RASGOS DEL MINIMALISMO EN EL SISTEMA PENAL PANAMEÑO

Features of minimalism in panamenian criminal law

Alberto H. González Herrera.Universidad de Panamá.
Centro Regional Universitario de San Miguelito
alberto.gonzalezh@up.ac.pa
https: //orcid.org/0000-001-5141-8528,

alberto.gonzalezh@up.ac.pa

Resumen

El presente trabajo analiza el artículo 289 del Código penal panameño que tipifica el acceso indebido a los datos, redes y sistemas informáticos, se utilizan los métodos dogmático jurídico y comparativo, así como tomamos en cuenta parte de la doctrina y algunos tipos similares en modelos del Derecho comparado.

Palabras clave: base de datos, red, sistema informático, uso indebido, delito, sanción.

Abstract

This paper analyzes Article 289 of the Panamanian Criminal Code, which criminalizes unauthorized access to data, networks, and computer systems. Employing both legal-dogmatic and comparative methodologies, this study incorporates contemporary legal doctrine and examines similar statutory frameworks within comparative law models.

Keywords: database, computer network, computer system, hacking, crime, sanction

Sumario: 1. Introducción 2. Aspectos generales 3. El delito de ingreso o uso indebido de base de datos, red o sistema informático 4. Las conscuencias juridicas. 5. .Algunos modelos del Derecho comparado 6. Conclusiones.

1. Introducción

El siglo XXI se ha destacado por la digitalización y automatización de la sociedad que no opera ni funciona sin el empleo de tecnología. A la fecha, el aprovechamiento de las bases de datos, redes y sistemas informáticos nos ha convertido en usuarios permanentes de los trámites en línea. Desde adquirir los boletos para una obra de teatro, comprar pasajes de avión, encargar productos diversos, pagar cuentas de servicios públicos y privados hasta reservar una cita médica.

Sin rubor alguno facilitamos datos personales, números de tarjetas de crédito y transferimos sumas de dinero.

Por esa preponderancia que tiene en el mundo la dinámica de los sistemas informáticos, las bases de datos y las redes, se torna necesaria la tutela penal garantizando el uso correcto y no abusivo de éstos, a fin de no afectar la economía, la intimidad personal y la seguridad informática.

2. Aspectos generales

A efectos de no confundirnos en torno a los conceptos básicos que requiere el ingreso o uso indebido de base de datos, red o sistema informático como conducta delictiva tomamos en cuenta algunos conceptos que nuestro ordenamiento jurídico contempla.

Señala la Ley 75 (2015) en el artículo 10.3 que la base de datos es un sitio donde se almacena, accede y mantiene un conjunto organizado de datos electrónicos, que pertenecen al mismo contexto, guardados sistemáticamente para su posterior uso. De semejante forma, la Ley 81 (2019) sobre protección de datos personales en el artículo 4.2 indica que la base de datos es el "conjunto ordenado de datos de cualquier naturaleza, cualquiera que sea la forma o modalidad de su creación, organización o almacenamiento, que permite relacionar los datos entre sí, así como realizar cualquier tipo de tratamiento o transmisión de estos por parte de su custodio".

En torno a la red no tenemos concepto legal por lo que resulta útil el que se encuentra en el Diccionario de la Real Academia (2014) ligado a la informática: conjunto de computadoras o de equipos informáticos conectados entre sí y que pueden intercambiar información (p. 1871).

La Convención de Budapest (2001) define en el artículo 1 al sistema informático como: todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de algunos de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

Asimismo, la Ley 75 (2015) define el sistema automatizado de gestión judicial como: la aplicación informática mediante la cual se realizan las actuaciones y gestiones total o parcialmente electrónicas utilizando preferentemente Internet.

2.1. Concepto de delito informático

Agelán (2011) destaca que los delitos informáticos se cometen a través de internet, son de naturaleza compleja como resultado de su itinerancia y de su capacidad de mutación debido a que la tecnología no permanece estática (p. 12).

Se trata de un delito informático o ciberdelito aquel en el cual se emplean equipos informáticos como instrumento a fin de cometer algún delito contra la economía, la libertad personal, la intimidad, la libertad e integridad sexual, el patrimonio, la seguridad de los medios informáticos, entre otros.

Refiere Beermann (2024) que en los ciberdelitos constituye el bien jurídico la confianza de las personas en el uso de los equipos electrónicos (p. 80).

El delito de ingreso o uso indebido de base de datos, red o sistema informático es un tipo de delito que hace imperativo entender que se realiza vulnerando los sistemas de seguridad de una o varias unidades de una red computacional, mediante el empleo de un ordenador o de una computadora personal, con el fin de utilizarla como medio de ejecución de una delito convencional u obtener de la base de datos de dicha red, la información que sobre un tema, una actividad o varios sujetos reposa en el mismo (González, 2010, p. 83). A la fecha podríamos indicar que cualquier dispositivo como una tableta, teléfono celular o artefacto electrónico semejante podría servir al propósito de lograr el acceso a la base de datos, la red o el sistema informático seleccionado.

3. El delito de ingreso o uso indebido de base de datos, red o sistema informático

El artículo 289 del Código penal describe el tipo básico que tutela las bases de datos, red y los sistemas informáticos al señalar lo siguiente: Quien indebidamente ingrese o utilice una base de datos, red o sistema informático será sancionado con dos a cuatro años de prisión.

El bien jurídico protegido que tutela este tipo penal se concreta al mantenimiento de la seguridad de las bases de datos, redes o sistemas informáticos no se distingue entre las públicas o las privadas por lo que abarca a cualquiera de estas. Tiende este tipo de conducta de la misma forma a la salvaguarda de la intimidad personal, los datos personales; la correcta operatividad del sistema o la base de datos e información contenida en estos. La conducta se puede poner de manifiesto de dos maneras, ingresando indebidamente a la base, red o el sistema informático o con la utilización indebida de la base de datos, la red o el sistema informático.

Asimismo, comenta Beermann (2024) que el acceso deliberado e ilegítimo a un sistema informático exige que se genere el quebrantamiento de una medida o dispositivo de seguridad del equipo electrónico, o la intención de obtener datos informáticos (p. 82).

La acción requiere el ingreso o la utilización de una base de datos que almacena o contiene información de manejo por personal determinado, sobre materias o asuntos de pluralidad de sujetos.

Es delito de mera actividad pues basta la realización de la conducta. Es una conducta autónoma, de formulación casuística, monoofensivo y anormal (Guerra/Villalaz/González, 2017, p. 228).

El tipo objetivo lo marcan los verbos rectores, el ingresar o utilizar a una base de datos, red o sistema informático.

El delito de ingreso o uso indebido de base de datos, red o sistema informático procura salvaguardar en primer lugar, la correcta operatividad de los medios electrónicos, que la base de datos, la red o el sistema informático público o privado no sea vulnerado por los denominados piratas informáticos, hackers o adictos a la informática que disfrutan pasar el rato, con la obtención de ganancias fáciles, engañando, simulando negocios o afectando la prestación de un servicio.

Aun cuando el sujeto activo es indeterminado o simple, podría ser cualquier persona, no obstante, la misma debe tener conocimiento o manejo de equipos informáticos. Podría ser uno el ejecutor de este delito o cometerlo en compañía de otra u otras personas tornándolo en delito plurisubjetivo. Al examinar al sujeto pasivo tenemos que es monosubjetivo, simple e indeterminado si solo se tiende a perjudicar a una persona, empresa o entidad no exige calidad determinada.

La Convención de las Naciones contra la Ciberdelincuencia (2024) en el artículo prevé el acceso ilícito a los sistemas informáticos de la siguiente manera:

Acceso ilícito.

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno el acceso deliberado y sin derecho a la totalidad o una parte de un sistema de tecnología de la información y las comunicaciones.
2. Los Estados partes podrán exigir como requisito que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos electrónicos o con otra intención deshonesta o delictiva o en relación con un sistema de tecnología de la información y las comunicaciones que esté conectado a otro sistema de tecnología de la información y las comunicaciones".

Esta propuesta de la Convención se asemeja a la que dispone el artículo de la 2 del Convenio de Budapest (2001).

4. Las consecuencia jurídicas

El legislador solamente fijó pena única de prisión que va dos a cuatro años. La que de resultar impuesta sea en el tramo mínimo, medio o máximo admite la aplicación de algún subrogado o pena sustitutiva como el de arresto de fines de semana, días-multa o trabajo comunitario conforme lo autoriza el artículo 102 del Código penal. Como pena accesoria se debería peticionar por el Fiscal que lleve la causa la inhabilitación para que el sancionado pueda desenvolverse en la profesión u oficio de ingeniero, técnico u operador informático o de sistemas informáticos con base en el artículo 74 del Código penal, no obstante, a los expertos en informática esto no les limita, dada la facilidad con que se pueden obtener o adquirir los dispositivos con acceso internet o plataforma digitales a fin de continuar en sus entretenidas actividades.

No encontramos precedente judicial que evidencie la aplicación de este injusto penal pero estaremos pendientes a ver si en algún momento se sanciona a alguien por ingreso o uso indebido de base de datos, redes o sistemas informáticos.

5. Algunos modelos del Derecho comparado

En el Derecho comparado, hemos dado un vistazo a algunos Códigos penales y leyes que contemplan la figura similar al delito de ingreso o uso indebido de base de datos, red o sistema informático que prevé nuestra legislación.

Tomamos en cuenta el artículo 269-A del Código penal colombiano, el artículo 234 del Código Orgánico Integral Penal de Ecuador, los artículos 4 y 5 del Decreto N°260 de 2016 de El Salvador, el artículo 197 bis del Código penal español, el artículo 274-F del Código penal de Guatemala, el artículo 616 ter del Código penal italiano, los artículos 4 y 5 de la Ley 1042 de 27 de octubre de 2020 de Nicaragua.

Tipifica el artículo 269-A del Código penal colombiano el acceso no autorizado a datos o sistemas informáticos de la siguiente manera: "El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático 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 excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes".

Respecto esta figura destaca Pabón (2013) que es un tipo de mera conducta, de peligro, de conducta instantánea, de conducta permanente y pluriofensivo (pp. 560-561).

Suárez (2019) afirma que el tipo contempla dos conductas alternativas, el acceso al sistema informático y el mantenimiento dentro del sistema informático; esta última conducta se puede manifestar si el sujeto está autorizado a ingresar al sistema manteniéndose dentro él contra la voluntad de quien tiene derecho a excluirlo, y, por otro lado, el sujeto ingresa sin estar autorizado al sistema, lo hizo por caso fortuito o imprudencia, y se mantiene allí (p. 27).

Asimismo, subraya Suárez (2019) que el delito de acceso abusivo a un sistema informático el bien jurídico no es únicamente de característica supraindividual, dado que no solo busca tutelar el interés social que se tiene en la seguridad de la información y los datos, que consiste en la integridad, confidencialidad y disponibilidad de estos, sino también de índole individual, porque protege la libertad y otras garantías (p. 24).

El artículo 234 del Código Orgánico Integral Penal de Ecuador señala: "Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años".

El tipo penal ecuatoriano se presenta con una técnica de tipificación casuística, dirige la conducta al objeto material comprendido por el sistema informático, sistema telemático o sistema de telecomunicaciones, el cual debe ser accedido total o parcialmente contra la voluntad de su titular legítimo. La acción debe dirigirse una vez se logra acceder, a modificar un portal web, desviar o redireccionar el tráfico de datos o de voz u ofrecer los servicios que estos sistemas proveen a terceros, sin pagarlos a los legítimos proveedores. En alguna medida a diferencia del tipo en Panamá, este exige el acceso parcial o total a alguno de los sistemas, o se mantenga sin autorización para explotarlo, modificar el portal web, desviar o redireccionar el tráfico de datos o de voz u ofrecer los servicios a terceros.

Espinosa/Paredes (2025) destacan que el delito de acceso no autorizado a sistemas informáticos, telemáticos o de telecomunicaciones presenta un sujeto activo simple o indeterminado, que la normativa requiere mayor precisión respecto a la medición del daño causado y la posible imposición de sanciones pecuniarias o reparaciones civiles que compensen la vulneración de datos y perjuicios causados (p. 563).

Mientras que los artículos 4 y 5 del Decreto 260 de El Salvador indican:

“Acceso Indebido a Sistemas Informáticos.

Art. 4- El que intencionalmente y sin autorización o excediendo la que se le hubiere concedido, acceda, intercepte o utilice total o parcialmente un sistema informático que utilice las Tecnologías de la Información o la Comunicación, será sancionado con prisión de uno a cuatro años.

Acceso Indebido a los Programas o Datos Informáticos.

Art. 5- El que a sabiendas y con la intención de usar cualquier dispositivo de la Tecnología de la Información o la Comunicación, accediera parcial o totalmente a cualquier programa o a los datos almacenados en él, con el propósito de apropiarse de ellos o cometer otro delito con éstos, será sancionado con prisión de dos a cuatro años.”

Estas disposiciones penales presentan similitud al tipo penal panameño en virtud que salvaguardan el sistema informático, los datos contenidos y sus programas. Las acciones deben ser ejecutadas con dolo directo de manera parcial o total y conllevan como sanción pena de prisión.

Por otra parte, España tipifica la conducta de intrusión informática en el artículo 197 bis del Código penal que señala:

1. El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

2. El que, mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los

mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.

Esta disposición fue adicionada al Código penal español mediante la Ley Orgánica 1/2015, de caras a brindar una mejor tutela a los sistemas informáticos.

Comenta Colás (2017,p.217) que la figura de intrusismo informático es un delito de peligro que tutela la intimidad y la seguridad de los sistemas informáticos..

En tanto, López (2021,p.139) apunta que el delito de intrusismo informático genera la discusión si se tutelan la intimidad o el patrimonio y quienes abogan por la tutela de los sistemas de información

Por su parte, el artículo 274-F del Código penal de Guatemala señala: "Se impondrá prisión de seis meses a dos años, y multa de doscientos a mil quetzales al que, sin autorización, utilizare los registros informáticos de otro, o ingresare, por cualquier medio, a su banco de datos o archivos electrónicos".

De manera sencilla el legislador guatemalteco diseña la conducta de utilización o ingreso no autorizado a registros informáticos, banco de datos o archivos electrónicos, tutela la información contenida en estos, el sujeto activo es simple o indeterminado y la consecuencias jurídicas conllevan sanciones conjuntas de prisión y de multa.

El Código penal de Italia lo prevé en el artículo 615 ter que señala:

"Accesso abusivo ad un sistema informatico o telematico :Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesamente armato;
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.
Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.
Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio".

Fusco (2020) expresa que en Italia el tipo de acceso no autorizado a sistema informático o telemático tutela la libertad individual, el "domicilio informático" -el lugar en el que la persona desarrolla sus facultades intelectuales y expresa su forma de ser, con la consiguiente facultad de excluir a terceros (p. 133).

El reato presenta un tipo básico que permite sancionar con hasta tres años de prisión a quien sin contar con autorización ingresa a un sistema informático o telemático, obviando las medidas de seguridad contra la voluntad expresa o manifiesta de quien tenga derecho a excluirlo.

Se agrava la sanción si la acción la ejecutan un funcionario público o la persona encargada de un servicio público, abusando del cargo o con violación del deber inherente a la función o al servicio; si se realiza por un detective privado o abusando de la calidad de servidor público.

También, si el sujeto comete el hecho empleando violencia sobre el sistema o la persona, o valiéndose de arma.

A la vez, si de la realización del hecho se genera la destrucción o el daño del sistema informático, la interrupción total o parcial de su operatividad, de los datos, de la información, o de los programas que operen en el sistema.

En caso de realizar la conducta de los numerales primero y segundo en sistema informático o sistema telemático de interés militar o relativo al orden público, la seguridad pública, la salud, la protección civil o el interés público.

A la vez, disponen los artículos 4 y 5 de la Ley 1042 de Nicaragua lo siguiente:

"Artículo 4 Acceso indebido a sistemas informáticos:

El que intencionalmente y sin autorización o excediendo la que se le hubiere concedido, acceda, intercepte o haga uso parcial o totalmente de un sistema informático que utilice las Tecnologías de la Información y la Comunicación, será sancionado con prisión de uno a tres años y doscientos a quinientos días.multa.

Artículo 5. Acceso indebido a los programas o datos informáticos

El que a sabiendas y con la intención de usar cualquier dispositivo de la Tecnología de la Información y la Comunicación, accediera directa o indirectamente, parcial o totalmente a cualquier programa o a los datos almacenados en él, con el propósito de apropiarse de ellos o cometer otro delito con éstos, será sancionado con prisión de dos a cuatro años y trescientos a quinientosdíasmulta.

Las penas para las conductas descritas en los Artículos 4 y 5, se incrementarán en un tercio en su límite inferior y superior, cuando se cometan con fines comerciales o en contra de:

1.Oficinas públicas o bajo su tutela.

2. Instituciones públicas, privadas o mixtas que prestan un servicio público.

3. Bancos, instituciones de microfinanzas, almacenes generales de depósitos, grupos financieros, compañías de seguros y demás instituciones financieras y bursátiles supervisadas y/o reguladas en Nicaragua".

Los tipos del acceso informático nicaraguense se dirigen a evitar que se afecten los sistemas, programas y datos de las Tecnologías de la Información y la Comunicación en dicha nación.

Se presentan como tipos penales con sujeto activo simple o indeterminado, ambos requieren que parcial o totalmente se acceda, intercepte o haga uso de un sistema informático que utiliza las tecnologías de la información y la comunicación, los que constituyen el bien jurídico tutelado y prevén sanciones privativas de libertad.

Se prevé sanción agravada de incremento de la pena de prisión, si el sujeto activo comete estos injustos penales con fines comerciales o en contra de oficinas públicas o bajo su tutela, instituciones públicas, privadas o mixtas que prestan servicio público, bancos, instituciones de microfinanzas, almacenes generales de depósitos, grupos financieros, compañías de seguros y demás instituciones financieras y bursátiles supervisadas y /o reguladas.

6.Conclusiones

La tutela de las bases de datos, redes y sistemas informáticos se hace necesaria a efecto de evitar la afectación la información que manejan y las actividades que se efectúan día a día con la tecnología.

La conducta conlleva la salvaguarda de la intimidad, la libertad, el patrimonio, la seguridad de los sistemas informáticos y su correcta explotación.

En los modelos observados del Derecho comparado también se estima necesaria la tutela de los sistemas informáticos de los accesos indebidos.

Bibliografía

Agelán Casasnovas, E. E. (2011). *Ciberdelincuencia y Política* criminal. *Internet: nuevo reto jurídico-penal*. Editora Premium.

Beermann Hemmerling, K. (2024). La ciberdelincuencia en Panamá y el Convenio de Budapest. *Boletín de Ciencias Penales, N°21,* pp. 77-97.

Código Orgánico Integral Penal Ecuador disponible en: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf (consultado el día 15 de junio de 2026).

Código penal español. (2025). Boletín Oficial del Estado.

Colás Turégano, A. (2016). El delito de intrusismo informático tras la reforma del CP español de 2015. *Revista boliviana de Derecho N°21,* pp. 210-229.

Convención de las Naciones Unidas contra la Ciberdelincuencia (2024).

Convenio sobre la Ciberdelincuencia (2001).

Decreto N°260 de 4 de febrero de 2016. Ley Especial contra los delitos informáticos y conexos. Diario Oficial N°40 (El Salvador).

Espinosa Carvajal, G. G./Paredes Fuentes, F. E. (2025). Los ciber delitos y la protección de datos personales en el sistema penal ecuatoriano. *Lex, Revista de Investigación en Ciencias Jurídicas*, pp. 559-572.

Fusco, L. E. (2020). Los delitos informáticos en el Código Penal Italiano. *Derecho Global, Estudios sobre Derecho y Justicia, vol. 5, número 14*, pp. 127-149.

González Herrera, A. (2010). La tipicidad de la revelación de secretos informáticos. *Holística jurídica N°8,* pp. 79-88.

Guerra de Villalaz, A./Villalaz de Allen, G./González Herrera, A. (2010). *Compendio de Derecho penal, parte especial*. Cultural Portobelo.

Ley 75 (2015), Que subroga la Ley 15 de 2008, Que adopta medidas para la informatización de los procesos judiciales, y dicta otras disposiciones. Gaceta N°27931-B (Panamá).

Ley 81 (2019), Sobre Protección de Datos personales. Gaceta N°28743-A (Panamá).

Ley 1042 (2020), Ley Especial de Ciberdelitos. Diario Oficial N°201 (Nicaragua).

López Gorostidi, J. (2021). Los valores tradicionales como bienes jurídicos protegidos también en el ciberespacio: a propósito del confinamiento provocado por la crisis sanitaria del COVID-19. *Revista penal n°47,* pp. 126-152.

Pabón Parra, P. (s/f). *Código penal de la república de Panamá*. Doctrina y Ley.

Pabón Parra, P. (2013). *Manual de Derecho penal, Tomo II, parte especial.* Doctrina y Ley.

Suárez Sánchez, A. (2019). Delitos informáticos. *Lecciones de Derecho penal, parte especial.* Universidad Externado de Colombia, pp. 13-72.

ALBERTO H. GONZÁLEZ HERRERA

Licenciatura en Derecho y Ciencias Políticas, Universidad de Panamá, 1995.Especialista en Ciencias Penales, Universidad de Costa Rica, 1997. Maestría en Derecho con Especialización en Ciencias Penales, Universidad de Panamá, 2005. Certificado de Diploma de Estudios Avanzados de Tercero Ciclo (Doctorando), Universidad Pablo de Olavide, Sevilla, 2008. Profesor de Derecho Penal, CRUSAM.

Artículo recibido: 15 de junio de 2026 Aprobado: 20 de julio de 2026