

GOBIERNO DE PUERTO RICO

20^{ma}. Asamblea
Legislativa

3^{ra}. Sesión
Ordinaria

SENADO DE PUERTO RICO

P. del S. 974

22 de enero de 2026

Presentado por el señor *Ríos Santiago*

Referido a

LEY

Para añadir un nuevo Título VI – Delitos Cibernéticos; reenumerar el actual Título VI como Título VII; reenumerar los actuales Artículos 301, 302, 303, 304, 305, 306, 307, 308 y 309, para ser reenumerados como los Artículos 377, 378, 379, 380, 381, 382, 383, 384 y 385, de la Ley Núm. 146-2012, según enmendada, conocida como “Código Penal de Puerto Rico”, a los fines de tipificar delitos cibernéticos y otros conexos de los mismos; y para otros fines relacionados.

EXPOSICIÓN DE MOTIVOS

Esta Asamblea Legislativa tiene la responsabilidad constitucional de salvaguardar la vida, propiedad y seguridad de todos los miembros de nuestra sociedad. En cumplimiento con dicha responsabilidad constitucional, corresponde tomar las medidas necesarias para prevenir, controlar y reducir la incidencia de la actividad criminal, incluyendo las conductas del mundo cibernético.

La aplicación de una pena sobre un individuo constituye una de las muestras más abarcadoras de la intensidad que puede asumir el castigo estatal. Esta afirmación se vuelve clara con solo pensar en el modo más usual en que una persona encontrada culpable de un delito es afectada con la pérdida de su libertad. Así, la detención o arresto de una persona para ser privada de su libertad se transforma en el ejemplo paradigmático

de la sanción penal. Desde luego existen otras penas que impactan sobre el patrimonio (sanciones y multas) o en la capacidad para ejercer algún cargo, profesión o función. La gravedad de las penas en su aplicación debe estar prevista únicamente para aquellos actos específicos que el estado ha identificado y establecido mediante Ley. No obstante, la tarea de creación de delitos debe ser llevada a cabo con sumo cuidado, a fin de evitar vaguedad en su tipificación y/o con el establecimiento de una punibilidad que resulte de manera excesiva o represiva por parte del estado.

La formulación de leyes penales es un proceso continuo que obedece a las condiciones sociales en determinado momento histórico. Según expresan las teorías de legislación penal, todo Código Penal debe ser el reflejo diáfano y genuino de los valores de la sociedad para la cual se legisla. De igual forma, no debemos perder de perspectiva que la creación de delitos va atada a ciertos principios fundamentales para una sociedad democrática. Así, toda tipificación de conducta delictiva, sanción y multa, deben ser realista, acorde con los tiempos que se viven y lo suficientemente abarcadora y flexible en miras de un futuro previsible o probable. Debe, además, ser susceptible de ajuste para atemperarlo a las situaciones cambiantes, según éstas acontecen.

Es por ello que, el debido proceso de ley pone sobre la Asamblea Legislativa la obligación de que las normas que prescriben las conductas prohibidas deben ser claras y precisas, de manera que se respete el principio de legalidad. En atención al tema cibernético, cabe destacar que, la tecnología se ha convertido en uno de los principales soportes del mundo que a su vez permite llevar a cabo muchas tareas en una fracción de tiempo. A medida que la computadora se ha convertido en algo común en un mundo globalizado, los crímenes han sobrepasado la esfera natural para llegar al mundo cibernético.

Se conoce como delito cibernético, cualquier conducta ilegal o delictiva en el que se haya utilizado un equipo, una Red o un dispositivo de hardware. Existen varios tipos de delitos cibernéticos, entre los cuales podemos mencionar: acoso cibernético, fraude, falsificación, crimen pornográfico, piratería cibernética, "Sexting", "Grooming", "Hacking", entre otros.

Además, traemos a colación algunos artículos periodísticos que datan y fundamentan la importancia de reglamentar este campo.

Según publicado en la Red noticiosa NotiCel, las víctimas de crímenes cibernéticos en Puerto Rico perdieron en el año 2019 alrededor de \$7.7 millones de dólares, de acuerdo con un informe estadístico publicado por el Negociado Federal de Investigaciones (FBI), para un total de 839 víctimas de crímenes cibernéticos.

Por otro lado, para el 26 de enero de 2019¹, se dijo que, Puerto Rico se encuentra entre los primeros cinco mercados de mayor incidencia de ciberataques de todo el Caribe, región que es víctima de sobre 150 millones de ciberataques anuales, con pérdidas multimillonarias, sostuvo Marc Asturias, vicepresidente de Mercadeo y Relaciones Públicas de Fortinet para América Latina y el Caribe. El problema se complica ya que, según el experto, la mayoría de las víctimas, empresas como ciudadanos, desconocen que han sido “hackeados”. La situación se agudiza en la medida en que se sigan ampliando “las superficies de interconexión”. Se estima que cada persona cuenta hoy con entre cinco a siete dispositivos conectados a la internet, pero alrededor del 60% de las empresas que sirven a estas conexiones no poseen la capacidad de servicio de seguridad adecuada para garantizar o minimizar los ciberataques. Esta práctica a nivel global representa pérdidas ascendentes a los \$7.8 trillones. Cada 39 segundos se registra un ataque y para el 2021 se estima que el daño por la ciberdelincuencia costará al mundo más de \$6 billones. El 65% de todas las vulneraciones de datos involucran errores de los empleados y el 65% de los ciberataques se dirigen a las pequeñas y medianas empresas.

Asimismo, se señaló que desde el año 2011 al 2018 se había “disparado 10,000 veces lo que era antes y aunque las empresas han aumentado en un 75% sus gastos en ciber seguridad, aun no es suficiente para detener la práctica”, apuntó Asturias. Sostuvo, además, que otro de los retos, es la expansión que se está experimentando a través de las cámaras de las computadoras, los monitores de los bebés, los sistemas de alarmas, entre

¹ Rosado, I. V., & Vocero, E. L. (2019, enero 26). *Fuerte el reto local contra el Ciberataque*. El Vocero de Puerto Rico. https://www.elvocero.com/economia/fuerte-el-reto-local-contra-el-ciberataque/article_85200d46-20e2-11e9-98c2-032f916e5677.html.

otros servicios, que son valiosos, pero amplían la superficie de ataque, porque no están protegidos contra el “hacker”.

Además, es claro que nuestro Gobierno no ha quedado inmune a la delincuencia cibernética. Como, por ejemplo, el pasado 2 de diciembre de 2025 el periódico Primera Hora publicó una noticia donde se explica que una compañía de tecnología contratada por el Gobierno de Puerto Rico sufrió un ataque cibernético, afectando al Departamento de Educación, ASES y a la Corporación del Fondo de seguro del Estado. Por otro lado, en reportaje de 1 de noviembre de 2024, el mismo rotativo publicó que PRITS había registrado la cantidad de 82,089,132 intentos de ataques cibernéticos.

Lamentablemente, existen delitos tipificados en el Código Penal y leyes especiales relacionadas a crímenes cibernéticos, de manera muy limitada. Los problemas ocasionados por los crímenes cibernéticos, por su complejidad y características particulares, deben contar con una sección propia dentro del Código Penal donde se recogen los delitos ordenados por todo por tópico de esta conducta delictiva. Ello motiva la presente legislación, además de la protección de nuestra ciudadanía de este tipo de conducta indeseable.

Por tales acontecimientos, otros similares y todo lo antes expuesto es que, esta pieza legislativa representa un esfuerzo legítimo para hacer la inclusión de múltiples delitos, penas, sanciones y/o multas dentro del mundo cibernético, reformulando ciertos actos y conductas por omisión y/o negligencia en nuestro ordenamiento jurídico penal, siendo el instrumento eficaz para la administración de la justicia criminal y devolver a la ciudadanía la seguridad jurídica que tanto merece.

El principio de legalidad de nuestro actual Código Penal esboza que no se instará acción penal contra persona alguna por hechos que no estén expresamente definidos como delito en el código o mediante leyes especiales, ni se impondrá pena o medidas de seguridad que la ley no establezca con anterioridad a los hechos. Tampoco se podrá crear ni imponer delitos, penas, ni medidas de seguridad por analogía a una conducta que se parezca, más no sea igual a la tipificada en el Código Penal.

Este nuevo Título VI ha sido atemperado a la legislación especial relativa a la administración de la justicia en este tipo de caso. Asimismo, se han redefinido e incluido nuevas figuras jurídicas para conformarlas a las directrices ofrecidas por el Tribunal Supremo de Puerto Rico y el Tribunal Supremo de Estados Unidos en interpretación de las garantías constitucionales. A esos efectos, hemos puesto énfasis sobre la protección a la intimidad, la propiedad, el patrimonio del Estado y de los individuos, los fondos públicos, la propiedad intelectual, la vida y la libertad de expresión, entre otros.

En tema del establecimiento de la responsabilidad penal, se mantiene muy presente la expresión contenida en nuestra Constitución que establece con jerarquía constitucional el carácter rehabilitador de la pena al disponer en su Artículo VI, Sección 19, que las instituciones penales preponderarán “el tratamiento adecuado de los delincuentes para hacer posible su rehabilitación moral y social”; que “no se impondrán castigos crueles e inusitados” y que las “multas no serán excesivas”. Artículo II, Secciones 11 y 12 de la Constitución de Puerto Rico. A esos efectos, se reconocen como principios fundamentales que la sanción penal no podrá atentar contra la dignidad humana y la rehabilitación moral y social del convicto como un objetivo general para la imposición de las penas. De igual manera, ponemos especial atención en velar por la confianza pública imponiendo sobre los funcionarios o empleados públicos la obligación de rectitud e integridad en el cumplimiento de su deber y la destitución de su cargo o empleo como pena cuando infrinja la ley en el desempeño de las funciones públicas.

DECRÉTASE POR LA ASAMBLEA LEGISLATIVA DE PUERTO RICO:

1 Sección 1.- Se añade un nuevo Título VI – Delitos Cibernéticos a la Ley Núm. 146-
2 2012, según enmendada, conocida como “Código Penal de Puerto Rico”, para que lea
3 como sigue:

4 "TITULO VI. - DELITOS CIBERNÉTICOS

5 CAPITULO I. – DELITOS INFORMÁTICOS COMO OBJETO

SECCIÓN PRIMERA. – *Definiciones.*

Artículo 301. – Definiciones.

1. ***“Acceso Ilícito” o “Piratería”***, se entiende como cualquier medio para entrar a otro sistema informático, con inclusión de los ataques por internet, así como el acceso ilícito a las redes inalámbricas y el acceso no autorizado a los ordenadores que no están conectados a ninguna red.
2. ***“Acceso Ilegal o Indebido a los Sistemas de Información”***, se entiende como el acceso no autorizado, al conjunto o a una parte de un sistema de información cuando se comete transgrediendo medidas de seguridad.
3. ***“Adquisición Ilegal”***, se entiende como la interceptación de los procesos de transferencia de datos.
4. ***“Ataques a la Integridad del Sistema”***, se entiende como toda obstaculización deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.
5. ***“Datos Informáticos”***, se entiende toda representación de hechos, información o conceptos de una forma que permita su procesamiento en un sistema de computadoras, incluido un programa capaz de provocar que un sistema informático realice una función.
6. ***“Difusión de Material Racista y Xenófobo Mediante Sistemas Informáticos”***, se entiende como todo material escrito, toda imagen o cualquier otra representación de ideas o teorías, que propugne, promueva o incite al odio, la discriminación o la

1 *violencia, contra cualquier persona o grupo de personas, por razón de raza, color,*
2 *ascendencia u origen nacional o étnico, así como de la religión.*

3 **7. “Espionaje de Datos”,** *se entiende como toda persona que, intencionalmente, sin*
4 *excusa o justificación legal o en exceso de una excusa o justificación legal obtenga, para*
5 *sí o para otro, datos informáticos que no estén destinados a él y que estén especialmente*
6 *protegidos contra el acceso no autorizado.*

7 **8. “Espionaje Económico”,** *se entiende como toda persona que, intencionalmente o a*
8 *sabiendas de que la intrusión beneficiará a cualesquiera gobiernos, agencias o agentes*
9 *extranjeros:*

10 *a) robe o, sin autorización, se apropie de, tome, se lleve u oculte, o mediante fraude,*
11 *artificio o engaño, obtenga un secreto comercial;*

12 *b) sin autorización copie, duplique, esboce, dibuje, fotografíe, descargue, cargue,*
13 *altere, destruya, fotocopie, replique, transmita, entregue, expida, envíe por*
14 *correo electrónico, comunique o transporte un secreto comercial;*

15 *c) reciba, compre o posea un secreto comercial, a sabiendas de que éste ha sido*
16 *robado o ha sido objeto de apropiación, obtenido o convertido sin autorización;*

17 *d) intente cometer cualesquiera de los actos descritos en los anteriores incisos a)*
18 *b) y c); o*

19 *e) conspire con una o más personas para cometer cualquiera de los actos descritos*
20 *en los anteriores incisos a) b) y c) y una o más de esas personas actúe para llevar*
21 *a la práctica el objeto de la conspiración.*

1 **9. “Falsificación Informática o Phishing”**, se entiende como la introducción,
2 alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que
3 genere datos no auténticos con la intención de que sean tomados o utilizados a efectos
4 legales como auténticos, con la independencia de que los datos sean legibles e
5 inteligibles directamente.

6 **10. “Hostigamiento, Intimidación o Cyberbullying”**, se entiende como cualquier
7 patrón de acciones realizados intencionalmente, ya sea mediante abuso psicológico,
8 físico, cibernético o social, que tenga el efecto de atemorizar a una persona o a un grupo
9 de personas.

10 **11. “Incautar”**, incluye:

- 11 a) activar cualquier computadora y medio de almacenamiento de datos
- 12 informáticos;
- 13 b) crear y conservar una copia de datos informáticos;
- 14 c) mantener la integridad de los datos informáticos pertinentes almacenados;
- 15 d) suprimir o hacer que no pueda accederse a datos informáticos existentes en el
- 16 sistema de computadoras al que se accede;
- 17 e) imprimir una copia de los datos informáticos salientes; o
- 18 f) incautar o asegurar de manera similar un sistema de computadoras o parte de
- 19 este, o un medio de almacenamiento de datos informáticos.

20 **12. “Infraestructura Esencial”**, se entiende como aquellos sistemas, aparatos y redes de
21 información, programas y datos informáticos que resultan tan vitales para el país que
22 la incapacitación, destrucción o interferencia de tales sistemas y activos supondría un

1 *menoscabo de la seguridad, la seguridad económica o nacional, la salud y protección*
2 *pública general o cualquier combinación de estos factores.*

3 **13. “Interceptación”**, se entiende, entre otras cosas, la adquisición, visualización y
4 *captación de cualquier comunicación de datos informáticos, ya sea por medios*
5 *alámbricos, inalámbricos, electrónicos, ópticos, magnéticos, verbales o de otro tipo,*
6 *durante la transmisión a través de la utilización de cualquier dispositivo técnico.*

7 **14. “Interferencia con Datos”**, se entiende cuando una persona, deliberada o
8 *imprudentemente, sin excusa o justificación legal, realice cualesquiera de los siguientes*
9 *actos:*

10 *a) destruya o altere datos;*

11 *b) haga que los datos resulten incompresibles, inútiles o ineficaces;*

12 *c) obstruya, interrumpa o interfiera con la utilización legal de los datos;*

13 *d) obstruya, interrumpa o interfiera con cualquier persona en la utilización legal*
14 *de los datos; o*

15 *e) deniegue el acceso a los datos a cualquier persona con derecho a acceder a los*
16 *mismos.*

17 *El inciso a) se aplica independientemente del hecho de que el acto de la persona tenga*
18 *un efecto temporal o permanente.*

19 **15. “Interceptación Ilegal”**, se entiende como la obtención o intrusión deliberada e
20 *ilegítima por medios técnicos de datos informáticos en transmisiones no públicas*
21 *dirigidas a un sistema informático, originados en un sistema informático o efectuados*

dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos.

16. “Material Erótico, Obsceno y Pornográfico”, se entiende como cualquier libro, revista, periódico u otro material impreso, escrito, o digital, o cualquier retrato, fotografía, dibujo, caricatura, película de movimiento, cinta cinematográfica u otra representación gráfica; o cualquier representación oral o visual transmitida o retransmitida a través de cables, ondas electromagnéticas, computadoras, tecnología digital o cualesquiera medios electrónicos o de comunicación telemática; o cualquier estatua, talla o figura, escultura; o cualquier grabación, transcripción o reproducción mecánica, química o eléctrica o cualquier otro artículo, equipo o máquina.

Además, se entiende como “material” todo aquello que considerado en su totalidad por una persona promedio y que al aplicar patrones comunitarios contemporáneos:

- a) apele al interés lascivo, o sea, a un interés morboso en la desnudez, sexualidad o funciones fisiológicas;
- b) represente o describa en una forma patentemente ofensiva conducta sexual; y
- c) carezca de un serio valor literario, artístico, religioso, científico o educativo.

La atracción del material al interés lascivo en el sexo se juzga en referencia al adulto promedio, a menos que se desprenda de la naturaleza del material, o de las circunstancias de su diseminación, distribución o exhibición, que está diseñado para grupos con desviaciones sexuales, en cuyo caso dicha atracción se juzgará con referencia al grupo a quien va dirigido.

1 *En procesos de violación a las disposiciones de esta Sección, donde las circunstancias*
2 *de producción, presentación, venta, diseminación, distribución, o publicidad indican que*
3 *el acusado está explotando comercialmente el material por su atracción lasciva, la prueba*
4 *de este hecho constituirá prueba prima facie de que el mismo carece de serio valor literario,*
5 *artístico, religioso, científico o educativo.*

6 *Cuando la conducta prohibida se lleve a cabo para, o en presencia de, personas menores*
7 *de edad, bastará que el material tenga por objeto suscitar o despertar un interés lascivo en*
8 *la actividad sexual. Incluirá, además, cualquier modalidad de anuncio, promoción o*
9 *facilitación de actividad sexual a través de medios electrónicos o de comunicación por*
10 *internet.*

11 **17. "Material Explícito",** *se entiende como todo material de contenido, íntimo sexual*
12 *alguna imagen del cuerpo humano o sus partes; o sexualmente explícito, que incluya*
13 *algún tipo de actividad sexual; íntima o de pareja, ya sea visual, ilustrativo o gráfico,*
14 *grabaciones de video o audio.*

15 **18. "Medio de Almacenamiento de Datos Informáticos",** *se entiende como todo*
16 *artículo o material a partir del cual es posible reproducir información, con o sin ayuda*
17 *de cualquier otro artículo o dispositivo.*

18 **19. "Permanencia Ilegal",** *se entiende como toda persona que intencionalmente, sin*
19 *autorización o justificación legal, o excediéndose de una excusa o justificación legal,*
20 *permanezca conectado en un sistema informático o en parte de un sistema informático*
21 *o siga utilizando un sistema informático.*

22 **20. "Perturbación",** *se entiende como manipulaciones que comprenden:*

- a) *cortar el suministro eléctrico a un sistema de computadoras;*
- b) *causar interferencias electromagnéticas a un sistema de computadoras;*
- c) *corromper por cualquier medio un sistema de computadoras; e*
- d) *ingresar, transmitir, dañar, borrar, deteriorar, alterar o suprimir datos informáticos del sistema.*

21. “Pornografía Infantil”, se entiende como toda representación, por cualquier medio, de un menor de edad o persona que luzca como tal, dedicado a actividades sexuales explícitas o implícitas, reales o simuladas, o toda representación de las partes genitales de un menor de edad o persona que luzca como tal, con fines primordialmente sexuales. Esta incluye, pero no se limita a, todo material pornográfico sonoro, visual o escrito.

22. “Programas Maliciosos o Malware”, se entiende como aquella programación creada para causar daño a un dispositivo, sistemas o a sus usuarios, que pueden incluir desde daños leves hasta destrucción total del sistema.

23. “Protocolo de Internet o IP”, se entiende como las direcciones numéricas estándar que se emplea para el envío y recepción de información mediante una red con la posibilidad de confirmar que un paquete de información o datos llegó a su destino.

24. “Proveedor de Hospedaje”, se entiende como toda persona física o jurídica que presta un servicio de transmisión electrónica de datos mediante el almacenamiento de la información proporcionada por un usuario del servicio.

25. “Proveedor de Servicio”, se entiende como toda entidad pública o privada que ofrece a los usuarios de su servicio la capacidad de comunicar por medio de un sistema de

computadoras, y cualquier otra entidad que procese o almacene datos informáticos en nombre de dicho servicio de comunicación o de los usuarios de dicho servicio.

26. “Redes Informáticas”, se entiende como un grupo de sistemas interconectados o relacionados en que uno o varios de ellos llevan a cabo, con arreglo a un programa, el procesamiento automático de datos o cualquier otra función análoga.

27. “Seducción de un Menor de Edad, Preparación o Captación, o Grooming”, se entiende como aquel acto preparatorio ejecutado a través de tecnologías de la información y la comunicación, cuyo propósito sea propiciar un encuentro con una persona menor de edad con la intención de perpetrar abuso sexual en su contra.

28. “Sistema Informático”, se entiende como la estructura integrada por uno o varios aparatos interconectados o relacionados que ejecutan, de conformidad con un programa, el procesamiento automático de datos u otras funciones.

29. “Usurpación de Identidad”, se entiende como el acto de obtener, poseer, transferir o utilizar información relacionada con la identidad de otra persona, sin autorización para ello.

SECCIÓN SEGUNDA – Delitos Informáticos y Conexos

Artículo 302. – Acceso Indebido a Sistema Informático.

El que, sin autorización o excediendo una autorización en todo o en parte utilice, instale o acceda a un sistema informático o sistema telemático o de telecomunicaciones, o a sus componentes, protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a exigirlo, incurrirá en delito menos grave.

1 *El acceso indebido a sistema informático incluye, pero no se limita a:*

- 2 a) *Modificar, a través de cualquier forma de engaño o treta cualesquiera de las*
3 *funciones de la computadora u ordenador, incluyendo, pero no limitado al acceso*
4 *a la computadora u ordenador, la página cibernética donde la computadora u*
5 *ordenador activa su sistema de navegación en la Internet y las marcas o*
6 *“bookmarks” que el usuario autorizado o dueño han registrado en la*
7 *computadora u ordenador.*
- 8 b) *Recolectar, a través del uso de cualquier forma de engaño o treta, información*
9 *personal confidencial del usuario autorizado o dueño, incluyendo cuando dicha*
10 *acción se realiza a través de uso de un dispositivo que graba todos los usos del*
11 *teclado de un usuario autorizado y transfiere tal información a otro ordenador o*
12 *persona; cuando dicha acción se realiza a través de acceder sin autorización el*
13 *historial de páginas de la “Internet” visitadas por el usuario autorizado y*
14 *cuando dicha acción se realiza extrayendo del disco duro del ordenador*
15 *información sin la autorización expresa del usuario autorizado o dueño.*
- 16 c) *Prevenir, a través del uso de cualquier forma de treta o engaño, el que un usuario*
17 *autorizado pueda detectar que su ordenador ha sido intervenido, se le ha*
18 *insertado programación o se ha sustraído información sin su autorización.*
- 19 d) *Representar, intencionalmente, de forma electrónica, que la computadora u*
20 *ordenador ha eliminado un programa de espionaje cibernético o un virus, a*
21 *sabiendas que dicha información es falsa.*

1 e) *Intencionalmente o a través de treta o engaño lograr inutilizar el sistema de*
2 *seguridad, anti-espionaje cibernético o antivirus en una computadora.*

3 *Cuando de dicho acceso ilícito resulte la supresión o la modificación de datos,*
4 *información o contenido en el sistema, o revelen o difundan datos confidenciales o personales*
5 *contenidos en el sistema accedido, será sancionada con pena de reclusión por un término fijo de*
6 *cinco (5) años.*

7 **Artículo 303. – Sabotaje Informático.**

8 *Toda persona que, sin autorización o excediendo una autorización, destruya o inutilice*
9 *en todo o en parte un sistema informático o sistema telemático o de telecomunicaciones o a sus*
10 *componentes, o impida, altere, entorpezca, obstaculice o modifique su funcionamiento o uso*
11 *regular o acceso, protegido o no con una medida de seguridad, será sancionada con pena de*
12 *reclusión por un término fijo de tres (3) años.*

13 **Artículo 304. – Sabotaje Informático Agravado.**

14 *Sera sancionada con pena de reclusión por un término fijo de cinco (5) años toda persona*
15 *que cometa el delito de sabotaje informático descrito en el Artículo 303, cuando se lleve a cabo*
16 *para obtener beneficio personal o de un tercero. El tercero beneficiado incurrirá igualmente en*
17 *este delito.*

18 *En caso de que la persona responsable obtenga o logre efectivamente el beneficio personal*
19 *perseguido, la pena de reclusión será por término fijo de ocho (8) años.*

1 **Artículo 305. – Ataque a la Integridad de Sistemas Informáticos del Sistema**
2 **Público.**

3 *Toda persona que, sin autorización o excediendo una autorización, destruya, dañe,*
4 *borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado*
5 *o suprima datos informáticos, mensajes de correo electrónicos, a sistemas del servicio público*
6 *del Gobierno de Puerto Rico, cuyo contenido sea esencial para su funcionamiento o desarrollo*
7 *de programas, de tratamiento de información, telemático o de telecomunicaciones a todo o en*
8 *parte de sus componentes, protegido o no con una medida de seguridad, será sancionada con*
9 *pena de reclusión por un término fijo de ocho (8) años.*

10 **Artículo 306. – Ataque a la Integridad de Sistemas Informáticos del Sistema**
11 **Público Agravado.**

12 *Sera sancionada con pena de reclusión por un término fijo de diez (10) años toda persona*
13 *que cometa el delito de ataque a la integridad de sistemas informáticos del sistema público*
14 *descrito en el Artículo 305, cuando de dicho acceso ilícito sobrevenga peligro colectivo o daño*
15 *social.*

16 *Si del delito descrito en el párrafo anterior sobreviene la pérdida de fondos públicos que*
17 *sobrepase de cinco (5,000) mil dólares, será sancionada con pena de reclusión por un término*
18 *fijo de quince (15) años. El Tribunal también podrá imponer pena de restitución.*

19 **Artículo 307. – Explotación Informática.**

20 *Será sancionada con pena de reclusión por término fijo de ocho (8) años toda persona*
21 *que, sin autorización o excediendo una autorización en todo o en parte, utilice, instale o acceda*
22 *a un sistema informático, telemático o de telecomunicaciones, esté o no protegido con medidas*

1 *de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien ostente el*
2 *legítimo derecho a exigirlo, con el propósito de explotar ilegítimamente el acceso logrado,*
3 *modificar un portal web, desviar o redireccionar el tráfico de datos o voz, u ofrecer a terceros*
4 *los servicios que estos sistemas proveen, sin que medie pago a los proveedores legítimos de tales*
5 *servicios.*

6 **Artículo 308. – Daño Informático.**

7 *Toda persona que, sin autorización o excediendo una autorización a propósito, con*
8 *conocimiento o temerariamente, destruya, dañe o vandalice en todo o en parte los datos*
9 *contenidos en un sistema de información, telemático o de telecomunicaciones o de sus*
10 *componentes, protegido o no con una medida de seguridad, o en perjuicio de un tercero,*
11 *suprima, modifique o destruya la información contenida, será sancionada con pena de reclusión*
12 *por un término fijo de cinco (5) años.*

13 *La persona que resulte convicta por el delito descrito en el párrafo anterior será*
14 *sancionada con pena de reclusión por un término fijo de tres (3) años cuando la comisión del*
15 *delito obedezca a negligencia, imprudencia, impericia o inobservancia de las normas aplicables.*

16 **Artículo 309. – Daño Informático Agravado.**

17 *Será sancionada con pena de reclusión por un término fijo de ocho (8) años toda persona*
18 *que cometa el delito de daño informático descrito en el Artículo 308, cuando se cometiere en*
19 *contra de los componentes de un sistema informático que utilice tecnologías de información y*
20 *comunicación, destinadas a la prestación de servicios públicos o financieros, o que contengan*
21 *información personal, confidencial, reservada, patrimonial, técnica o propia de personas*
22 *naturales o jurídicas.*

1 **Artículo 310. – Revelación De Secretos.**

2 *Toda persona que, sin autorización o excediendo una autorización a propósito, con*
3 *conocimiento o temerariamente modifique, destruya, obtenga, copie o utilice información de*
4 *seguridad pública en todo o en parte de los datos contenidos en un sistema de información,*
5 *telemático o de telecomunicaciones o de sus componentes, protegido o no con una medida de*
6 *seguridad, será sancionada con pena de reclusión por un término fijo de cinco (5) años.*

7 **Artículo 311. – Revelación de Secretos Agravado.**

8 *Sera sancionada con pena de reclusión por un término fijo de ocho (8) años toda persona*
9 *que para beneficio personal o de un tercero, cometa el delito de revelación de secretos descrito*
10 *en el Artículo 310, cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite*
11 *la administración o aplicación de la justicia, o recaiga sobre los registros relacionados con un*
12 *procedimiento penal resguardados por las autoridades competentes. El tercero beneficiado*
13 *incurrirá igualmente en este delito.*

14 *Cuando el delito descrito en el párrafo anterior sea perpetrado por un funcionario*
15 *público, éste será sancionado con pena de reclusión por un término fijo de quince (15) años.*
16 *Además, se impondrá destitución inmediata del cargo público e inhabilitación por término de*
17 *cuatro (4) a diez (10) años para desempeñarse en cualquier empleo, puesto o cargo público,*
18 *contados a partir del cumplimiento de la pena de reclusión.*

19 **Artículo 312. – Instalación o Propagación de Programas Informáticos**
20 **Maliciosos.**

21 *Toda persona que, sin autorización o excediendo una autorización a propósito y por*
22 *cualquier medio, instale programas informáticos maliciosos en un sistema o red informática o*

1 *telemática, o en los contenedores electrónicos, ópticos o magnéticos, o de sus componentes,*
2 *protegidos o no con medidas de seguridad, será sancionada con pena de reclusión por un*
3 *término fijo de tres (3) años.*

4 **Artículo 313. – Instalación O Propagación De Programas Informáticos**
5 **Maliciosos Agravado.**

6 *Será sancionada con pena de reclusión por un término fijo de cinco (5) años toda persona*
7 *que cometa el delito de instalación o propagación de programas informáticos descrito en el*
8 *Artículo 312, cuando:*

- 9 a) *Induzca a error a otra persona para que instale un programa malicioso en un sistema*
10 *o red informática o telemática, o en los contenedores electrónicos, ópticos o*
11 *magnéticos, sin la debida autorización;*
- 12 b) *Sin autorización, instale programas o aplicaciones informáticas dañinas en sitios de*
13 *internet legítimos, con el propósito de convertirlos en medios idóneos para la*
14 *propagación de programas informáticos maliciosos;*
- 15 c) *Para propagar programas informáticos maliciosos, invite a otras personas a*
16 *descargar archivos o acceder a sitios de internet que faciliten la instalación de*
17 *programas informáticos maliciosos;*
- 18 d) *Distribuya programas informáticos diseñados para la creación de programas*
19 *informáticos maliciosos;*
- 20 e) *Ofrezca, contrate o brinde servicios de denegación de servicios, envío de*
21 *comunicaciones masivas no solicitadas, o propagación de programas informáticos*
22 *maliciosos, para beneficio personal o de un tercero.*

1 *Será sancionada con una pena de reclusión por un término fijo de ocho (8) años cuando*
2 *el autor del delito descrito en el párrafo anterior afecte:*

- 3 *a) Entidades bancarias, financieras, cooperativas de ahorro y crédito, asociaciones*
4 *solidaristas o entes estatales;*
- 5 *b) El funcionamiento de servicios públicos;*
- 6 *c) Sistemas Informáticos que permitan obtener control a distancia para integrar redes*
7 *de ordenadores;*
- 8 *d) Sistemas Informáticos diseñados para realizar acciones dirigidas a procurar*
9 *beneficio patrimonial para sí o para un tercero;*
- 10 *e) Sistemas Informáticos de la salud, cuya afectación pueda poner en peligro la vida o*
11 *salud de las personas;*
- 12 *f) Programas con capacidad de reproducción autónoma sin intervención adicional del*
13 *usuario legítimo del sistema informático.*

14 ***Artículo 314. - Uso de Programas Destructivos.***

15 *Será sancionada con pena de reclusión por un término fijo de un (1) año toda persona*
16 *que, con la intención de producir daño, adquiera, distribuya o ponga en circulación programas*
17 *o instrucciones informáticas destructivas susceptibles de causar perjuicio a registros,*
18 *programas o equipos de computación.*

19 ***Artículo 315. - Dispositivos Fraudulentos.***

20 *Será sancionada con pena de reclusión por término fijo de ocho (8) años toda persona*
21 *que, sin autoridad o causa legítima, produzca, use, posea, trafique o distribuya programas*

1 *informáticos, equipos, materiales o dispositivos cuyo uso exclusivo o fundamental sea emplearse*
2 *como herramienta para la comisión de crímenes y delitos de alta tecnología.*

3 ***Artículo 316. – Suplantación de Páginas Electrónicas.***

4 *Será sancionada con pena de reclusión por un término fijo de tres (3) años toda persona*
5 *que, sin estar facultada para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o*
6 *suplante páginas electrónicas, enlaces o ventanas emergentes.*

7 ***Artículo 317. – Suplantación de Páginas Electrónicas Agravado.***

8 *Será sancionada con pena de reclusión por un término fijo de ocho (8) años toda persona*
9 *que, para beneficio personal o de un tercero, cometa el delito de suplantación de páginas*
10 *electrónicas descrito en el Artículo 316, cuando la conducta modifique el sistema de resolución*
11 *de nombres de dominio de manera que redirija al usuario hacia una dirección de protocolo de*
12 *internet (IP) diferente, bajo la creencia de que acceda a su banco o a otro sitio de carácter*
13 *personal o de confianza.*

14 ***Artículo 318. – Facilitación del Delito.***

15 *Será sancionada con pena de reclusión por un término fijo de cinco (5) años toda persona*
16 *que facilite los medios para la perpetración de un delito ejecutado mediante un sistema o red*
17 *informática o telemática, o contenedores electrónicos, ópticos o magnéticos.*

18 ***Artículo 319. – Facilitación del Delito Agravado.***

19 *Será sancionada con pena de reclusión por un término fijo de ocho (8) años toda persona*
20 *que cometa el delito de facilitación del delito descrito en el Artículo 318, cuando la información*
21 *obtenida se utilice para beneficio propio o de terceros.*

22 ***Artículo 320. – Utilización Ilícita de Redes de Comunicaciones.***

1 *Toda persona que, con fines ilícitos, haga uso de aparatos de radiofonía o televisión, o de*
2 *cualquier medio electrónico diseñado o adaptado para interferir, emitir o reproducir señales, sin*
3 *autorización, será sancionada con pena de reclusión por un término fijo de tres (3) años.*

4 ***Artículo 321. – Manipulación de Equipos o Terminales Móviles.***

5 *Será sancionada con pena de reclusión por un término fijo de cuatro (4) años toda*
6 *persona que, manipule, re programe, remarque o modifique terminales móviles de los servicios*
7 *de comunicaciones en cualquiera de sus componentes, con el propósito de alterar las bases de*
8 *datos positivas y negativas que se establecerán para tal efecto y que serán administradas por la*
9 *entidad regulatoria correspondiente.*

10 ***Artículo 322. – Manipulación de Equipos o Terminales Móviles Agravado.***

11 *Será sancionada con pena de reclusión por un término fijo de ocho (8) años toda persona*
12 *que, cometa el delito de manipulación de equipos o terminales móviles descrito en el Artículo*
13 *321, cuando las conductas resulten ser parte de una red, grupo u organización de carácter*
14 *delincuencial o criminal.*

15 ***Artículo 323. – Manipulación de Equipos de Localización y Vigilancia.***

16 *Toda persona que, retire, modifique o inutilice, sin la debida autorización, dispositivos*
17 *de localización y vigilancia, será sancionada con pena de reclusión por un término fijo de cinco*
18 *(5) años.*

19 ***Artículo 324. – Manipulación de Equipos de Localización y Vigilancia***
20 ***Agravado.***

21 *Será sancionada con pena de reclusión por un término fijo de diez (10) años toda persona*
22 *que, cometa el delito de manipulación de equipos de localización y vigilancia descrito en el*

1 *Artículo 323, cuando se cometiere por un funcionario público. Además, se impondrá*
2 *destitución inmediata del cargo público e inhabilitación por término de cuatro (4) a diez (10)*
3 *años para desempeñarse en cualquier empleo, puesto o cargo público, contados a partir del*
4 *cumplimiento de la pena de reclusión.*

5 ***Artículo 325. – Intercambio, Comercialización o Compra de Información de***
6 ***Equipos o Terminales Móviles.***

7 *Toda persona que, intercambie, comercialice o adquiera bases de datos que contengan*
8 *información de identificación de equipos terminales móviles, será sancionada con pena de*
9 *reclusión por un término fijo de tres (3) años.*

10 ***CAPITULO II. – DELITOS INFORMÁTICOS COMO MEDIO***

11 ***SECCIÓN PRIMERA – Delitos Sexuales***

12 ***Artículo 326. – Corrupción.***

13 *Será sancionada con pena de reclusión por un término fijo de cinco (5) años toda persona*
14 *que, mediante tecnologías de la información y la comunicación, procure la excitación sexual*
15 *propia o de un tercero realizando ante una persona menor de edad acciones de significación*
16 *sexual, o exponiéndola a material pornográfico o exhibiciones de similar naturaleza.*

17 ***Artículo 327. – Corrupción Agravado.***

18 *Será sancionada con pena de reclusión por un término fijo de diez (10) años toda persona*
19 *que, cometa el delito de corrupción descrito en el Artículo 326, cuando con el propósito de*
20 *procurar su excitación sexual o la de otro, obligue, induzca, persuada, sugiera, incite, o*
21 *convenza a una persona menor de edad a realizar acciones de significación sexual delante suyo*

1 o de terceros; o a enviar, entregar o exhibir imágenes o grabaciones de su persona a otra persona
2 menor de edad, aunque haya expresado su consentimiento.

3 Será sancionada con pena de reclusión por un término fijo de quince (15) años, quien
4 procure, promueva, obligue, publicite, gestione, facilite o induzca, por cualquier medio, a una
5 persona menor de dieciocho (18) años de edad, o que carezca de capacidad de comprender el
6 significado del hecho o de capacidad de resistir la conducta, a realizar actos sexuales o de
7 exhibicionismo corporal, con fines sexuales, reales o simulados, con el objeto de producir
8 material mediante video grabación, audio grabación, fotografía, filmación, exhibición o
9 descripción a través de anuncios impresos, sistemas de cómputo, electrónicos o análogos, y se
10 beneficie económicamente de la explotación de la persona.

11 Cuando en la perpetración de la conducta descrita en el párrafo anterior se haya
12 utilizado fuerza, engaño, violencia física o psicológica, coerción, abuso de poder o de situación
13 de vulnerabilidad, dependencia de sustancias, posición jerárquica o de confianza, concesión o
14 recepción de pagos o beneficios para obtener el consentimiento, o cuando exista relación de
15 autoridad de una persona sobre otra, o cualquier otra circunstancia que disminuya o elimine la
16 capacidad volitiva de la víctima para resistirse, la pena prevista en el párrafo anterior se
17 aumentará en una mitad.

18 **Artículo 328. – Explotación Sexual, Pornografía y Acto Sexual con Menores de**
19 **Edad.**

20 Toda persona que, con ánimo de lucro, beneficio personal o para un tercero, induzca
21 facilite, promueva o utilice, con fines sexuales o eróticos a una persona menor de edad o con
22 discapacidad haciéndola presenciar o participar en un comportamiento sexual, espectáculo

1 público o privado, aunque la víctima consienta presenciar tal comportamiento o participar en
2 él, por medio de las tecnologías de la información y la comunicación, será sancionada con pena
3 de reclusión por un término fijo de diez (10) años.

4 **Artículo 329. - Fabricación, Producción, Difusión o Reproducción de**
5 **Pornografía.**

6 Toda persona que participare en la producción, financiación, fabricación, reproducción,
7 publicación, comercialización, importe, exporte, difusión, o en la distribución de material
8 pornográfico, por cualquier medio, sea directo, mecánico, digital, audio, visual o con soporte
9 informático, electrónico u otros conexos, en cuya elaboración hubieren sido utilizados menores
10 de edad, será sancionada con pena de reclusión por un término fijo de diez (10) años. Se
11 entenderá por material pornográfico en cuya elaboración hubieren sido utilizados menores de
12 edad, toda representación de éstos dedicados a actividades eróticas o sexuales explícitas o
13 implícitas, reales o simuladas, o toda representación de sus partes genitales con fines sexuales,
14 o toda representación de dichos menores en que se emplee su voz o imagen, con los mismos
15 fines.

16 **Artículo 330. - Pornografía Relativa a Menores de Edad.**

17 Toda persona que fotografíe, filme, grabe, produzca, divulgue, ofrezca, venda, compre,
18 posea, porte, almacene, trasmita o exhiba, por cualquier medio, para uso personal o intercambio,
19 representaciones reales de actividad sexual que involucre una persona menor de edad, será
20 sancionada con pena de reclusión por un término fijo de diez (10) años.

1 Artículo 331. – Pornografía Relativa a Menores de Edad Agravado.

2 *Será sancionada con pena de reclusión por un término fijo de quince (15) años toda*
3 *persona que, cometa el delito de pornografía relativa a menores de edad descrito en el Artículo*
4 *330, quien alimente con pornografía infantil bases de datos de Internet, con o sin fines de lucro.*

5 *La pena se aumentará de una tercera parte a la mitad cuando el responsable sea*
6 *integrante de la familia de la víctima, dentro del cuarto grado de consanguinidad o segundo de*
7 *afinidad.*

8 Artículo 332. – Pornografía Virtual y Pseudo Pornografía.

9 *Toda persona que posea, produzca, venda, distribuya, exhiba o facilite, por cualquier*
10 *medio, material pornográfico en el que no habiendo utilizado personas menores de edad, emplee*
11 *a una persona adulta que simule ser una persona menor de edad realizando actividades*
12 *sexuales; o emplee imagen, caricatura, dibujo o representación, de cualquier clase, que aparente*
13 *o simule a una persona menor de edad realizando actividades sexuales, será sancionada con*
14 *pena de reclusión por un término fijo de quince (15) años.*

15 Artículo 333. – Tenencia, Adquisición o Posesión de Material Pornográfico de
16 Menores de Edad o Personas con Impedimentos.

17 *Toda persona que adquiera para sí o para un tercero a través de cualquier medio que*
18 *involucre el uso de las tecnologías de la información y la comunicación, o posea material*
19 *pornográfico en el que se haya utilizado a un menor de edad o persona con discapacidad o su*
20 *imagen para su producción, será sancionada con pena de reclusión por un término fijo de diez*
21 *(10) años.*

1 **Artículo 334. – Difusión de Pornográfica.**

2 *Será sancionada con pena de reclusión por un término fijo de diez (10) años toda persona*
3 *que, mediante el uso de tecnologías de la información y la comunicación o por cualquier otro*
4 *medio, entregue, comercialice, difunda, distribuya o exhiba material pornográfico en el que se*
5 *represente a personas menores de edad o incapaces, o que adquiriera para sí o para un tercero, o*
6 *posea material pornográfico en cuya producción se haya utilizado a una persona menor de edad*
7 *o con discapacidad, o su imagen.*

8 *Será sancionada con pena de reclusión por un término fijo de tres (3) años el que*
9 *maliciosamente adquiriera o almacene material pornográfico, cualquiera sea su soporte, en cuya*
10 *elaboración hayan sido utilizados menores de edad,*

11 **Artículo 335. – Utilización o Facilitación de Medios de Comunicación para**
12 **Actividades Sexuales con Menores de Edad o Personas con Impedimentos.**

13 *Toda persona que, de cualquier modo, facilitare, en beneficio propio o ajeno, la*
14 *comercialización, difusión, exhibición, importación, exportación, distribución, oferta,*
15 *almacenamiento o adquisición de material pornográfico que contenga la imagen o cualquier*
16 *otra forma de representación de una o más personas menores de edad o incapaces, será*
17 *sancionada con pena de reclusión por un término fijo de cinco (5) años.*

18 **Artículo 336. – Comercialización de Pornografía con Menores de Edad o**
19 **Personas con Discapacidad.**

20 *Toda persona que, publique, compre, posea, porte, transmita, descargue, almacene,*
21 *importe, exporte o venda, por cualquier medio, para uso personal o para intercambio*

1 *pornografía de menores de edad, será sancionada con pena de reclusión por un término fijo de*
2 *diez (10) años.*

3 ***Artículo 337. – Exhibición Pornográfica.***

4 *Toda persona que, ofrezca o publique espectáculos teatrales o cinematográficos obscenos,*
5 *transmita audiciones o efectúe publicaciones de idéntico carácter, será sancionado con pena de*
6 *reclusión por un término fijo de diez (10) años.*

7 ***Artículo 338. – Turismo Sexual.***

8 *Será sancionada con pena de reclusión por un término fijo de quince (15) años toda*
9 *persona que, por cualquier medio, promueva, publique, invite, facilite o gestione que una o más*
10 *personas viajen dentro o fuera del territorio y jurisdicción de Puerto Rico con el propósito de*
11 *que realicen actos sexuales, reales o simulados, con una o varias personas menores de edad, o*
12 *con una o varias personas que carezcan de capacidad para comprender el significado del hecho*
13 *o resistir la conducta.*

14 ***Artículo 339. – Destrucción de Material.***

15 *Cuando medie condena mediante sentencia firme por cualquier delito comprendido en*
16 *esta Sección, el tribunal ordenará la destrucción de todo material o anuncio obsceno o de*
17 *pornografía infantil que haya motivado la condena del acusado y que se encuentre en poder o*
18 *bajo control del tribunal, del ministerio público o de un funcionario del orden público.*

19 ***SECCIÓN SEGUNDA – Delitos Contra La Intimidad***

20 ***Artículo 340. – Acceso Indebido a Datos.***

21 *Será sancionada con pena de reclusión por un término fijo de tres (3) años toda persona*
22 *que, sin autorización y violando sistemas de seguridad, obtenga para sí o para terceros acceso a*

1 *datos no destinados a ella y que se encuentren especialmente protegidos contra el acceso no*
2 *autorizado.*

3 ***Artículo 341. – Acceso Indebido a Datos del Sistema Público y del Gobierno de***
4 ***Puerto Rico.***

5 *Será sancionada con pena de reclusión por un término fijo de cinco (5) años toda persona*
6 *que, cometa el delito de acceso indebido a datos descrito en el Artículo 340, cuando se cometiere*
7 *por un funcionario público. Además, se impondrá destitución inmediata del cargo público e*
8 *inhabilitación por término de cuatro (4) a diez (10) años para desempeñarse en cualquier*
9 *empleo, puesto o cargo público, contados a partir del cumplimiento de la pena de reclusión.*

10 ***Artículo 342. – Uso de Equipos para Invasión de Privacidad.***

11 *Será sancionada con pena de reclusión por un término fijo de dos (2) años toda persona*
12 *que, sin causa legítima o autorización de la entidad legalmente competente, use sistemas*
13 *electrónicos, informáticos, telemáticos, de telecomunicaciones, o dispositivos susceptibles de*
14 *realizar operaciones que atenten contra la privacidad en cualquiera de sus manifestaciones.*

15 ***Artículo 343. – Acceso Indebido a Correspondencia o Comunicaciones del***
16 ***Sistema Público y del Gobierno de Puerto Rico.***

17 *Será sancionada con pena de reclusión por un término fijo de cinco (5) años, toda*
18 *persona que:*

19 *a) opere o abuse de los servicios o instalaciones de telecomunicaciones de libre*
20 *recepción o de radiodifusión sin autorización de la autoridad correspondiente, y el*
21 *que permita que, en su domicilio, residencia, morada o medio de transporte, operen*
22 *tales servicios o instalaciones;*

- 1 b) maliciosamente interfiera, intercepte o interrumpa un servicio de
2 telecomunicaciones, y la confiscación de los equipos e instalaciones;
- 3 c) intercepte o capte maliciosamente o grave sin la debida autorización, cualquier tipo
4 de señal que se emita a través de un servicio público de telecomunicaciones; o
- 5 d) divulgue de manera pública o privada, cualquier comunicación obtenida por
6 infracción de las disposiciones de este Artículo.

7 **Artículo 344. – Acceso Indebido a Correspondencia o Comunicaciones del**
8 **Sistema Público y del Gobierno de Puerto Rico Agravado.**

9 *Será sancionada con pena de reclusión por un término fijo de diez (10) años toda persona*
10 *que cometa el delito de acceso indebido a correspondencia o comunicaciones del sistema público*
11 *y del gobierno de Puerto Rico descrito en el Artículo 343, cuando tal conducta sea cometida por*
12 *un funcionario público, o persona encargada de la recolección, entrega o salvaguarda de los*
13 *documentos o comunicaciones, o persona encargada de administrar o prestar soporte técnico al*
14 *sistema o red informática o telemática, o que por razón de sus funciones tenga acceso a tal*
15 *sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.*

16 *Además, si la condena recae sobre un funcionario público, se impondrá destitución*
17 *inmediata del cargo público e inhabilitación por término de cuatro (4) a diez (10) años para*
18 *desempeñarse en cualquier empleo, puesto o cargo público, contados a partir del cumplimiento*
19 *de la pena de reclusión.*

20 **Artículo 345. – Acceso Indebido o Ilícito de Información Médica.**

21 *Toda persona que, sin autorización, violando o no los sistemas de seguridad, obtuviere*
22 *para sí o para terceros, el acceso a datos médicos de otra persona, no destinados a él y*

1 *especialmente protegidos contra el acceso no autorizado, será sancionada con pena de reclusión*
2 *por un término fijo de cinco (5) años.*

3 *Será sancionada con pena de reclusión por un término fijo de siete (7) años toda persona*
4 *que, cometa el delito de acceso indebido o ilícitos de información médica, cuando se cometiere*
5 *por un funcionario público. Además, se impondrá destitución inmediata del cargo público e*
6 *inhabilitación por término de cuatro (4) a diez (10) años para desempeñarse en cualquier*
7 *empleo, puesto o cargo público, contados a partir del cumplimiento de la pena de reclusión.*

8 ***Artículo 346. – Acceso Indebido O Ilícito De Información Médica Agravado.***

9 *Será sancionada con pena de reclusión por un término fijo de diez (10) años toda persona*
10 *que, cometa el delito de acceso indebido o ilícito de información médica descrito en el Artículo*
11 *345, cuando utilice o difunda el contenido de comunicaciones o documentos privados carentes*
12 *de interés público, causando peligro o daño a la intimidad de otra persona.*

13 ***Artículo 347. – Interceptación de Datos Informáticos.***

14 *Será sancionada con pena de reclusión por un término fijo de tres (3) años toda persona*
15 *que, sin orden judicial previa, intercepte datos informáticos en su origen, destino o en el interior*
16 *de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema*
17 *informático que los transporte, cuando:*

18 *a) en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en*
19 *cualquier forma, un dato informático en su origen, destino o en el interior de un*
20 *sistema informático, una señal o una transmisión de datos o señales, con la finalidad*
21 *de obtener información registrada o disponible;*

- 1 b) *diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de*
2 *seguridad o páginas electrónicas, enlaces o ventanas emergentes, o modifique el*
3 *sistema de resolución de nombres de dominio de un servicio financiero o pago*
4 *electrónico, u otro sitio personal o de confianza, de manera que induzca a una*
5 *persona a ingresar a una dirección o sitio de internet diferente al que pretende*
6 *acceder:*
- 7 c) *a través de cualquier medio, copie, clone o comercialice información contenida en las*
8 *bandas magnéticas, chips u otro dispositivo electrónico que constituya de tarjetas de*
9 *crédito, débito, pago o similares; o*
- 10 d) *produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos*
11 *o sistemas informáticos destinados a la comisión del delito descrito en el inciso*
12 *anterior.*

13 ***Artículo 348. – Obtención y Transferencia de Información Confidencial.***

14 *Será sancionada con pena de reclusión por un término fijo de cinco (5) años toda persona*
15 *que, deliberadamente, obtenga y transfiera información de carácter confidencial y que, mediante*
16 *el uso de tal información vulnere un sistema o datos informáticos, utilizando para ello cualquier*
17 *modalidad de tecnologías de la información y la comunicación, incluidas las emisiones*
18 *electromagnéticas.*

19 ***Artículo 349. – Obtención y Transferencia de Información Confidencial del***
20 ***Sistema Público o del Gobierno de Puerto Rico.***

21 *Será sancionada con pena de reclusión por un término fijo de siete (7) años toda persona*
22 *que, cometa el delito de acceso indebido a correspondencia o comunicaciones del sistema público*

1 y del gobierno de Puerto Rico descrito en el Artículo 348, cuando la conducta sea cometida por
2 un funcionario público. Además, se impondrá destitución inmediata del cargo público e
3 inhabilitación por término de cuatro (4) a diez (10) años para desempeñarse en cualquier
4 empleo, puesto o cargo público, contados a partir del cumplimiento de la pena de reclusión.

5 **Artículo 350. – Apertura o Interceptación Ilegal de Comunicaciones.**

6 Será sancionada con pena de reclusión por un término fijo de un (1) año toda persona
7 que ilegítimamente abra, intercepte, o por cualquier otro medio tome conocimiento del
8 contenido de un documento, pliego cerrado o despacho telegráfico, telemático, electrónico o de
9 otra naturaleza que no le esté dirigido.

10 **Artículo 351. – Violación a la Intimidad.**

11 Será sancionada con pena de reclusión por un término fijo de tres (3) años toda persona
12 que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine,
13 retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio
14 y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones
15 privadas o reservadas de otra persona, por cualquier medio.

16 **Artículo 352. – Revelación Indebida de Datos e Información.**

17 Será sancionada con pena de reclusión por un término fijo de diez (10) años toda persona
18 que, cometa el delito de extorsión informática “ransomware” descrito en el Artículo 363,
19 cuando la conducta se haya realizado con ánimo de lucro, o en orden a la comisión de otro delito,
20 o cuando se difunda material sexual explícito en perjuicio de un tercero.

Artículo 353. – Preparación de Acceso Indevido o Interceptación de Datos.

Será sancionada con pena de reclusión por un término fijo de tres (3) años toda persona que prepare un hecho punible conforme a los Artículos 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351 y 352, produciendo, difundiendo o haciendo accesible de otra manera a terceros:

- a) las claves de acceso u otros códigos de seguridad, que permitan el acceso a datos; o
- b) los programas de computación destinados a la realización de tal hecho.

SECCIÓN TERCERA – Delitos Contra la Identidad

Artículo 354. – Hurto, Supresión, Alteración de Identidad o de Estado Civil.

Será sancionada con pena de reclusión por un término fijo de cinco (5) años toda persona que, ilegalmente impida, altere, añada o suprima la inscripción de los datos de identidad propios, o inscriba como suya o de otra persona datos de identidad en programas informáticos, partidas, tarjetas de identificación “Real ID”, licencia de conducir, o en cualquier otro documento emitido por el Gobierno de Puerto Rico.

Será sancionada con pena de reclusión por un término fijo de siete (7) años toda persona que ilegalmente altere la identidad de un menor de edad; la sustituya por otra; entregue o consigne datos falsos o supuestos relativos a un nacimiento; usurpe la filiación legítima de un menor de edad, o declare falsamente el fallecimiento de un recién nacido,

SECCIÓN CUARTA – Delitos Contra la Persona

Artículo 355. – Revelación y Transmisión Ilegal de Base de Datos.

Será sancionada con pena de reclusión por un término fijo de tres (3) años toda persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros,

1 *archivos, bases de datos o medios análogos, a través de o dirigidas a un sistema electrónico,*
2 *informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente*
3 *la violación del secreto, la intimidad y la privacidad de las personas,*

4 ***Artículo 356. – Revelación y Transmisión Ilegal de Base de Datos Agravado.***

5 *Será sancionada con pena de reclusión por un término fijo de cinco (5) años toda persona*
6 *que, cometa el delito de revelación y transmisión ilegal de base de datos descrito en el Artículo*
7 *358, cuando se cometiere por un funcionario público, empleadas o empleados bancarios internos*
8 *o de instituciones de la economía popular y solidaria que realicen intermediación financiera o*
9 *contratistas. Además, se impondrá destitución inmediata del cargo público e inhabilitación por*
10 *término de cuatro (4) a diez (10) años para desempeñarse en cualquier empleo, puesto o cargo*
11 *público, contados a partir del cumplimiento de la pena de reclusión.*

12 ***Artículo 357. – Publicidad o Comercio de Personas, Órganos, Servicios o Bienes***
13 ***Ilícitos.***

14 *Será sancionada con pena de reclusión por un término fijo de quince (15) años toda*
15 *persona que, por cualquier medio que involucre el uso de las tecnologías de la información y la*
16 *comunicación, promueva, favorezca, facilite o publique la oferta, la obtención o el tráfico ilegal*
17 *de órganos y tejidos humanos o el trasplante de los mismos, o se beneficie económicamente de*
18 *la explotación de una persona mediante el comercio, distribución, exposición, circularización u*
19 *oferta de libros, revistas, escritos, grabaciones, filmes, fotografías, anuncios impresos, imágenes*
20 *u objetos, de carácter lascivo o sexual, reales, o simulados, sea de manera física, o a través de*
21 *cualquier medio.*

1 **Artículo 358. – Propalación o Venganza Pornográfica.**

2 *Será sancionada con pena de reclusión por un término fijo de tres (3) años toda persona*
3 *quien, hallándose legítimamente en posesión de una comunicación, documentos o grabación de*
4 *carácter privado, los haga públicos, difunda, revele o ceda a un tercero, sin la debida*
5 *autorización de la víctima, aunque le hayan sido dirigidos.*

6 *Además, será sancionada con pena de reclusión por un término fijo de cinco (5) años*
7 *cuando se trate de documentos divulgados por internet, o grabaciones, imágenes,*
8 *comunicaciones o documentos hechos públicos de contenido explícito de carácter íntimo, sexual*
9 *o erótico, aunque hayan sido obtenidos con el consentimiento.*

10 **Artículo 359. – Acecho, Hostigamiento, Intimidación o “Cyber-Bulling”.**

11 *Será sancionada con pena de reclusión por un término fijo de tres (3) años toda persona*
12 *que, mediante el uso de cualquier comunicación electrónica oral, escrita, visual o textual, o*
13 *utilizando dispositivo tecnológico para determinar o monitorear la localización o movimiento*
14 *de una persona, realice conducta destinada a acosar, molestar, intimidar o afligir a otra persona*
15 *o a un grupo de personas, ocasionando daño a la integridad física, mental o emocional o*
16 *patrimonial de la víctima.*

17 **Artículo 360. – Intimidación o Amenazas.**

18 *Será sancionada con pena de reclusión por un término fijo de un (1) año toda persona*
19 *que, mediante expresiones verbales, escritos, mensajes electrónicos o cualquier otro medio*
20 *intimide o amenace a una persona con la que se halle o hubiere estado ligado por relación de*
21 *consanguinidad, afinidad, sujeción a tutela, vínculo conyugal, convivencia en unión de hecho*

1 estable, noviazgo, o relación de afectividad; con amenaza de causarle daño grave y probable de
2 naturaleza física, psicológica, sexual, laboral o patrimonial.

3 **Artículo 361. – Calumnia o Injuria.**

4 Será sancionada con pena de reclusión por un término fijo de dos (2) años toda persona
5 que, impute falsamente a otra la comisión o participación en un delito concreto. Si la calumnia
6 se propagara con publicidad, será sancionada con pena de reclusión por un término fijo de tres
7 (3) años.

8 **Artículo 362 – Difamación.**

9 Será sancionada con pena de reclusión por un término fijo de cinco (5) años toda persona
10 que difame a través de medios electrónicos, informáticos, telemáticos, de telecomunicaciones o
11 audiovisuales.

12 **Artículo 363. – Extorsión Informática “Ransomware”.**

13 Será sancionada con pena de reclusión por un término fijo de cinco (5) años toda persona
14 que, para procurar un lucro, obligue a otra con intimidación o amenazas graves, a tomar una
15 disposición patrimonial perjudicial para sí misma o para un tercero.

16 La pena de reclusión será por un término fijo de ocho (8) años cuando la conducta se
17 ejecute valiéndose de cualquier manipulación informática, telemática, electrónica o tecnológica.

18 **SECCIÓN QUINTA – Delitos Económicos y Colectivos**

19 **Artículo 364. – Clonación o Uso Fraudulento de Tarjetas de Crédito o Débito.**

20 Constituyen delito de uso fraudulento de tarjeta de crédito o débito las siguientes
21 conductas:

22 a) falsificar tarjetas de crédito o débito;

- 1 *b) usar, vender, exportar, importar o distribuir tarjetas de crédito o débito falsificadas*
2 *o sustraídas;*
- 3 *c) negociar, en cualquier forma, con tarjetas de crédito o débito falsificadas o*
4 *sustraídas;*
- 5 *d) usar, vender, exportar, importar o distribuir los datos o el número de una tarjeta de*
6 *crédito o débito, posibilitando que terceros realicen operaciones de compra o de*
7 *acceso al crédito o al débito que corresponden exclusivamente al titular;*
- 8 *e) negociar, en cualquier forma, con datos o números de tarjeta de crédito o débito, para*
9 *las operaciones descritas en el inciso anterior; o*
- 10 *f) usar maliciosamente una tarjeta bloqueada, en cualquiera de las modalidades*
11 *señaladas en los incisos precedentes.*

12 *Toda persona que cometa cualquiera de tales conductas será sancionada con pena de*
13 *reclusión por un término fijo de ocho (8) años.*

14 ***Artículo 365. – Estafa Informática.***

15 *Será sancionada con pena de reclusión por un término fijo de tres (3) años toda persona*
16 *que, en perjuicio de una persona natural o jurídica, manipule o influya en el ingreso,*
17 *procesamiento o resultado de datos en un sistema automatizado de información, ya sea mediante*
18 *el uso de datos falsos o incompletos, uso indebido de datos, programación, valiéndose de alguna*
19 *operación informática o artificio tecnológico, o cualquier otra acción que incida en el*
20 *procesamiento de los datos del sistema o que produzca información falsa, incompleta o*
21 *fraudulenta, con el propósito de procurar u obtener beneficio patrimonial o indebido para sí o*
22 *para un tercero.*

1 *La pena será de cinco (5) años de reclusión cuando las conductas sean perpetradas*
2 *contra sistemas de información públicos, sistemas de información bancarios y de entidades*
3 *financieras, o cuando el autor sea empleado encargado de administrar o brindar soporte técnico*
4 *al sistema o red informática o telemática, o que debido a sus funciones tenga acceso a dicho*
5 *sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.*

6 *Será sancionada con pena de reclusión por un término fijo de siete (7) años la persona*
7 *que, para obtener beneficio patrimonial para sí misma o para un tercero, mediante simulación*
8 *de hechos falsos o deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con*
9 *el fin de que realice un acto que perjudique su patrimonio o el de un tercero.*

10 *Será sancionada con pena de reclusión por un término fijo de diez (10) años toda persona*
11 *que, defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o*
12 *dupliquen los dispositivos originales de cajero automático para capturar, almacenar, copias o*
13 *reproducir información de tarjetas de crédito, débito, pago o similares.*

14 ***Artículo 366. – Transferencia Electrónica de Activo Patrimonial.***

15 *Será sancionada con pena de reclusión por un término fijo de cinco (5) años toda persona*
16 *que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema*
17 *informático, telemático o mensaje de datos, para procurarse la transferencia o apropiación no*
18 *consentida de activo patrimonial de otra persona, en perjuicio de esta o de un tercero. Con igual*
19 *pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la*
20 *intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de*
21 *transferencia electrónica producto de este delito para sí misma o para un tercero.*

Artículo 367. – Apropiación Fraudulenta por Medios Electrónicos.

Será sancionada con pena de reclusión por un término fijo de tres (3) años toda persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de bien ajeno, o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona, alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones,.

Además, será sancionada con pena de reclusión por un término fijo de cinco (5) años, cuando el delito se cometa utilizando sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, tarjetas magnéticas o perforadas, controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras análogas.

Artículo 368. – Difusión de Información Falsa.

Será sancionada con pena de reclusión por un término fijo de seis (6) años toda persona que, a través de medios electrónicos, informáticos, o mediante un sistema de telecomunicaciones, propague o difunda noticias o hechos falsos capaces de distorsionar o causar perjuicio a la seguridad y estabilidad del sistema financiero o de sus usuarios.

Artículo 369. – Pánico Económico o Financiero.

Será sancionada con pena de reclusión por un término fijo de siete (7) años toda persona que publique, difunda o divulgue noticias falsas susceptibles de causar daño a la economía nacional, con el propósito de alterar los precios de bienes o servicios para beneficiar a un sector, mercado o producto específico.

1 *Será sancionada con pena de reclusión por un término fijo de diez (10) años quien*
2 *divulgue noticias falsas capaz de causar alarma en la población y provoque el retiro masivo de*
3 *depósitos de cualquier institución del sistema financiero y de las entidades de la economía*
4 *popular y solidaria que realicen intermediación financiera, cuando tales actos pongan en peligro*
5 *la estabilidad patrimonial o provoquen el cierre definitivo de la institución afectada.*

6 **Artículo 370. – Registros Prohibidos.**

7 *Será sancionada con pena de reclusión por un término fijo de tres (3) años toda persona*
8 *que, sin autorización, promueva, facilite, autorice, financie, cree o comercialice un banco de*
9 *datos o registro informático que contenga datos susceptibles de afectar a personas naturales o*
10 *jurídicas.*

11 **Artículo 371. – Divulgación de Información Financiera Reservada.**

12 *Será sancionada con pena de reclusión por un término fijo de cinco (5) años toda persona*
13 *que, en beneficio propio o de terceros, divulgue información financiera clasificada como*
14 *reservada por la autoridad competente en materia de finanzas públicas, cuando tal divulgación*
15 *genere condiciones económicas desfavorables para el Estado.*

16 **Artículo 372. – Transferencia de Activos.**

17 *Será sancionada con pena de reclusión por un término fijo de cinco (5) años toda persona*
18 *que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante,*
19 *consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero.*

20 *La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa*
21 *de computador destinado a la comisión del delito descrito en el párrafo anterior, o de una estafa.*

Artículo 373. – Sabotaje al Sistema Financiero.

Será sancionada con pena de reclusión por un término fijo de tres (3) años toda persona que, sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de instituciones integrantes del sistema financiero, siempre que tales sistemas se encuentren protegidos por algún mecanismo de seguridad.

Será sancionada con pena de reclusión por un término fijo de cinco (5) años quien, sin autorización legal, acceda, conozca o copie información contenida en sistemas o equipos de informática de las instituciones integrantes del sistema financiero, siempre que tales sistemas se encuentren protegidos por algún mecanismo de seguridad.

Artículo 374. – Delitos Contra la Autoridad.

Será sancionada con pena de reclusión por un término fijo de ocho (8) años toda persona natural o el representante de la persona jurídica que, siendo requerido por el Ministerio Público o por autoridad competente, se rehusare con dolo a colaborar o aportar información para la localización geográfica en tiempo real de los dispositivos de comunicación, conforme a las disposiciones de las leyes federales o estatales aplicables, cuando tales dispositivos estén relacionados con investigaciones en materia de delincuencia organizada, delitos contra la salud, secuestro, extorsión, amenazas u otros delitos de igual gravedad.

La misma sanción se aplicarán a la persona natural, o al representante de la persona jurídica que, de forma dolosa, obstaculice, retrase sin justa causa o se rehusé a colaborar en la intervención de comunicaciones privadas, o a proporcionar información a la cual estén obligados, conforme a la legislación aplicable.

SECCIÓN SEXTA– *Delitos Contra la Prueba Documental*

Artículo 375. – Destrucción o Daño a Documentos o Señales.

Será sancionada con pena de reclusión por un término fijo de cinco (5) años toda persona que, con la intención de perjudicar a otro:

- a) destruyera, dañara, ocultara o de otra forma suprimiera un documento o una certificación técnica, en contravención del derecho de otro a utilizarlo como prueba;*
- b) borrara, suprimiera, inutilizara o alterara, en contravención del derecho de disposición de otro, información o dato de relevancia probatoria; o*
- c) destruyera o de otra forma suprimiera señales destinadas a indicar un límite o la altura de las aguas.*

Artículo 376. – Falsificación de Medios Electrónicos de Pago.

Será sancionada con pena de reclusión por un término fijo de cinco (5) años toda persona que, persiguiendo la intención de inducir error en las relaciones jurídicas o de facilitar tal inducción:

- a) falsificare o alterar una tarjeta de crédito o débito u otro medio electrónico de pago;*
- o*
- b) adquiriera para sí o para un tercero, ofreciere, entregare a otro o utilizare tales tarjetas o medios electrónicos.*

Cuando el autor actuare comercialmente o como miembro de una organización criminal dedicada a la realización de los hechos punibles, será sancionada con pena de reclusión por un término fijo de siete (7) años.”

1 Sección 2.- Se reenumera el Título VI como Título VII, y los actuales Artículos 301,
2 302, 303, 304, 305, 306, 307, 308 y 309 como los Artículos 377, 378, 379, 380, 381, 382,
3 383, 384 y 385 de la Ley 146-2012, según enmendada, conocida como “Código Penal
4 de Puerto Rico”.

5 Sección 3.- Aplicabilidad.

6 Esta Ley será aplicable a toda conducta perpetrada con posterioridad a su entrada
7 en vigor. La conducta perpetrada con anterioridad a la entrada en vigor de esta Ley
8 continuará rigiéndose por las disposiciones legales vigentes al momento de su
9 comisión.

10 Sección 4.- Clausula de Separabilidad.

11 Si cualquier artículo, inciso, parte, párrafo o cláusula de este Código o su aplicación
12 a cualquier persona o circunstancia, es declarada inconstitucional por un tribunal, la
13 sentencia dictada no afectará ni invalidará las demás disposiciones, sino que su efecto
14 quedará limitado y será extensivo al artículo, inciso, parte, párrafo o cláusula, o su
15 aplicación, que haya sido declarada inconstitucional.

16 Sección 5. - Delitos no Incorporados.

17 La incorporación en el Código Penal, por virtud de esta Ley, de ciertos delitos o
18 disposiciones contemplados en leyes especiales, no constituirá causa de derogación de
19 tales leyes especiales, ni tampoco de aquellos delitos tipificados en leyes especiales
20 cuya incorporación al Código Penal no se hubiere efectuado mediante esta Ley.

1 Sección 6.- Vigencia.

2 Esta Ley comenzará a regir a partir de los ciento ochenta (180) días de su
3 aprobación.