

H. Congreso del Estado de Nuevo León



LXXVI Legislatura

PROMOVENTE: C. DIP. ALHINNA BERENICE VARGAS GARCÍA, INTEGRANTE DEL GRUPO LEGISLATIVO DEL PARTIDO REVOLUCIONARIO INSTITUCIONAL DE LA LXXVI LEGISLATURA

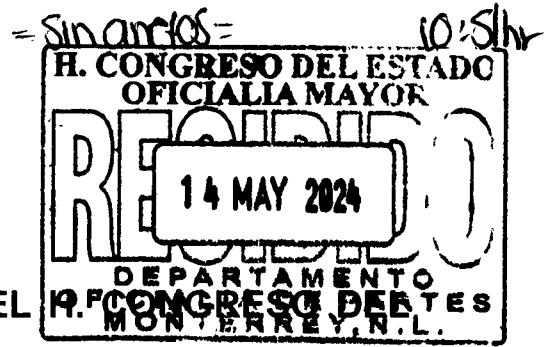
ASUNTO RELACIONADO: MEDIANTE EL CUAL PRESENTA INICIATIVA DE REFORMA A POR ADICIÓN DE UN CAPÍTULO SEGUNDO DEL TÍTULO SEXTO DENOMINADO CIBERDELITOS, DEL ARTÍCULO 225 BIS 1 Y AL TÍTULO DEL ARTÍCULO 207 BIS DEL CÓDIGO PENAL PARA EL ESTADO DE NUEVO LEÓN.

INICIADO EN SESIÓN: 5 DE JUNIO DEL 2024

SE TURNÓ A LA (S) COMISIÓN (ES): JUSTICIA Y SEGURIDAD PÚBLICA

Mtra. Armida Serrato Flores

Oficial Mayor



DIP. RICARDO CANAVATI HADJÓPULOS
PRESIDENTE DE LA MESA DIRECTIVA DEL
ESTADO DE NUEVO LEÓN

Presente.-

La suscrita, **Diputada Alhinna Berenice Vargas García**, integrante del Grupo Legislativo del Partido Revolucionario Institucional del Congreso del Estado de Nuevo León, con fundamento en los Artículos 87 y 88 de la Constitución Política del Estado de Nuevo León, y en los artículos 102, 103 y 104 del Reglamento para el Gobierno Interior del Congreso del Estado de Nuevo León, acudo a presentar ante el pleno de la LXXVI Legislatura una iniciativa con proyecto de decreto para reformar el Código Penal del Estado de Nuevo León, por adición de un capítulo segundo del título sexto, denominado ciberdelitos, de un párrafo al artículo 225 Bis 1, y por modificación del numeral del artículo 207 Bis del título séptimo, todos ellos del citado Código Penal, bajo la siguiente:

EXPOSICIÓN DE MOTIVOS

Desde noviembre del año 2001, los Estados miembros del Consejo de Europa reconocieron la necesidad de establecer mecanismos de cooperación entre ellos mismos y el sector privado para hacer frente a una de las actividades ilícitas más grandes que sufren en el mundo entero, la ciberdelincuencia.

Para ello, firmaron en la ciudad de Budapest el “*Convenio sobre la Ciberdelincuencia*” a fin de proteger los intereses legítimos en la utilización y el desarrollo de tecnologías de la información.

La ciberseguridad se ha convertido en un tema sumamente relevante porque cada vez se producen más ciberataques que generan grandes

1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025



problemas a empresas, organismos públicos y desde luego a los habitantes del estado.

Con el convenio de Budapest se pretende prevenir las acciones que pongan en riesgo la confidencialidad, integridad y disponibilidad de los sistemas, redes y datos informáticos; además de evitar el abuso de los mismos sistemas, redes y datos.

Especialmente se enfoca el convenio a prevenir los actos que ponen en peligro las implicaciones económicas de los ciberataques, que no son menores. Algunos estudios estiman que las pérdidas globales por virus maliciosos, ascendió a 350 mil millones de euros, durante el año 2016.

Desde entonces tanto la Organización de las Naciones Unidas, la Unión Europea y los países que integran el conocido grupo G8, han realizado diversas iniciativas destinadas a mejorar el entendimiento y la cooperación internacional en la lucha contra la delincuencia cibernética.

Por otra parte, en Estados Unidos se declaró estado de emergencia durante el mes de mayo del año 2021 tras un ciberataque a la mayor red de oleoductos del país.

Un grupo de hackers desconectó por completo y robó más de 100 giga bites de información del Oleoducto Colonial, que transportaba más de 2.5 millones de barriles de combustible.

Es importante señalar que nuestro país representa un gran mercado con un gran potencial de ganancias económicas para cibercriminales. Entre los ataques más recientes a establecimientos nacionales, están los realizados en el año 2020 contra la CONDUSEF, el SAT y el Banco de México.

El ataque de *ransomware* a la Lotería Nacional en junio de 2021, donde se encriptó información crítica, financiera, interna y de empleados, pidiendo un rescate de casi un millón de pesos a cambio de las claves para descifrar esta información y que no se publicara.

Más recientemente, un conocido grupo de hackers denominado Guacamaya realizó una intrusión ilegal a los archivos de la Secretaría de la Defensa Nacional y filtró a los medios 4.1 millones de correos electrónicos que incluyen reportes especiales de operativos, informaciones sobre el presupuesto y comunicaciones privadas entre distintas dependencias del gobierno, así como la salud del titular del Poder Ejecutivo de la Nación.

En el siguiente cuadro comparativo se muestra la propuesta de reforma al Código Penal del Estado para adicionar un capítulo dedicado a los ciberdelitos para establecer sanciones a los ciberdelincuentes.

**CÓDIGO PENAL DEL ESTADO DE NUEVO LEÓN
TÍTULO SEXTO**

Texto vigente	Texto propuesto
CAPÍTULO I REVELACIÓN DE SECRETOS ARTÍCULO 206.- ... ARTÍCULO 206 BIS.- ... ARTÍCULO 207.- ...	CAPÍTULO I REVELACIÓN DE SECRETOS ARTÍCULO 206.- ... ARTÍCULO 206 BIS.- ... ARTÍCULO 207.- ...
SIN CORRELATIVO	CAPÍTULO II CIBERDELITOS

	<p>ARTÍCULO 207 BIS. SE CONSIDERARÁ QUE SE COMETE UN CIBERDELITO CUANDO:</p> <p>I. A QUIEN REVELE, DIVULGUE O UTILICE INDEBIDAMENTE O EN PERJUICIO DE OTRO, INFORMACIÓN, CONVERSACIONES O MENSAJES DE TEXTO, IMÁGENES O ARCHIVOS DE VOZ, CONTENIDOS EN SISTEMAS O EQUIPOS INFORMÁTICOS, OBTENIDOS A TRAVÉS DE MECANISMOS DISTINTOS A LA INTERVENCIÓN DE COMUNICACIÓN PRIVADA, MEDIANTE EL EMPLEO DE APARATOS O DISPOSITIVOS ELECTRÓNICOS FIJOS O MÓVILES O A TRAVÉS DE LA SUPLANTACIÓN DE IDENTIDAD.</p> <p>II. A QUIEN SIN AUTORIZACIÓN ACCEDA, MODIFIQUE, DESTRUYA O PROVOQUE PÉRDIDA DE INFORMACIÓN CONTENIDA EN SISTEMAS O</p>
--	---

EQUIPOS DE INFORMÁTICA QUE NO ESTÉN O NO PROTEGIDOS POR ALGÚN MECANISMO DE SEGURIDAD, O TAMBIÉN SIN AUTORIZACIÓN ACCEDA A DICHOS SISTEMAS O EQUIPOS DE INFORMÁTICA O MEDIANTE CUALQUIER MECANISMO QUE DE MANERA DIRECTA O REMOTA LES CAUSE UN DAÑO.

III. A QUIEN, CON O SIN AUTORIZACIÓN CONOZCA, COPIE, MODIFIQUE, DESTRUYA O PROVOQUE PÉRDIDA DE INFORMACIÓN CONTENIDA EN SISTEMAS O EQUIPOS DE INFORMÁTICA QUE PERTENEZCAN AL ESTADO, PROTEGIDOS POR ALGÚN MECANISMO DE SEGURIDAD.

SIN PERJUICIO DE LA SANCIÓN CORRESPONDIENTES, SI EL RESPONSABLE ES O HUBIERA SIDO SERVIDOR PÚBLICO,

SERÁ ACREEDOR A LA INHABILITACIÓN.

IV. A QUIEN CON O SIN AUTORIZACIÓN CONOZCA, COPIE, MODIFIQUE, DESTRUYA O PROVOQUE PÉRDIDA DE INFORMACIÓN CONTENIDA EN SISTEMAS O EQUIPOS DE INFORMÁTICA DE LAS INSTITUCIONES QUE INTEGRAN EL SISTEMA FINANCIERO, PROTEGIDOS POR ALGÚN MECANISMO DE SEGURIDAD.

LA PENA PREVISTA EN ESTE ARTÍCULO SE INCREMENTARÁ EN UNA MITAD CUANDO LAS CONDUCTAS SEAN COMETIDAS POR FUNCIONARIOS O EMPLEADOS DE LAS INSTITUCIONES QUE INTEGRAN EL SISTEMA FINANCIERO.

LAS PENAS ESTABLECIDAS EN EL PRESENTE ARTÍCULO SE INCREMENTARÁN HASTA

EN DOS TERCERAS PARTES Y SE IMPONDRÁN SIN PERJUICIO DE LAS QUE RESULTEN APLICABLES POR LA COMISIÓN DE OTROS DELITOS AL QUE REALICE, PARA BENEFICIO PROPIO O DE CUALQUIER TERCERO, LAS CONDUCTAS QUE DESCRIBEN LOS PÁRRAFOS ANTERIORES, CON LA FINALIDAD DE REALIZAR O ENCUBRIR LAS OPERACIONES CON RECURSOS DE PROCEDENCIA ILÍCITA A QUE SE REFIERE EL ARTÍCULO 431 DE ESTE ORDENAMIENTO.

A QUIEN COMETA ALGUNO DE LOS DELITOS PREVISTOS EN LAS FRACCIONES I, Y II SE LES IMPONDRÁ UNA PENA DE 1 A 6 AÑOS DE PRISIÓN, Y DE CIENTO A SEISCIENTAS CUOTAS DE MULTA.

LAS CONDUCTAS PREVISTAS EN LAS FRACCIONES III Y IV TENDRÁN UNA PENA DE 2 A 8 AÑOS DE PRISIÓN Y DE

	<p>TRECIENTAS A NOVECIENTAS CUOTAS DE MULTA.</p> <p>PARA EFECTOS DEL PRESENTE ARTÍCULO, EN LOS CASOS EN QUE EL DAÑO PROVOCADO OBSTACULICE O DISMINUYA LA CAPACIDAD DE FUNCIONAMIENTO DEL SISTEMA O EQUIPO INFORMÁTICO, LAS PENAS PREVISTAS EN LOS PÁRRAFOS ANTERIORES SE INCREMENTARÁN HASTA EN DOS TERCERAS PARTES.</p>
<p>TÍTULO SÉPTIMO DELITOS POR HECHOS DE CORRUPCIÓN</p> <p>ARTÍCULO 207 BIS.- ...</p>	<p>TÍTULO SÉPTIMO DELITOS POR HECHOS DE CORRUPCIÓN</p> <p>ARTÍCULO 207 TER.- ...</p>
<p>TITULO OCTAVO DELITOS COMETIDOS EN LA ADMINISTRACIÓN Y PROCURACIÓN DE JUSTICIA</p> <p>ARTÍCULO 225 BIS 1.- A QUIEN INDEBIDAMENTE CONOZCA, OBTENGA, COPIE O UTILICE INFORMACIÓN CONTENIDA EN CUALQUIER SISTEMA</p>	<p>TITULO OCTAVO DELITOS COMETIDOS EN LA ADMINISTRACIÓN Y PROCURACIÓN DE JUSTICIA</p> <p>ARTÍCULO 225 BIS 1.- A QUIEN INDEBIDAMENTE CONOZCA, OBTENGA, COPIE O UTILICE INFORMACIÓN CONTENIDA EN</p>

INFORMÁTICO DE ALGUNA INSTITUCIÓN DE SEGURIDAD PÚBLICA O PROCURACIÓN DE JUSTICIA, PROTEGIDO POR ALGÚN MEDIO DE SEGURIDAD, SE LE IMPONDRÁ PENA DE CINCO A DIEZ AÑOS DE PRISIÓN Y MULTA DE QUINIENTAS A MIL CUOTAS.

CUALQUIER SISTEMA INFORMÁTICO DE ALGUNA INSTITUCIÓN DE SEGURIDAD PÚBLICA O PROCURACIÓN DE JUSTICIA, PROTEGIDO POR ALGÚN MEDIO DE SEGURIDAD, SE LE IMPONDRÁ PENA DE CINCO A DIEZ AÑOS DE PRISIÓN Y MULTA DE QUINIENTAS A MIL CUOTAS, ASÍ COMO LA DESTITUCIÓN DE SU CARGO.

LA SANCIÓN SEÑALADA EN EL PRESENTE ARTÍCULO SE DUPLICARÁ CUANDO SE OBSTRUYA, ENTORPEZCA, OBSTACULICE O IMPOSIBILITE LA PROCURACIÓN O IMPARTICIÓN DE JUSTICIA, O RECAIGA SOBRE LOS REGISTROS RELACIONADOS CON UN PROCEDIMIENTO PENAL RESGUARDADO POR LA AUTORIDAD COMPETENTE.

Con base a lo anteriormente expuesto, presento a esta Soberanía el siguiente proyecto de

DECRETO

Artículo único: Se reforma el Código Penal del Estado de Nuevo León, con la adición de un capítulo segundo del título sexto, denominado ciberdelitos, de un párrafo al artículo 225 Bis 1, y por modificación del numeral del artículo 207 Bis del título, todos ellos del citado Código Penal, para quedar de la siguiente manera:

CAPÍTULO I REVELACIÓN DE SECRETOS

ARTÍCULO 206.- ...

ARTÍCULO 206 BIS.- ...

ARTÍCULO 207.- ...

CAPÍTULO II CIBERDELITOS

ARTÍCULO 207 BIS. SE CONSIDERARÁ QUE SE COMETE UN CIBERDELITO CUANDO:

I. A QUIEN REVELE, DIVULGUE O UTILICE INDEBIDAMENTE O EN PERJUICIO DE OTRO, INFORMACIÓN, CONVERSACIONES O MENSAJES DE TEXTO, IMÁGENES O ARCHIVOS DE VOZ, CONTENIDOS EN SISTEMAS O EQUIPOS INFORMÁTICOS, OBTENIDOS A TRAVÉS DE MECANISMOS DISTINTOS A LA INTERVENCIÓN DE COMUNICACIÓN PRIVADA, MEDIANTE EL EMPLEO DE APARATOS O DISPOSITIVOS ELECTRÓNICOS FIJOS O MÓVILES O A TRAVÉS DE LA SUPLANTACIÓN DE IDENTIDAD.

II. A QUIEN SIN AUTORIZACIÓN ACCEDA, MODIFIQUE, DESTRUYA O PROVOQUE PÉRDIDA DE INFORMACIÓN CONTENIDA EN SISTEMAS O EQUIPOS DE INFORMÁTICA QUE NO ESTÉN O NO

PROTEGIDOS POR ALGÚN MECANISMO DE SEGURIDAD, O TAMBIÉN SIN AUTORIZACIÓN ACCEDA A DICHOS SISTEMAS O EQUIPOS DE INFORMÁTICA O MEDIANTE CUALQUIER MECANISMO QUE DE MANERA DIRECTA O REMOTA LES CAUSE UN DAÑO.

III. A QUIEN, CON O SIN AUTORIZACIÓN CONOZCA, COPIE, MODIFIQUE, DESTRUYA O PROVOQUE PÉRDIDA DE INFORMACIÓN CONTENIDA EN SISTEMAS O EQUIPOS DE INFORMÁTICA QUE PERTENEZCAN AL ESTADO, PROTEGIDOS POR ALGÚN MECANISMO DE SEGURIDAD.

SIN PERJUICIO DE LA SANCIÓN CORRESPONDIENTES, SI EL RESPONSABLE ES O HUBIERA SIDO SERVIDOR PÚBLICO, SERÁ ACREEDOR A LA INHABILITACIÓN.

IV. A QUIEN CON O SIN AUTORIZACIÓN CONOZCA, COPIE, MODIFIQUE, DESTRUYA O PROVOQUE PÉRDIDA DE INFORMACIÓN CONTENIDA EN SISTEMAS O EQUIPOS DE INFORMÁTICA DE LAS INSTITUCIONES QUE INTEGRAN EL SISTEMA FINANCIERO, PROTEGIDOS POR ALGÚN MECANISMO DE SEGURIDAD.

LA PENA PREVISTA EN ESTE ARTÍCULO SE INCREMENTARÁ EN UNA MITAD CUANDO LAS CONDUCTAS SEAN COMETIDAS POR FUNCIONARIOS O EMPLEADOS DE LAS INSTITUCIONES QUE INTEGRAN EL SISTEMA FINANCIERO.

LAS PENAS ESTABLECIDAS EN EL PRESENTE ARTÍCULO SE INCREMENTARÁN HASTA EN DOS TERCERAS PARTES Y SE IMPONDRÁN SIN PERJUICIO DE LAS QUE RESULTEN

APLICABLES POR LA COMISIÓN DE OTROS DELITOS AL QUE REALICE, PARA BENEFICIO PROPIO O DE CUALQUIER TERCERO, LAS CONDUCTAS QUE DESCRIBEN LOS PÁRRAFOS ANTERIORES, CON LA FINALIDAD DE REALIZAR O ENCUBRIR LAS OPERACIONES CON RECURSOS DE PROCEDENCIA ILÍCITA A QUE SE REFIERE EL ARTÍCULO 431 DE ESTE ORDENAMIENTO.

A QUIEN COMETA ALGUNO DE LOS DELITOS PREVISTOS EN LAS FRACCIONES I, Y II SE LES IMPONDRÁ UNA PENA DE 1 A 6 AÑOS DE PRISIÓN, Y DE CIEN A SEISCIENTAS CUOTAS DE MULTA.

LAS CONDUCTAS PREVISTAS EN LAS FRACCIONES III Y IV TENDRÁN UNA PENA DE 2 A 8 AÑOS DE PRISIÓN Y DE TRECIENTAS A NOVECIENTAS CUOTAS DE MULTA.

PARA EFECTOS DEL PRESENTE ARTÍCULO, EN LOS CASOS EN QUE EL DAÑO PROVOCADO OBSTACULICE O DISMINUYA LA CAPACIDAD DE FUNCIONAMIENTO DEL SISTEMA O EQUIPO INFORMÁTICO, LAS PENAS PREVISTAS EN LOS PÁRRAFOS ANTERIORES SE INCREMENTARÁN HASTA EN DOS TERCERAS PARTES.

**TÍTULO SÉPTIMO
DELITOS POR HECHOS DE CORRUPCIÓN**

ARTÍCULO 207 TER.- ...

**TÍTULO OCTAVO
DELITOS COMETIDOS EN LA ADMINISTRACIÓN Y PROCURACIÓN
DE JUSTICIA**

ARTÍCULO 225 BIS 1.- A QUIEN INDEBIDAMENTE CONOZCA, OBTENGA, COPIE O UTILICE INFORMACIÓN CONTENIDA EN CUALQUIER SISTEMA INFORMÁTICO DE ALGUNA INSTITUCIÓN DE SEGURIDAD PÚBLICA O PROCURACIÓN DE JUSTICIA, PROTEGIDO POR ALGÚN MEDIO DE SEGURIDAD, SE LE IMPONDRÁ PENA DE CINCO A DIEZ AÑOS DE PRISIÓN Y MULTA DE QUINIENTAS A MIL CUOTAS, ASÍ COMO LA DESTITUCIÓN DE SU CARGO.

LA SANCIÓN SEÑALADA EN EL PRESENTE ARTÍCULO SE DUPLICARÁ CUANDO SE OBSTRUYA, ENTORPEZCA, OBSTACULICE O IMPOSIBILITE LA PROCURACIÓN O IMPARTICIÓN DE JUSTICIA, O RECAIGA SOBRE LOS REGISTROS RELACIONADOS CON UN PROCEDIMIENTO PENAL RESGUARDADO POR LA AUTORIDAD COMPETENTE.

TRANSITORIO

Artículo único. El presente decreto entrará en vigor el día siguiente al de su publicación en el Periódico Oficial del Estado.

Monterrey, N. L. al mes de mayo del año 2024

Atentamente


DIPUTADA ALHINNA BERENICE VARGAS GARCÍA

