos Humanos;
- IV. Fiscalía Especializada en Delitos Electorales;
- V. Fiscalía Especializada en Combate a la Corrupción;
- VI. Fiscalía Especializada de Asuntos Internos;
- VII. Fiscalía Especializada en Delitos Informáticos;
- VIII. Coordinación de Investigación y Persecución Penal;
- IX. Coordinación de Métodos de Investigación;
- X. Coordinación de Planeación y Administración;
- XI. Órgano Interno de Control;
- XII. Centro de Formación y Servicio Profesional de Carrera;
- XIII. Órgano de Mecanismos Alternativos de Solución de Controversias, y

XIV. Las Fiscalías, órganos o unidades que determine la persona titular de la Fiscalía General, a través de acuerdos generales, de conformidad con la presente Ley y su Reglamento, y acorde con el Plan de Persecución Penal.

(...)
(...)
(...)
(...)
(...)
(...)
(...)
(...)

Artículo 30 Bis. Funciones de la Fiscalía Especializada en Delitos Informáticos

La Fiscalía Especializada en Delitos Informáticos tendrá bajo su cargo la investigación, prevención y persecución de los delitos contenidos en el Capítulo II del Título Noveno del Libro Segundo del Código Penal Federal, y en cualquier otro ordenamiento legal en la materia. Deberá informar mensualmente al titular de la Fiscalía General de la República sobre la cantidad y naturaleza de las denuncias recibidas, el estado de las investigaciones, así como las determinaciones o procesos según sea el caso.

Igualmente, de forma anual, presentará ante el Senado de la República y al Comité Coordinador del Sistema Nacional Anticorrupción, este último sólo en los casos en que exista correlación entre los delitos informáticos y posibles actos de corrupción cometidos desde la función pública, un informe sobre actividades sustantivas y sus resultados, el cual será público, en términos de lo previsto en la Ley General de Transparencia y Acceso a la Información Pública y demás disposiciones aplicables en la materia.

ARTÍCULOS TRANSITORIOS

PRIMERO.- El presente decreto entrará en vigor ciento ochenta días después de su publicación en el Diario Oficial de la Federación, a efecto de llevar a cabo los ajustes presupuestales y de personal necesarios dentro de la Fiscalía General de la República para la implementación y funcionamiento de la Fiscalía Especializada en Delitos Informáticos.

SEGUNDO.- A partir del año fiscal siguiente a la publicación del presente decreto, la Cámara de Diputados deberá considerar dentro del Presupuesto de Egresos de la Federación el presupuesto destinado al funcionamiento y operación de la Fiscalía Especializada en Delitos Informáticos.

TERCERO.- Se derogan todas las disposiciones que contravengan el presente.

Dado en el Salón de Plenos de la Cámara de Senadores a los cinco días del mes de diciembre de dos mil diecinueve.

Atentamente

Sen. Cora Cecilia Pinedo Alonso

Sen. Geovanna del Carmen Bañuelos de la Torre

Sen. Nancy de la Sierra Arámburo

Sen. Alejandra del Carmen León Gastélum

Sen. Miguel Ángel Lucero Olivas

Sen. Joel Padilla Peña