DIP. LAURA IVONNE PANTOJA ABASCAL
PRESIDENTA DE LA MESA DIRECTIVA DEL HONORABLE CONGRESO DEL ESTADO DE MICHOACÁN DE OCAMPO.
PRESENTE.

JUAN CARLOS BARRAGÁN VÉLEZ, Diputado integrante de la Septuagésima Quinta Legislatura del Congreso del Estado de Michoacán, así como integrante del grupo parlamentario del partido MORENA, y de conformidad con lo establecido en los artículos 36, fracción II; 37 y 44, fracción I y XXX de la Constitución Política del Estado Libre y Soberano de Michoacán de Ocampo; 8, fracción II; 234 y 235 de la Ley Orgánica y de Procedimientos del Congreso del Estado de Michoacán de Ocampo; sometemos a consideración de este Honorable Congreso la presente iniciativa con proyecto de Decreto por el que se ***reforman el artículo 29, fracciones VII y VIII; y se adiciona al artículo 29, la fracción IX, ambos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo***, en base a la siguiente:

EXPOSICIÓN DE MOTIVOS:

La delincuencia informática o ciberdelincuencia es todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir, o manipular, cualquier sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico, de conformidad con la Oficina de las Naciones Unidas Contra la Droga y el Delito, menciona que la

ciberdelincuencia es un problema a nivel mundial, dándonos claridad sobre el tamaño del problema.

El uso indebido de la tecnología permite que los delincuentes cibernéticos puedan llevar a las empresas a la ruina e incluso afectar la vida de las personas que son víctimas de este delito. Diferentes países y organizaciones de todo el mundo luchan para poner un alto a los delincuentes cibernéticos y contribuir a la seguridad de los sistemas, en las últimas décadas las redes de computadoras e internet han crecido de manera asombrosa, hoy en día, el número de usuarios que se comunican, hacen sus compras, pagan sus cuentas, realizan negocios y hasta consultan con sus médicos online supera los 200 millones, comparado con 26 millones en 1995, esto con base al "*Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente"*. De manera acertada a medida que se va ampliando la Internet, asimismo es más la probabilidad de que se le dé un uso indebido.

Los delincuentes cibernéticos navegan en el mundo virtual, incurriendo en delitos tales como el acceso sin autorización o piratería informática, el fraude, el sabotaje informático, el narcotráfico, la trata de niños con fines pornográficos y el acecho, entre algunos otros delitos relacionados con el internet. Los delincuentes de la informática son tan diversos como sus delitos; puede tratarse de estudiantes, terroristas o figuras del crimen organizado. De acuerdo al Manual de la Naciones Unidas de 1997 sobre la prevención y la fiscalización de los delitos relacionados con las computadoras, en materia de delitos financieros como el fraude o el robo de información, la mayor categoría la forman los empleados de empresas, que son responsables del 90% de estos delitos.

El panorama ha alcanzado un nuevo nivel de comercialización, debido a la expansión de los delitos cibernéticos como servicio, facilitados por mercados clandestinos, como

Génesis, en el que se puede comprar malware y donde también hay venta masiva de credenciales robadas.

Las principales características que revisten los delitos informáticos son:

a) Conductas criminógenas de cuello blanco.

b) Son acciones ocupacionales, en cuanto que muchas veces se realizan cuando el sujeto se halla trabajando.

c) Oportunidad, en cuanto a que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

d) Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que los realizan.

e) Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.

f) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.

g) Son muy sofisticados y relativamente frecuentes en el ámbito militar.

De acuerdo con la Comisión Económica para América Latina y el Caribe (CEPAL) de las Naciones Unidas, la ciberseguridad[1] se considerada como un eje de desarrollo de la

[1] **CIBERSEGURIDAD**: La seguridad informática, también conocida como ciberseguridad o seguridad de tecnología de la información, es el área relacionada con la informática y la telemática que se enfoca en la

Estrategia de Gobierno Digital en un 85% de los casos revisados en América Latina y el Caribe, la ciberseguridad se ha establecido como una prioridad y una condición sine qua non para la entrega de servicios digitales y la comunicación no presencial entre las personas y el Estado.

Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas, y leyes concebidas para minimizar los posibles riesgos a la infraestructura y/o a la propia información. La ciberseguridad comprende software (bases de datos, metadatos, archivos), hardware, redes de computadoras, y todo lo que la institución entienda y valore como un riesgo si la información confidencial involucrada pudiera llegar a manos de otras personas, por ejemplo, convirtiéndose así en información privilegiada.

Nuestro país ha sido una de las naciones que mayormente ha tenido una tendencia al alza en ciberataques, lo cual indica la necesidad de impulsar estrategias de ciberseguridad en las distintas órdenes de gobierno, así como crear estrategias y/o políticas empresariales para prevenir ser vulnerados desde el exterior.

De acuerdo con el estudio del Estado Global de la Ciberseguridad en México de 2023, realizado por la empresa privada de seguridad y automatización de TI con sede en Silicon Valley, California, *"Infoblox"*, nuestro país ocupa el primer puesto de Latinoamérica en recibir más ciberataques, de hecho, el sondeo encontró que el 70% de los encuestados confesó que sufrió uno o más ataques de phishing o ransomware en los últimos 12 meses.

protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente la información contenida en una computadora o circulante a través de las redes de computadoras.

Fuente: *https://biblioguias.cepal.org/gobierno-digital/ciberseguridad*

Estas vulneraciones implican la manipulación, exposición o bloqueo de datos confidenciales y/o la interrupción del tiempo de inactividad del sistema, e incluso se registró que el daño causó lesiones corporales o psicológicas y la pérdida de la vida, en 2022, la fuga de datos y el ransomware fueron los ataques más preocupantes para el 51% de las organizaciones mexicanas.

Mientras tanto, el 43% temió por los ataques directos a través de servicios en la nube, 35% a los ataques a través de conexiones de trabajadores remotos, 27% a amenazas persistentes avanzadas, 21% a ataques a través de IoT en red, 18% a amenazas internas, 10% a ataques a la cadena de suministro o de terceros y 3% a ataques patrocinados por un estado.

El Índice de Ciberseguridad Global publicado por primera vez en 2015 por la Unión Internacional de Telecomunicaciones de la Organización de las Naciones Unidas para medir el grado de compromiso de sus 193 Estados Miembros en lo que respecta a la ciberseguridad, con el fin de ayudarles a determinar los aspectos susceptibles de mejora e instar a los países a tomar medidas, asignando en el Índice Mundial de Ciberseguridad 2020 a México una puntuación de 81,68 de 100 posibles y con una clasificación de 52 de 193 países, y en caso de la Región de las Américas su clasificación regional fue de 4 de 35 países, tal y como se puede observar a continuación:

SIN TEXTO

Resultados del ICG: Puntuación global y clasificación

Nombre del país	Puntuación	Clasificación
Estados Unidos de América**	100	1
Reino Unido	99,54	2
Arabia Saudí	99,54	2
Estonia	99,48	3
Corea (Rep. de)	98,52	4
Singapur	98,52	4
España	98,52	4
Federación de Rusia	98,06	5
Emiratos Árabes Unidos	98,06	5
Malasia	98,06	5
Lituania	97,93	6
Japón	97,82	7
Canadá**	97,67	8
Francia	97,6	9
India	97,5	10
Turquía	97,49	11
Australia	97,47	12
Luxemburgo	97,41	13
Alemania	97,41	13
Portugal	97,32	14
Letonia	97,28	15
Países Bajos**	97,05	16
Noruega**	96,89	17
Mauricio	96,89	17
Brasil	96,6	18
Bélgica	96,25	19

Nombre del país	Puntuación	Clasificación
Italia	96,13	20
Omán	96,04	21
Finlandia	95,78	22
Egipto	95,48	23
Indonesia	94,88	24
Viet Nam	94,59	25
Suecia	94,55	26
Qatar	94,5	27
Grecia	93,98	28
Austria	93,89	29
Polonia	93,86	30
Kazajstán	93,15	31
Dinamarca	92,6	32
China	92,53	33
Croacia	92,53	33
Eslovaquia	92,36	34
Hungría	91,28	35
Israel**	90,93	36
Tanzanía	90,58	37
Macedonia del Norte	89,92	38
Serbia	89,8	39
Azerbaiyán	89,31	40
Chipre	88,82	41
Suiza**	86,97	42
Ghana	86,69	43
Tailandia	86,5	44
Túnez	86,23	45

(continuación)

Nombre del país	Puntuación	Clasificación
Irlanda	85,86	46
Nigeria	84,76	47
Nueva Zelandia**	84,04	48
Malta	83,65	49
Marruecos	82,41	50
Kenya	81,7	51
México	81,68	52
Bangladesh	81,27	53
Irán (República Islámica de)	81,07	54
Georgia	81,06	55
Benin	80,06	56
Rwanda	79,95	57
Islandia	79,81	58
Sudáfrica**	78,46	59
Bahrein	77,86	60
Filipinas	77	61
Rumania	76,29	62
Moldova	75,78	63
Uruguay	75,15	64
Kuwait	75,07	65
República Dominicana	75,05	66
Eslovenia	74,93	67
República Checa	74,37	68
Mónaco	72,57	69
Uzbekistán	71,11	70
Jordania	70,96	71
Uganda	69,98	72
Zambia	68,88	73
Chile	68,83	74
Côte d'Ivoire	67,82	75
Costa Rica	67,45	76
Bulgaria	67,38	77
Ucrania	65,93	78
Pakistán	64,88	79
Albania	64,32	80
Colombia	63,72	81
Cuba	58,76	82
Sri Lanka	58,65	83
Paraguay	57,09	84
Brunei Darussalam	56,07	85
Perú	55,67	86
Montenegro	53,23	87
Botswana	53,06	88
Bielorrusia	50,57	89
Armenia**	50,47	90
Argentina	50,12	91
Kirguistán	49,64	92
Camerún	45,63	93
Nepal (República de)	44,99	94
Chad	40,44	95
Burkina Faso**	39,98	96
Malawi	36,83	97
Zimbabwe	36,49	98
Myanmar	36,41	99
Senegal	35,85	100
Liechtenstein**	35,15	101
Sudán	35,03	102
Panamá	34,11	103
Argelia	33,95	104
Togo	33,19	105
Jamaica**	32,53	106
Gambia	32,12	107
Suriname	31,2	108
Líbano**	30,44	109
Bosnia y Herzegovina	29,44	110
Samoa	29,33	111
Fiji	29,08	112
Libia	28,78	113
Guyana	28,11	114
Etiopía	27,74	115
Venezuela	27,06	116
Andorra**	26,38	117
Papúa Nueva Guinea**	26,33	118
Ecuador	26,3	119

(continuación)

Nombre del país	Puntuación	Clasificación
Mongolia	26,2	120
Sierra Leona	25,31	121
Estado de Palestina	25,18	122
Mozambique	24,18	123
Madagascar**	23,33	124
Trinidad y Tabago	22,18	125
República Árabe Siria**	22,14	126
Nauru**	21,42	127
Tonga**	20,95	128
Iraq**	20,71	129
Guinea**	20,53	130
Lao P.D.R.	20,34	131
Camboya**	19,12	132
Mauritania	18,94	133
Bután	18,34	134
Eswatini	18,23	135
Cabo Verde	17,74	136
Somalia	17,25	137
Tayikistán**	17,1	138
Barbados	16,89	139
Bolivia (Estado Plurinacional de)	16,14	140
Santo Tomé y Príncipe	15,64	141
Antigua y Barbuda	15,62	142
Congo (Rep. del)**	14,72	143
Turkmenistán**	14,48	144
Kiribati	13,84	145
San Marino	13,83	146
Bahamas	13,37	147
El Salvador**	13,3	148
Seychelles**	13,23	149
Guatemala	13,13	150
Angola	12,99	151
Vanuatu	12,88	152
Saint Kitts y Nevis**	12,44	153
San Vicente y las Granadinas**	12,18	154
Namibia	11,47	155
Níger	11,38	156
Gabón	11,36	157
Santa Lucía**	10,96	158
Belice	10,29	159
Malí**	10,14	160
Guinea-Bissau	9,85	161
Liberia	9,72	162
Granada	9,41	163
Lesotho	9,08	164
Nicaragua**	9	165
Islas Salomón	7,08	166
Haití	6,4	167
Tuvalu**	5,78	168
Sudán del Sur**	5,75	169
Rep. Dem. del Congo	5,3	170
Afganistán	5,2	171
Islas Marshall**	4,9	172
Timor-Leste**	4,26	173
Dominica	4,2	174
Comoras**	3,72	175
República Centroafricana **	3,24	176
Maldivas**	2,95	177
Honduras**	2,2	178
Djibouti	1,73	179
Burundi	1,73	179
Eritrea**	1,73	179
Guinea Ecuatorial**	1,46	180
Rep. Pop. Dem. de Corea**	1,35	181
Micronesia*	0	182
Vaticano*	0	182
Yemen*	0	182

* No se han recopilado datos
** No ha respondido al cuestionario

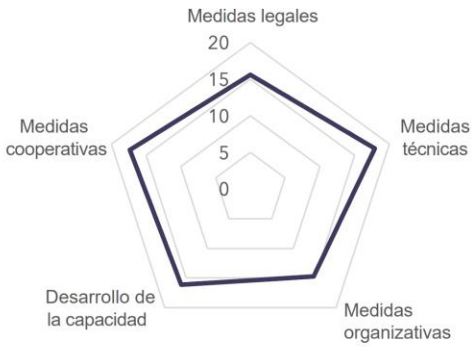
Resultados del ICG: Puntuación global y clasificación

Nombre del país	Puntuación global	Clasificación regional
Estados Unidos de América**	100	1
Canadá**	97,67	2
Brasil	96,6	3
México	81,68	4
Uruguay	75,15	5
República Dominicana	75,07	6
Chile	68,83	7
Costa Rica	67,45	8
Colombia	63,72	9
Cuba	58,76	10
Paraguay	57,09	11
Perú	55,67	12
Argentina	50,12	13
Panamá	34,11	14
Jamaica**	32,53	15
Suriname	31,2	16
Guyana	28,11	17

Nombre del país	Puntuación global	Clasificación regional
Venezuela	27,06	18
Ecuador	26,3	19
Trinidad y Tabago	22,18	20
Barbados	16,89	21
Bolivia (Estado Plurinacional de)	16,14	22
Antigua y Barbuda	15,62	23
Bahamas	13,37	24
El Salvador**	13,3	25
Guatemala	13,13	26
Saint Kitts y Nevis	12,44	27
San Vicente y las Granadinas**	12,18	28
Santa Lucía**	10,96	29
Belice	10,29	30
Granada	9,41	31
Nicaragua	9	32
Haití	6,4	33
Dominica	4,2	34
Honduras**	2,2	35

En el caso de México, su puntuación en el Índice Mundial de Ciberseguridad 2020 se compuso de la forma siguiente:

México



Nivel de desarrollo:
País en desarrollo

Área(s) de fortaleza relativa
Medidas cooperativas
Área(s) de posible crecimiento
Medidas organizativas

Puntuación global	Medidas legales	Medidas técnicas	Medidas organizativas	Desarrollo de la capacidad	Medidas cooperativas
81,68	15,61	17,90	14,70	16,13	17,34

Fuente: Índice de Ciberseguridad Global v4, UIT 2020

De ahí que Lenovo hubiera reportado en agosto de este año 2023 que México recibe el 23% de todos los ciberataques que se registran en América Latina. Esto lo posiciona como el segundo país de la región con mayor volumen de hacking, sólo detrás de Brasil.

En Latinoamérica, el 50% de los ciberataques tienen lugar en Brasil. Le siguen México, con el 23%; Colombia, con el 8%, y Perú, también con el 8%. El resto de los países del continente representan sólo el 11%.

Para dimensionar el número de ciberataques, Lenovo precisó que, en México, tan solo durante el primer semestre de 2022, se registraron 85,000 millones.

Por eso las numerosas dificultades que existen hoy en día menoscaban la confianza en línea e impiden que la sociedad digital alcance su pleno potencial. Por ejemplo, la empresa de seguridad informática McAfee estima que las pérdidas a escala mundial debido a la ciberdelincuencia oscilarán entre 1 billón de dólares en 2020.

Y por otro lado, la Revista Cybersecurity Ventures señaló en año 2020 que los costos globales de la ciberdelincuencia crecerían un 15 por ciento anual durante los siguientes cinco años, alcanzando los 10,5 billones de dólares anuales para 2025, frente a los 3 billones de dólares de 2015, representando esto la mayor transferencia de riqueza económica de la historia, poniendo en riesgo los incentivos para la innovación y la inversión, es exponencialmente mayor que el daño infligido por desastres naturales en un año y será más rentable que el comercio global de todas las principales drogas ilegales juntas.

A pesar de que no existen datos firmes a nivel global sobre los costos de la ciberdelincuencia, resulta importante que existe un problema a nivel global, que requiere que en todos los países se fortalezcan los marcos jurídicos y reglamentarios que definen lo que constituye actividades ilícitas en el ciberespacio y los instrumentos necesarios para

investigar, perseguir y hacer cumplir dicha legislación; el establecimiento de parámetros de referencia sobre ciberseguridad y mecanismos de observancia para un conjunto de actores nacionales; y procedimientos para garantizar la coherencia con las obligaciones internacionales.

Y es que la ciberseguridad evoluciona sin cesar, tanto en lo que respecta a las conductas como a las prácticas. Ya sea que se trate de una emergencia sanitaria mundial, del cambio climático, del envejecimiento de la población o de cualquier otro reto que nos depare el futuro, las tecnologías digitales constituyen una herramienta eficaz que contribuye al progreso del mundo. Cuando los Objetivos de Desarrollo Sostenible (ODS) de las Naciones Unidas lleguen a su vencimiento en 2030, se prevé que el 90% de la población mundial prevista, es decir, 7 500 millones de personas, estará en línea[2], con una cantidad estimada de entre 24 100[3] y 125 000[4] millones de dispositivos con Internet conectados. Para que no decaigan los esfuerzos dedicados a los ODS, la ciberseguridad será imprescindible, por cuanto permitirá garantizar que las soluciones digitales sean seguras, fiables y dignas de confianza.

La seguridad informática y de redes, o ciberseguridad, son cuestiones críticas. Pero no basta con proteger los sistemas que contienen datos sobre ciudadanos, corporaciones y agencias gubernamentales. La infraestructura de redes, enrutadores, servidores de nombres de dominio y conmutadores que unen estos sistemas no debe fallar, o las computadoras ya no podrán comunicarse de manera precisa o confiable. Dada la magnitud de la seguridad del ciberespacio, parece conveniente reflexionar sobre lo que estamos intentando hacer. Surgen varias preguntas, como qué es exactamente la

[2] *https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/*

[3] https://www.prnewswire.com/news-releases/global-iot-market-will-grow-to-24-1-billion-devices-in-2030--generating-1-5-trillion-annual-revenue-301061873.html

[4] https://cdn.ihs.com/www/pdf/IoT_ebook.pdf

infraestructura, contra qué amenazas se debe proteger y cómo se puede brindar protección de manera rentable. Pero detrás de todas estas preguntas está cómo definir un sistema seguro. ¿Qué es la seguridad? Obviamente tenerlo es bueno; todo el mundo lo dice. Pero pocas personas lo definen exactamente, o incluso de manera confusa.

Por las razones expuestas, en mi carácter de Diputado integrante de la Septuagésima Quinta Legislatura del Congreso del Estado de Michoacán, en ejercicio de las facultades que me confieren los artículos 36, fracción II; 37 y 44, fracción I y XXX de la Constitución Política del Estado Libre y Soberano de Michoacán de Ocampo, someto a consideración de ese Honorable Congreso, el siguiente proyecto de:

DECRETO:

ÚNICO. Se reforman el artículo 29, fracciones VII y VIII; y se adiciona al artículo 29, la fracción IX, ambos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Michoacán de Ocampo, para quedar como sigue:

Artículo 29…

I a la VI…

VII. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales***;***

VIII. Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales***; y,***

IX. Establecer un sistema de ciberseguridad o seguridad de tecnología de la información, que se enfoque en la protección de los datos personales en posesión de los sujetos obligados.

TRANSITORIOS

PRIMERO. El presente Decreto entrará en vigor el día siguiente al de su publicación en el Periódico Oficial del Gobierno Constitucional del Estado de Michoacán de Ocampo.

SEGUNDO. Los sujetos obligados deberán contemplar en el ejercicio fiscal subsecuente a la aprobación de este Decreto, el presupuesto relativo a establecer el sistema de ciberseguridad o seguridad de tecnología de la información que se enfoque en la protección de los datos personales en su posesión.

Dado en el Palacio del Poder Legislativo de Morelia, Michoacán, a 05 de octubre de 2023.

ATENTAMENTE

JUAN CARLOS BARRAGÁN VÉLEZ

LA PRESENTE HOJA DE FIRMAS CORRESPONDE AL PROYECTO DE DECRETO QUE REFORMAN EL ARTÍCULO 29, FRACCIONES VII Y VIII; Y SE ADICIONA AL ARTÍCULO 29, LA FRACCIÓN IX, AMBOS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DEL ESTADO DE MICHOACÁN DE OCAMPO, DE FECHA 04 DE OCTUBRE DE 2023.

JCBV/amhm*