ANÁLISIS TÉCNICO PRELIMINAR

No. Expediente: 0524-2CP1-25

I.- DATOS DE IDENTIFICACIÓN DE LA INICIATIVA	
1.- Nombre de la Iniciativa.	Que adicionan diversas disposiciones en el Código Penal Federal y en el Código Nacional de Procedimientos Penales.
2.- Tema de la Iniciativa.	Justicia.
3.- Nombre de quien presenta la Iniciativa.	Dip. Rubén Ignacio Moreira Valdez.
4.- Grupo Parlamentario del Partido Político al que pertenece.	PRI.
5.- Fecha de presentación ante el Pleno de la Comisión Permanente.	27 de agosto de 2025.
6.- Fecha de publicación en la Gaceta Parlamentaria.	27 de agosto de 2025.
7.- Turno a Comisión.	Justicia.

II.- SINOPSIS

Incluir un capítulo denominado Del Ciberterrorismo y delitos informáticos, en el cual se tipifican los delitos de ciberterrorismo, ciberespionaje, suplantación de identidad cibernética y secuestro de datos. Establecer la competencia territorial para delitos cometidos a través de instrumentos informáticos, al Órgano Jurisdiccional Federal.

III.- ANÁLISIS DE CONSTITUCIONALIDAD

El derecho de iniciativa se fundamenta en la fracción II del artículo 71 y la facultad del Congreso de la Unión para legislar en la materia se sustenta en las fracciones XXI y XXIII del artículo 73, todos de la Constitución Política de los Estados Unidos Mexicanos.

IV.- ANÁLISIS DE TÉCNICA LEGISLATIVA

En la parte relativa al texto legal que se propone, se sugiere lo siguiente:

- Conforme a la terminología y desarrollo del proceso legislativo, previstos por los artículos 70 y 72 constitucionales, respectivamente, usar el término "Iniciativa con Proyecto de Decreto", toda vez que éste aún se encuentra en proceso de aprobación.

La iniciativa, salvo la observación antes señalada, cumple en general con los requisitos formales que se exigen en la práctica parlamentaria y que de conformidad con el artículo 78 del Reglamento de la Cámara de Diputados, son los siguientes:

Encabezado o título de la propuesta; planteamiento del problema que la iniciativa pretenda resolver; problemática desde la perspectiva de género, en su caso; argumentos que la sustenten; fundamento legal; denominación del proyecto de ley o decreto; ordenamientos a modificar; texto normativo propuesto; artículos transitorios; lugar; fecha, nombre y rúbrica del iniciador.

V.- CUADRO COMPARATIVO DEL TEXTO VIGENTE Y DEL TEXTO QUE SE PROPONE

TEXTO VIGENTE	TEXTO QUE SE PROPONE
CÓDIGO PENAL FEDERAL	**DECRETO POR EL QUE SE ADICIONA EL CAPÍTULO III DENOMINADO "DEL CIBERTERRORISMO Y DELITOS INFORMÁTICOS" CON LOS ARTÍCULOS 211 TER, 211 TER 1, 211 TER 2, 211 TER 3 Y 211 TER 4 AL TÍTULO NOVENO DEL CÓDIGO PENAL FEDERAL; Y UNA FRACCIÓN IX AL ARTÍCULO 20 DEL CÓDIGO NACIONAL DE PROCEDIMIENTOS PENALES.** **Artículo Primero**. Se **adiciona** un Capítulo III denominado del Ciberterrorismo y delitos informáticos con los artículos 211 ter, 211 ter 1, 211 ter 2, 211 ter 3 y 211 ter 4, al título Noveno del Código Penal Federal para quedar como sigue: TITULO NOVENO Revelación de secretos y acceso ilícito a sistemas y equipos de informática
CAPITULO I **Revelación de secretos** **Artículo 210**.- … a **Artículo 211 Bis**.- …	
CAPÍTULO II **Acceso ilícito a sistemas y equipos de informática** **Artículo 211 bis 1**.- … a **Artículo 211 bis 7.-** …	

No tiene correlativo.	**Capítulo III** **Del Ciberterrorismo y delitos informáticos** **211 Ter. Comete el delito de ciberterrorismo quien, por medio del uso de sistemas informáticos, redes de comunicación, programas, algoritmos o cualquier tipo tecnología digital:** **I. Realice actos directamente encaminados a intimidar, coaccionar o desestabilizar a la población, o a las instituciones del Estado Mexicano;** **II. Mediante la intimidación, amenaza, coacción, inste a un funcionario público a realizar actos a actos que atenten en contra de la estabilidad a seguridad de la nación, de o a una organización internacional, o a forzar ilegítimamente a una autoridad a realizar un acto o abstenerse de hacerlo; y** **III. Produzca alguno de los siguientes resultados:** **a) Interrupción total o parcial, sabotaje o destrucción de infraestructuras críticas o servicios esenciales en los ámbitos de seguridad, salud, energía, transporte, abastecimiento de agua, comunicaciones o financieros;** **b) Acceso, manipulación, alteración o destrucción de datos sensibles cuyo efecto cause un peligro**

No tiene correlativo.	**serio para la seguridad nacional o para la vida e integridad física de las personas; o** **c) Difusión de software malicioso o ataques masivos que pongan en peligro grave la estabilidad económica, social o política de un país.** **211 ter 1. Comete el delito de ciberespionaje quien, por sí o por interpósita persona, sin autorización legítima y utilizando medios informáticos, digitales, electrónicos o cualquier tecnología de la información y la comunicación, acceda, obtenga, intercepte, copie, transfiera, modifique o utilice información, datos, comunicaciones, archivos o sistemas informáticos ajenos, con la finalidad de obtener, divulgar, transmitir o utilizar información reservada o confidencial perteneciente a personas físicas, morales, organismos públicos, empresas, instituciones gubernamentales o entidades de interés estratégico.** **A quien cometa ciberespionaje se le impondrá prisión de cinco a quince años de prisión y multa de quinientas a mil unidades de medida de actualización, sin perjuicio de las sanciones que correspondan por los delitos que con dicha información se llegaren a cometer.** **211 ter 2. Comete el delito de suplantación de identidad cibernética quien mediante el uso de**

No tiene correlativo.	**correos electrónicos, sitios webs falsos, mensajes de texto, aplicaciones digitales, interfaces digitales o cualquier otro medio electrónico:** **I. Suplante, simule o haga creer fraudulentamente a otra persona que se trata de una entidad, institución, empresa o individuo legítimo con la finalidad de obtener, sin derecho, datos personales, contraseñas, información financiera, patrimonial o confidencial de un usuario; o** **II. Induzca a error al destinatario para que revele, confirme o transmita información que pueda ser utilizada para cometer fraudes, apropiación de bienes, afectación patrimonial o vulneración de la seguridad de sistemas informáticos.** **A quien cometa el delito de suplantación de identidad cibernética se le impondrá de dos a ocho años de cárcel y multa de doscientas a seiscientas unidades de medida de actualización, sin perjuicio de las sanciones que resulten de la comisión de los delitos que se generen con la suplantación.** **211 ter 3. Comete el delito de secuestro de datos, la persona física o moral que por cualquier medio informático, digital o electrónico, sin autorización legítima y con ánimo de obtener un beneficio ilícito para sí o para un tercero:**

No tiene correlativo.	**I. Acceda, intervenga, opere o altere sistemas, redes, datos, archivos o programas informáticos ajenos, cifrándolos o bloqueando su acceso total o parcial,** **II. Exija, directa o indirectamente, el pago de un rescate, beneficio, contraprestación o condición a cambio de restablecer el acceso o devolver el control al legítimo titular.** **Se impondrá prisión de cinco a doce años y multa de seiscientas a mil unidades de medida de actualización a quien cometa el delito de secuestro de datos.** **La pena máxima se incrementará en una mitad cuando el ataque se realice en contra de infraestructuras críticas, servicios esenciales de salud, finanzas, seguridad, comunicaciones, o afecta gravemente los derechos fundamentales de los titulares.** **Artículo 211 ter 4. Las penas previstas en este capítulo serán impuestas sin perjuicio de las sanciones que resulten por la comisión de otros delitos cometidos como resultado del uso de información digital.**
CÓDIGO NACIONAL DE PROCEDIMIENTOS PENALES	**Artículo Segundo**. Se **adiciona** una fracción IX al artículo 20 del Código Nacional de Procedimientos Penales para quedar como sigue:

Artículo 20. Reglas de competencia ... **I.** ... a **VI**. ... **VII.** Cuando el hecho punible haya iniciado su ejecución en un lugar y consumado en otro, el conocimiento corresponderá al Órgano jurisdiccional de cualquiera de los dos lugares, *y* **VIII**. Cuando el hecho punible haya comenzado su ejecución o sea cometido en territorio extranjero y se siga cometiendo o produzca sus efectos en territorio nacional, en términos de la legislación aplicable, será competencia del Órgano jurisdiccional federal. **No tiene correlativo.**	Artículo 20. Reglas de competencia. Para determinar la competencia territorial de los Órganos jurisdiccionales federales o locales, según corresponda, se observarán las siguientes reglas: I a VI … VII. Cuando el hecho punible haya iniciado su ejecución en un lugar y consumado en otro, el conocimiento corresponderá al Órgano jurisdiccional de cualquiera de los dos lugares**;** VIII. Cuando el hecho punible haya comenzado su ejecución o sea cometido en territorio extranjero y se siga cometiendo o produzca sus efectos en territorio nacional, en términos de la legislación aplicable, será competencia del Órgano jurisdiccional federal**, y** **IX. Cuando el hecho punible haya sido cometido mediante el uso de instrumentos informáticos y no sea posible determinar la territorialidad del mismo, será competencia del Órgano jurisdiccional federal.**
	TRANSITORIO. **ÚNICO**. El presente decreto entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación

Alondra Hernández