INICIATIVA QUE REFORMA LOS ARTÍCULOS 211 BIS 2 Y 211 BIS 3 DEL CÓDIGO PENAL FEDERAL, EN MATERIA DE DELITOS INFORMÁTICOS EN CONTRA DEL ESTADO, A CARGO DEL DIPUTADO HUMBERTO COSS Y LEÓN ZÚÑIGA, DEL GRUPO PARLAMENTARIO DE MORENA

Quien suscribe, diputado Humberto Coss y León Zúñiga, integrante del Grupo Parlamentario de Morena en la LXVI Legislatura del honorable Congreso de la Unión, con fundamento en lo dispuesto en los artículos 71, fracción II, y 72 de la Constitución Política de los Estados Unidos Mexicanos, así como en los artículos 77 y 78 del Reglamento de la Cámara de Diputados, someto a consideración de esta asamblea la iniciativa con proyecto de decreto por el que se reforman los artículos 211 bis 2 y 211 bis 3 del Código Penal Federal, en materia de delitos informáticos en contra del Estado, al tenor de la siguiente

Exposición de Motivos

Los avances tecnológicos y el acceso a internet han revolucionado nuestras formas de interactuar en la vida cotidiana, de trabajar y realizar transacciones. Sin embargo, esta revolución también ha dado paso a un alarmante aumento en la comisión de delitos informáticos, que van desde el fraude en línea en contra de particulares, hasta el robo de información sensible, tanto del Estado como del sector privado (empresarial y financiero).

En México, a pesar del conjunto de medidas preventivas no punitivas y de carácter penal, tal como la Estrategia Nacional de Ciberseguridad (2017) o la creación de la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (2006), persiste una problemática crucial: la existencia de penalidades ineficaces para castigar a los autores de delitos informáticos, lo que ha debilitado la disuasión de estos eventos antisociales.

Dentro del Código Penal Federal y en virtud del *test* de proporcionalidad abstracta en materia penal empleado por la Suprema Corte de Justicia de la Nación, por el cual resulta obligatorio para el legislador justificar una correspondencia entre la severidad del delito y la magnitud de su sanción, las penalidades asociadas a los delitos informáticos tipificados en el Capítulo II del Título Noveno del ordenamiento sustantivo federal (artículos 211 Bis 1 a 211 Bis 7) resultan en su mayoría leves y no correspondientes a los daños que su actualización ocasiona a la esfera de derechos de las víctimas, físicas o morales, y al propio Estado mexicano.

Lo anterior crea un ambiente propicio para que los delincuentes informáticos persistan en sus operaciones, ya que las consecuencias legales no son suficientemente disuasorias. La baja probabilidad de que se les impongan sanciones privativas de libertad *ad hoc* a la gravedad de la vulneración a los bienes jurídicos tutelados genera un incremento en su comisión, en perjuicio de más de 106.7 millones de personas usuarias que acceden a internet con fines tan diversos como el uso de redes sociales, plataformas académicas o de entretenimiento, descarga de *softwares* , compraventas u operaciones bancarias, entre muchas otras.[1]

De esta forma, los diversos delitos cibernéticos constituyen una amenaza para el sector privado y para la población en general, con independencia de la edad, sexo o condición socioeconómica de la víctima; delitos como el fraude y extorsión en línea han ocasionado suplantación de identidad y daños irreparables al patrimonio, reputación, honor y al libre desarrollo de la personalidad, e incluso conducido al padecimiento de cuadros de ansiedad, depresión e inducción al suicidio.[2]

Las empresas y el sector financiero también han sido víctimas de estos delitos, los cuales han derivado en pérdidas económicas significativas y daños al patrimonio moral como son los derechos de autor y los relativos a la propiedad intelectual.

En México, tan sólo en 2023 y según datos del Instituto Nacional de Estadística y Geografía (INEGI), el 20.9 por ciento de la población usuaria de internet (aproximadamente 18.4 millones de personas mayores de 12 años) vivió alguna situación de ciberacoso, siendo las tres entidades federativas con mayor incidencia Durango (28.8 por ciento), Oaxaca (25.5 por ciento) y Puebla (25 por ciento).[3]

En relación, de acuerdo con el Censo Nacional de Seguridad Pública Estatal (CNSPE), en 2023 se registraron 106 mil 218 incidentes cibernéticos atendidos por las unidades estatales de policía cibernética u homólogas, de los cuales resaltan conductas como el acoso, amenazas, difamación, extorsión, fraude al comercio electrónico, fraude al usuario de la banca electrónica, fraude de soporte técnico, fraude de empleo, *ciberbullying* , pornografía infantil, robo de contraseñas en redes sociales a menores de edad, trata de menores de edad, reclutamiento forzado y terrorismo cibernético.

De esta misma estadística, en la categoría de “Eventos de seguridad informática” las unidades de policía cibernética identificaron 22 mil 216 incidentes, de los cuales encontramos la intrusión a sistemas, *hacking, malware* (virus policía), *phishing, pharming, criptolocker* , entre otros.[4]

Delitos informáticos en contra de la seguridad nacional

Asimismo, en la era digital, delitos como el ciberespionaje o el ciberterrorismo pueden generar efectos devastadores para el funcionamiento y continuidad de las instituciones de los tres poderes de la Unión y de los tres órdenes de gobierno, en consecuencia, de la propia soberanía nacional, lo cual derivaría en amenazas y riesgos directos en contra de la integridad, estabilidad y permanencia del Estado, convirtiendo a estos delitos, invariablemente, en asuntos de seguridad nacional.

En efecto, el Estado cuenta con una amplia red de **infraestructuras críticas de información** en áreas estratégicas como son el sector energético, de infraestructura, comunicaciones y transportes, así como en distintos servicios públicos, cuya protección es esencial para la funcionalidad, seguridad y bienestar de la población. De acuerdo con la *Directiva 2008/114/CE* del Consejo de la Unión Europea, por infraestructura crítica se entiende “el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la

seguridad y el bienestar de la sociedad, cuya perturbación o destrucción afectaría gravemente a un Estado".[5]

Así, las Tecnologías de la Información y la Comunicación (TIC) son ya factor clave en el funcionamiento del Estado, en la medida en que posibilitan la operación de infraestructuras críticas, el desarrollo de los procesos económicos y financieros en el país y gestiones gubernamentales en *pro* de los derechos fundamentales de la ciudadanía. Un claro ejemplo de esto son los productos de inteligencia generados por el Sistema Nacional de Información e Investigación en materia de Seguridad Pública (2025).

A decir del Ministerio de Tecnologías de la Información y las Comunicaciones de la República de Colombia, las TIC constituyen el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios que permiten la compilación, procesamiento, almacenamiento y transmisión de información.[6]

En consecuencia, el Estado debe "generar las condiciones para que la población realice sus actividades en el ciberespacio de manera libre y confiable, a fin de mejorar su calidad de vida mediante el desarrollo digital en un marco de respeto a la libertad de expresión, vida privada y protección de datos personales".[7] Asimismo, desarrollar las capacidades tendentes a prevenir riesgos y amenazas en el ciberespacio que puedan alterar la independencia, integridad y soberanía nacional,[8] con especial énfasis en la prevención de acceso y manejo indebido a los sistemas y equipos de informática del Estado que contengan información sensible o clasificada como de seguridad nacional, es decir, aquella cuyo buen manejo es indispensable "para garantizar la integridad y la soberanía de la república, así como salvaguardar al país de riesgos y amenazas a fin de construir una paz duradera y fructífera."[9]

Si bien el Estado cuenta con áreas especializadas en materia de combate a los delitos informáticos, como la Dirección General Científica de la Guardia Nacional, la cual tiene entre sus facultades implementar acciones de vigilancia, identificación, monitoreo y rastreo en la red pública de Internet a fin de prevenir conductas ilícitas y el esclarecimiento de hechos delictivos de su competencia en su calidad de autoridad investigadora, o con instrumentos tales como el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos que tiene por objeto fortalecer la ciberseguridad en las dependencias federales, estatales, Organismos Constitucionales Autónomos, academia y sector privado, lo cierto es que sigue siendo imperativa una reforma al Código Penal Federal que establezca penalidades proporcionales a la comisión de estas conductas criminales.

No obstante, es importante destacar que la actual administración del Gobierno Federal ha fijado mediante los objetivos estratégicos 1.2 y 3.2 de la Estrategia Nacional de Seguridad Pública 2024-2030, precisamente como acciones estratégicas, el "implementar campañas de seguridad digital, con el fin de promover una cultura de prevención y denuncia de delitos en medios digitales" (1.2.1.6)[10] y "colaborar con las instancias competentes en el rastreo, análisis y preservación de evidencia digital, que contribuya a la prevención e investigación de delitos cibernéticos" (3.2.1.3),[11] por lo que la presente iniciativa es acorde, coherente y complementaria en relación a la visión de seguridad pública del Ejecutivo Federal.

Contexto Internacional

En el ámbito internacional, el Consejo de Seguridad de la Organización de las Naciones Unidas (ONU) ha exhortado a los Estados Miembros a establecer y reforzar alianzas nacionales, regionales e internacionales, tanto públicas como privadas, con el propósito de "prevenir, mitigar, investigar y responder a los daños ocasionados por ataques contra infraestructuras críticas, mediante el intercambio de información, la capacitación conjunta y el establecimiento de redes de alerta y comunicación pertinentes."[12]

Como resultado de este exhorto, en noviembre de 2001 se adoptó el Convenio de Budapest sobre Ciberdelincuencia, primer tratado internacional en la materia elaborado por el Consejo de Europa en Estrasburgo, cuyo objeto consiste en aplicar una política penal común encaminada a la protección de la sociedad frente al cibercrimen, mediante la armonización legislativa, el fortalecimiento de la cooperación internacional y el perfeccionamiento de las técnicas de investigación.

Este Convenio dio la pauta para la clasificación y tipificación de delitos cometidos por medio de herramientas electrónicas y el Internet, pero dados los rápidos avances tecnológicos, los países se han visto en la necesidad de modificar y actualizar sus leyes e incluso, en algunos casos, de crear agencias para la protección de sus ciudadanos y sus datos personales.

Ejemplo de lo anterior son:

- La Agencia Europea para Redes y Seguridad de la Información (ENISA);
- El Centro Nacional de Ciberseguridad del Reino Unido (NCSC);
- El Centro Australiano de Ciberseguridad.

Además, se ha realizado la modificación o creación de leyes específicas para la defensa de los usuarios y sus datos personales en el ciberespacio, como:

- Las directivas europeas del Network Information Service (NIS);
- La Ley de Protección Nacional de Ciberseguridad del 2015 de Estados Unidos (Nacional Cybersecurity Protection Advancement Act of 2015);
- La Ley de Ciberseguridad del 2017 de China;
- La adición de los artículos 579 al 588 de la Ley de Enjuiciamiento Criminal de España en 2015, y
- El Manual de Tallin 2.0 de Estonia, entre otras.

Si bien México no forma parte del Convenio de Budapest, se ha considerado indispensable crear un ambiente propicio para la cooperación internacional en materia de ciberseguridad,

con objeto de prevenir y mitigar los riesgos que implica la seguridad en las Tecnologías de la Información y Comunicación, así como la creación de figuras jurídico penales que inhiban las actividades delictivas vinculadas a la ciberdelincuencia entendida esta como "*aquellos delitos que se cometen mediante las TIC, ya sea en contra de individuos, empresas o gobierno*".

Derecho Comparado

El derecho comparado en relación con las penas por delitos informáticos implica analizar cómo diferentes países abordan y sancionan estas conductas delictivas.

El **Código de los Estados Unidos** (*US Code*), específicamente en su Título 18, Sección 1030 (18 U.S.C. § 1030), que lleva por nombre "Fraude y actividades relacionadas con la conexión a computadoras (*fraud and related activity in connection with* computers), es la principal legislación federal que aborda los delitos informáticos en perjuicio del gobierno de aquel país, al tiempo que tipifica una amplia gama de conductas delictivas vinculadas con el acceso indebido a sistemas informáticos, el fraude, la extorsión y abuso en el ciberespacio. Entre dichas conductas encontramos el acceso no autorizado o en exceso a la autorización a cualquier computadora protegida, la obtención ilícita de registros financieros, de agencias de crédito y a cualquier sistema de cualquier departamento o agencia de los Estados Unidos. Para ciertas hipótesis previstas en esta sección, el *US Code* prevé una punibilidad entre **10 y 20 años de prisión** .[13]

Por su parte, el **Código Penal brasileño** establece en su artículo 359-K, contenido en el Título XII "Delitos contra el Estado Democrático de Derecho", Capítulo I "Delitos contra la Soberanía Nacional" que revelar a un gobierno extranjero, a sus agentes o a una organización criminal, en contravención de lo dispuesto por la ley o normativa vigente, documentos o información clasificada como secreta o ultrasecreta, cuya divulgación pueda amenazar la preservación del orden constitucional o la soberanía nacional, se sanciona con **reclusión de 3 a 15 años** .

A continuación, se reproduce la cita textual de la disposición en comento:

> "Artículo 359-K. Entregar a gobierno extranjero, a sus agentes, o a organización criminal extranjera, en desacuerdo con determinación legal o reglamentaria, documento o información clasificados como secretos o ultrasecretos en los términos de la ley, cuya revelación pueda poner en peligro la preservación del orden constitucional o la soberanía nacional:
>
> **Pena – reclusión, de 3 (tres) a 12 (doce) años.**
>
> 1o. Incurre en la misma pena quien presta auxilio a espía, conociendo tal circunstancia, para sustraerlo a la acción de la autoridad pública
>
> 2o. Si el documento, dato o información es transmitido o revelado con violación del deber de sigilo:

Pena – reclusión, de 6 (seis) a 15 (quince) años. "[14]

Finalmente, el **Código Penal De La Federación De Rusia** en su sección X. "Delitos contra el Poder del Estado", Capítulo 29. "Delitos contra los fundamentos del Sistema Constitucional y Seguridad del Estado" artículo 276 establece que:

> "La transferencia, así como la recopilación, el robo o la conservación con el propósito de transferir a un Estado extranjero, a una organización extranjera o a sus representantes, **información que constituya un secreto de Estado**, así como la transferencia o **recopilación de otra información** bajo la orden de un servicio de inteligencia extranjero, **en detrimento de la seguridad exterior** de la Federación Rusa, si estos hechos han sido cometidos por un ciudadano extranjero o un apátrida, será punible con la privación de libertad por **un período de 10 a 20 años**."

Proporcionalidad de la pena

La proporcionalidad de las penas refiere a la idea de que la gravedad de la pena impuesta debe ser proporcional a la gravedad del delito cometido. Es decir, las sanciones deben ser adecuadas y proporcionales a la magnitud del daño causado y al nivel de culpabilidad del infractor.[15]

Al respecto, para el jurista y criminólogo Luis Rodríguez Manzanera:

> "Cualitativamente, la punibilidad debe ser idónea para la prevención, es decir, debe ser la adecuada para cumplir con su finalidad. Cuantitativamente, debe regir la magnitud del bien tutelado y la forma y calidad del ataque a este. De aquí, que la punibilidad tenga marcados limites, los cuales están determinados en primer lugar por la legitimación y la necesidad, y en segundo lugar por los derechos humanos y por el bien protegido." [16]

Ahora bien, la proporcionalidad de las penas encuentra sus fundamentos en la Constitución Política de los Estados Unidos Mexicanos.

Se establece en el artículo 22 de la Constitución mexicana,[17] el cual funda que las penas deben ser proporcionales al delito cometido y que no debe imponerse ninguna pena cruel, inhumana o degradante. Este principio constitucional se deriva de la idea de que las sanciones deben ser adecuadas y proporcionadas a la gravedad del delito y al nivel de culpabilidad del infractor.

La proporcionalidad de las penas también ha sido desarrollada y aplicada por la jurisprudencia de la Suprema Corte de Justicia de la Nación (SCJN), que es el máximo órgano judicial en México. La SCJN ha establecido criterios jurisprudenciales que exigen a los jueces considerar la proporcionalidad al imponer una pena, tomando en cuenta factores como la gravedad del delito, las circunstancias del caso y las características del infractor.

Al respecto, el ministro en retiro José Ramón Cossío Díaz, en su ponencia derivada del amparo directo en revisión 3931/2016, menciona:

> “Esta Suprema Corte ha concluido que **la gravedad de la pena debe ser proporcional a la del hecho antijurídico y del grado de afectación al bien jurídico protegido** , de manera que las penas más graves deben dirigirse a los tipos penales que protegen los bienes jurídicos más importantes. La gravedad de la conducta incriminada como la cuantía de la pena no sólo está determinada por el bien jurídico tutelado, la afectación a éste o el grado de responsabilidad subjetiva del agente, sino también por la incidencia del delito o la **afectación a la sociedad que éste genera** , siempre y cuando haya elementos para pensar que el legislador ha tomado en cuenta esta situación al establecer la pena. **Al respecto, este Alto Tribunal ha puesto de manifiesto la conveniencia de que el legislador exprese las razones que lo llevan a determinar una pena para un delito como un elemento especialmente relevante para evaluar la constitucionalidad de una intervención pena** l.”

Es importante destacar que, a pesar de los fundamentos legales y jurisprudenciales existentes, la aplicación efectiva y uniforme del principio de proporcionalidad de las penas en México puede presentar desafíos. La interpretación y determinación de la proporcionalidad puede variar entre jueces y tribunales, lo que puede dar lugar a disparidades en las penas impuestas. Esto ha generado debates y llamados a fortalecer la consistencia y uniformidad en la aplicación de la proporcionalidad de las penas en el sistema de justicia mexicano.

Conclusión

Finalmente, aumentar las penas por delitos informáticos enviaría un mensaje claro de que México toma en serio la protección de la ciberseguridad y está comprometido en combatir la delincuencia en línea. Penas más severas actuarían como un disuasivo significativo para los posibles delincuentes y reducirían la prevalencia de estos delitos.

Además, estaría en línea con los avances tecnológicos y la sofisticación de las tácticas utilizadas por los delincuentes informáticos. Es crucial que el marco legal se mantenga actualizado y refleje la gravedad y la complejidad de estos delitos para garantizar una justicia efectiva y proporcional.

Asimismo, el fortalecimiento de las penas en los delitos informáticos permitiría proteger la soberanía y la seguridad nacional, especialmente en un entorno en el que los ataques cibernéticos pueden tener consecuencias devastadoras en términos de estabilidad política, económica y social. La defensa de la infraestructura crítica y la protección de la información y datos gubernamentales son esenciales para preservar la integridad del Estado Mexicano.

Penas más elevadas garantizarían que las víctimas de delitos informáticos obtengan una sensación de justicia y compensación por los daños sufridos. Esto sería esencial para restaurar la confianza en el sistema legal y brindar alivio a aquellos afectados por la delincuencia cibernética.

Por tal razón, considero de particular importancia reformar el artículo 211 Bis 2 y el 211 Bis 3 con la finalidad de modificar la pena en los delitos informáticos contra el Estado Mexicano,

tomando en cuenta que el delito de sabotajes se encuentra en el artículo 140 del Código Penal Federal y es considerado una amenaza a la Seguridad Nacional y por ello debemos tomar como base su punibilidad para los demás delitos informáticos en contra del Estado.

> "**Artículo 140.-** Se impondrá pena de **cinco a diez años de prisión y multa de mil a cincuenta mil pesos** , al que dañe, destruya, perjudique o ilícitamente entorpezca vías de comunicación, servicios públicos, funciones de las dependencias del Estado, organismos públicos descentralizados, empresas de participación estatal, órganos constitucionales autónomos o sus instalaciones; plantas siderúrgicas, eléctricas o de las industrias básicas; centros de producción o distribución de artículos de consumo necesarios de armas, municiones o implementos bélicos, con el fin de trastornar la vida económica del país o afectar su capacidad de defensa.
>
> Se aplicará pena de **seis meses a cinco años** de prisión y multa hasta de cinco mil pesos, al que, teniendo conocimiento de las actividades de un saboteador y de su identidad, no lo haga saber a las autoridades. Las sanciones a que se refiere el primer párrafo de este artículo se aumentarán hasta en una mitad, cuando los actos de sabotaje se realicen en los ductos, equipos, instalaciones o activos, de asignatarios, contratistas, permisionarios o distribuidores a que se refiere la Ley Federal para Prevenir y Sancionar los Delitos Cometidos en Materia de Hidrocarburos.[18]

A efecto de aportar mayor claridad a la propuesta realizada, presento el siguiente cuadro comparativo:

CÓDIGO PENAL FEDERAL	
TEXTO VIGENTE	**TEXTO PROPUESTO**
Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.	**Artículo 211 bis 2.-** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de **cinco** a **diez** años de prisión y de doscientos a seiscientos días multa.
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.	Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de **cinco** a **diez** años de prisión y de cien a trescientos días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.	A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de **cinco** a **diez** años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.
Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.	Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.

Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.	**Artículo 211 bis 3.-** Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de **cinco** a **diez** años de prisión y de trescientos a novecientos días multa.
Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.	Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de **cinco** a **diez años** de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.
A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y	A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de **cinco** a **diez**

multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.	años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Por lo anteriormente expuesto, someto a consideración de este Honorable Pleno la siguiente iniciativa con proyecto de

Decreto por el que se reforman diversas disposiciones del Código Penal Federal

Artículo Único. – Se **reforman** los artículos 211 Bis 2 y 211 Bis 3 del Código Penal Federal para quedar como sigue:

Artículo 211 Bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de **cinco** a **diez** años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de **cinco** a **diez** años de prisión y de cien a trescientos días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de **cinco** a **diez** años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá, además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.

Artículo 211 Bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de **cinco** a **diez** años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de **cinco** a **diez años** de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de **cinco** a **diez** años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá, además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Transitorio

Único. - El presente decreto entrara en vigor el día siguiente al de su publicación en el Diario Oficial de la Federación.

Notas

1 INEGI, Encuesta Nacional sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares (ENDUTIH). 2023.

2 Balcombe, Luke. The Mental Health impacts of internet scams. Int J. Environ Res Public Health. 2025.

3 INEGI, Módulo sobre Ciberacoso (MOCIBA) 2023. Consultable en: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2024/MOCIBA/MOCIBA2023.pdf

4 INEGI, Censo Nacional de Seguridad Pública Estatal (CNSPE) 2024. Consultable en: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2024/CNSPE/CNSPE2024.docx

5 Consejo de la Unión Europea. Directiva 2008/114/CE de 8 de diciembre de 2008. Publicada en el Diario Oficial de la Unión Europea de fecha 23 de diciembre de 2008. Consultable en: www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/DirectivaEu ropea2008-114-CE.pdf

6 Ministerio de Tecnologías de la Información y las Comunicaciones de la República de Colombia. Tecnologías de la Información y las Comunicaciones (TIC) Consultable en:

https://mintic.gov.co/portal/inicio/Glosario/T/5755:Tecnologias-de-la-Informacion-y-las-Comunicaciones-TIC

7 Instituto Federal de Telecomunicaciones (IFT). Ciberseguridad en México y en otros países. 2021. Página 4.

8 Ibidem.

9 Centro Nacional de Inteligencia (CNI), ¿Qué es la seguridad nacional?, Consultable en: https://www.gob.mx/cni/documentos/conoce-que-es-la-seguridad-nacional

10 Gobierno de México, Estrategia Nacional de Seguridad Pública 2024-2030. México. 2024. Página 27. Consultable en: https://sil.gobernacion.gob.mx/Archivos/Documentos/2025/04/asun_4874274_20250408_1744153605.pdf

11 Ídem, p. 33.

12 https://www.un.org/counterterrorism/es/cybersecurity

13 United States Code. (n.d.). Title 18, Section 1030: Fraud and related activity in connection with computers. Consultable en: https://uscode.house.gov/

14 Camara dos Deputades do Brasil. (1940). Código Penal, Art. 359-K: Espionaje y violación del deber de secreto. Ley número 2.848, de 7 de diciembre de 1940. Consultable en: https://legis.senado.leg.br/sdleg-getter/documento?disposition=inline&dm=8965742&utm_source=chatgpt.com.

15 Yenissei Rojas, Ivonne. La proporcionalidad de las penas. En Cienfuegos Salgados, David (et. al) El ilícito y su castigo. Reflexiones sobre la cadena perpetua, la pena de muerte y la idea de sanción en el derecho. Instituto de Investigaciones Jurídicas. Universidad Nacional Autónoma de México. 2009. Consultable en: https://archivos.juridicas.unam.mx/www/bjv/libros/6/2937/15.pdf

16 Rodríguez Manzanera, Luis. Penología. Cuarta edición. Porrúa. México.

17 https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

18 https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf

Dado en el Palacio Legislativo de San Lázaro, a 17 de septiembre de 2025.

Diputado Humberto Coss y León Zúñiga (rúbrica)