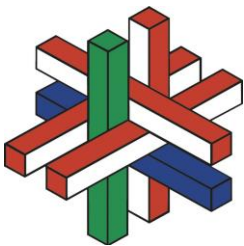


---

**“Enfoque transversal en ciberseguridad para la promoción de las alianzas público-privada”**

Dr. Juan Manuel Aguilar Antonio





## Una idea clave

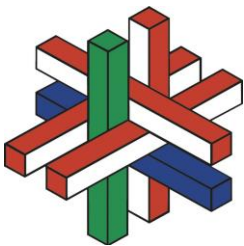
*“La ciberseguridad nacional es una herramienta para alcanzar un estado de cosas deseado, no un fin en sí mismo. E implica una serie de dilemas, como estimular la economía y mejorar la seguridad nacional, promover la protección de datos y la libertad de expresión que son difíciles de equilibrar.”*



**CCDCOE**

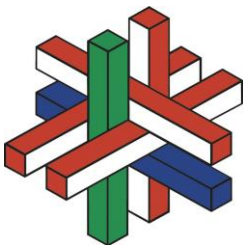
NATO Cooperative Cyber Defence  
Centre of Excellence Tallinn, Estonia

*Eneken Tikk, The Ten Rules of Cybersecurity*

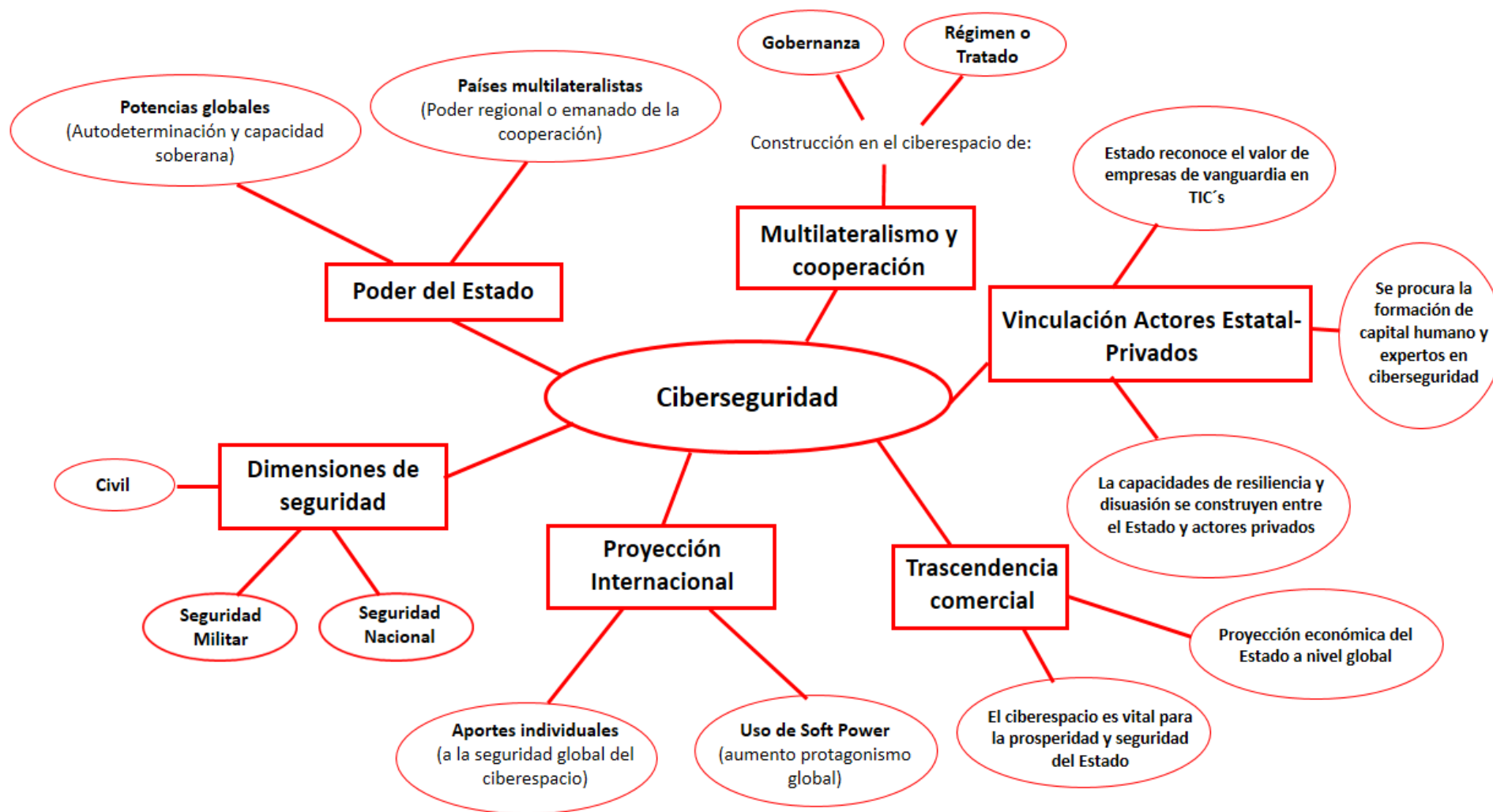


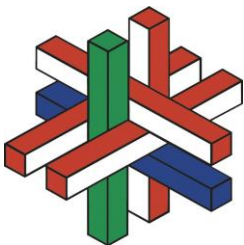
*“La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas.”*

<http://www.seguridadinternacional.es/resi/index.php/revista/article/view/303?fbclid=IwAR3Imt2ZRIOqQtL4ZULRMsPnHmFEv2eYnE0tMA2pugv0c89rsFXg-tYdeR4>



# Elementos clave de ENCS de países de la OTAN



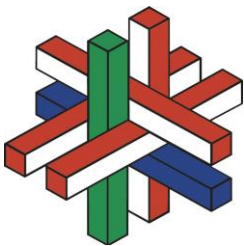


# La construcción de una estrategia nacional de ciberseguridad

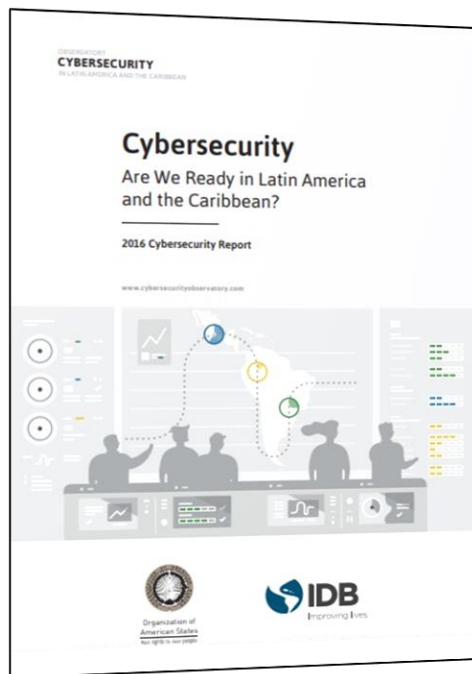
País/Gobierno	Definición de Ciberseguridad	Estrategia Nacional de Ciberseguridad
<b>Australia</b>	<i>“Medidas de seguridad relacionadas con la confidencialidad, disposición e integridad de la información que es procesada, almacenada o compartida por vía electrónica.”</i>	<ol style="list-style-type: none"><li>1. Mantener a salvo a los australianos de ciber riesgos, resguardar y proteger su información de <b><u>identidad, privacidad y finanzas en línea.</u></b></li><li>2. Que las empresas australianas operen con seguridad de su información.</li><li>3. Que el gobierno asegure su información y TIC's así como tenga capacidad de resiliencia.</li></ol>
<b>Canadá</b>	<i>“detectar, identificar y recuperar información electrónica vinculada al internet o la infraestructura física, para su protección, procesamiento, almacenamiento”</i>	<ol style="list-style-type: none"><li>1. <b><u>Seguridad de los sistemas gubernamentales.</u></b></li><li>2. Crear alianza para asegurar los ciber sistemas vitales de Canadá con actores privados.</li><li>3. Ayudar a los canadienses a estar seguros en internet.</li></ol>
<b>Alemania</b>	<i>“la ciber seguridad se divide en seguridad civil y militar, y es el objetivo deseable de utilizar las TIC's para reducir los riesgos de amenaza en el ciberespacio a un nivel aceptable”</i>	<ol style="list-style-type: none"><li>1. <b><u>Efectivo control del crimen en el ciberespacio.</u></b></li><li>2. Coordinación efectiva para la seguridad en Europa y el mundo.</li><li>3. Uso confiable y honesto de información.</li><li>4. Desarrollo de instrumentos para responder a ciber ataques.</li></ol>

País/Gobierno	Definición de Ciberseguridad	Estrategia Nacional de Ciberseguridad
<b>Francia</b>	“el estado deseable de los sistemas de información en que estos puedan resistir eventos del ciberespacio que comprometan su viabilidad, integridad, confidencialidad, almacenamiento y transmisión.”	<ol style="list-style-type: none"> <li>1. <b><u>Ser una potencia en ciberdefensa en el mundo.</u></b></li> <li>2. Salvaguardar la habilidad de Francia para tomar decisiones de protección de información vinculadas a su soberanía.</li> <li>3. Robustecer la ciberseguridad de Infraestructura Nacional Crítica.</li> <li>4. Asegurar la seguridad del ciberespacio.</li> </ol>
<b>Países Bajos</b>	“la libertad de peligro y daño, ruptura, descomposición, o desuso de las TIC’s y la disponibilidad de información”	<ol style="list-style-type: none"> <li>1. <b><u>Seguridad y certeza abierta y libre en la sociedad digital.</u></b></li> <li>2. Robustecer seguridad individual para seguridad colectiva.</li> <li>3. Estimular la economía, incrementar la prosperidad y el bienestar a través del ciberespacio.</li> </ol>
<b>Reino Unido</b>	“acciones tomadas para reducir los riesgos y asegurar los beneficios de un confiable entorno digital para los negocios e individuos”	<ol style="list-style-type: none"> <li>1. <b><u>Combatir al ciber crimen para hacer al ciberespacio un lugar seguro para los negocios.</u></b></li> <li>2. Mejorar la resiliencia a ciber ataques y proteger los intereses de RU en el ciber espacio.</li> <li>3. Ayudar al formar un internet libre, estable y vibrante para la población del RU.</li> <li>4. Desarrollar el conocimiento, habilidades y capacidades que se necesiten para alcanzar los objetivos del RU en el ciberespacio.</li> </ol>

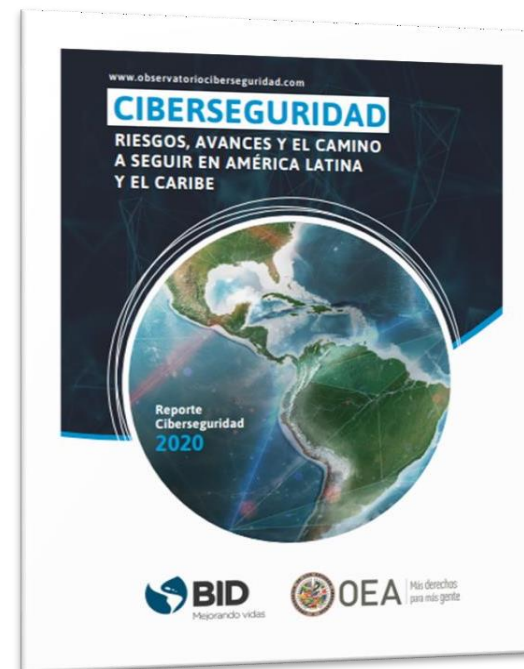




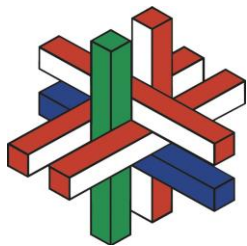
## Un enfoque de partes interesada en México



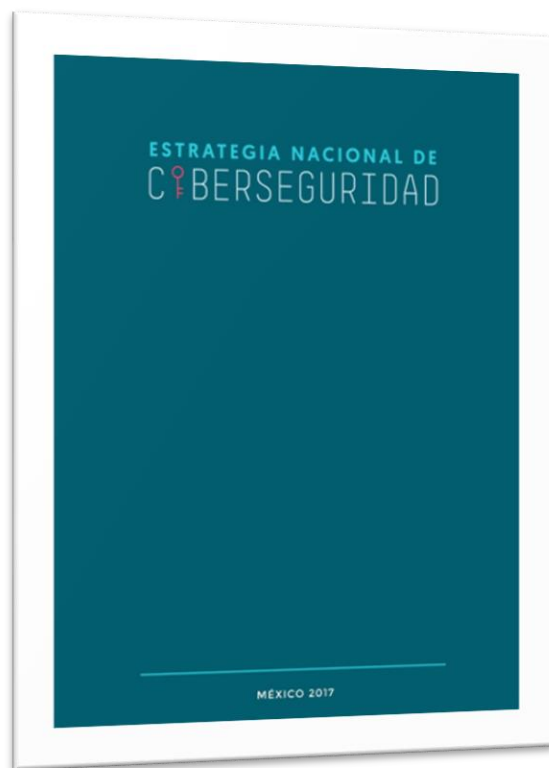
*Cybersecurity Are We Ready in Latin America and the Caribbean?, (OEA/BID)*



Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe (OEA/BID)



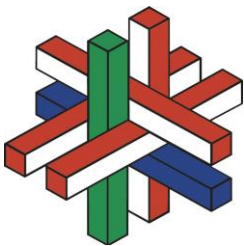
# Estructura de la Estrategia Nacional de Ciberseguridad



**Estrategia Nacional de Ciberseguridad de México (2017)**

<b>Objetivos Estratégicos</b>	<ol style="list-style-type: none"><li>1. Sociedad y derechos.</li><li>2. Economía e innovación.</li><li>3. Instituciones públicas.</li><li>4. Seguridad pública.</li><li>5. Seguridad nacional.</li></ol>
<b>Principios rectores</b>	<ol style="list-style-type: none"><li>1. Perspectiva de derechos humanos.</li><li>2. Enfoque basado en gestión de riesgos.</li><li>3. Colaboración multidisciplinaria y de múltiples actores.</li></ol>
<b>8 ejes transversales</b>	<ol style="list-style-type: none"><li>1. Cultura de ciberseguridad.</li><li>2. Desarrollo de capacidades.</li><li>3. Coordinación y colaboración.</li><li>4. Investigación, desarrollo e innovación TIC.</li><li>5. Estándares y criterios técnicos.</li><li>6. Infraestructuras críticas.</li><li>7. Marco jurídico y autorregulación.</li><li>8. Medición y seguimiento</li></ol>





# Estructura de la Estrategia Digital Nacional 2021-2024

**Visión**

**Independencia Tecnológica**

**Autonomía Tecnología**

**Ejes de la  
Estrategia**

**Política Digital en la APF**

**Política Social Digital**

**Principios**

**Austeridad**

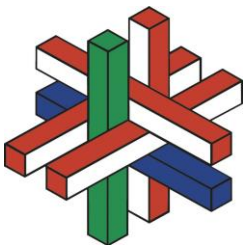
**Combate a la corrupción**

**Eficiencia en los procesos digitales**

**Seguridad de la Información**

**Objetivos**

**Líneas de Acción**



# La ciberseguridad es diferentes para...



**Usuarios**



**Empresas privadas**

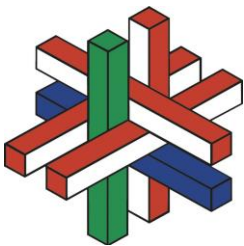
**GOBIERNO DE  
MÉXICO**



**Gobiernos**



**Organismos  
Internacionales**



# La oportunidad de las Asociaciones Público Privadas

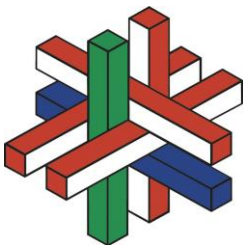
GOBIERNO DE  
**MÉXICO**



**1. Intereses económicos:** Las APP se crean para identificar barreras al crecimiento de la industria de ciberseguridad, exportar productos y colaborar con el sector público en la lucha contra el cibercrimen.

**2. Requisitos regulatorios:** Las APP se establecen como la mejor forma de implementar leyes específicas, especialmente en casos de crisis o emergencias, proporcionando un marco claro para la colaboración público-privada.





## La oportunidad de las Asociaciones Público Privadas

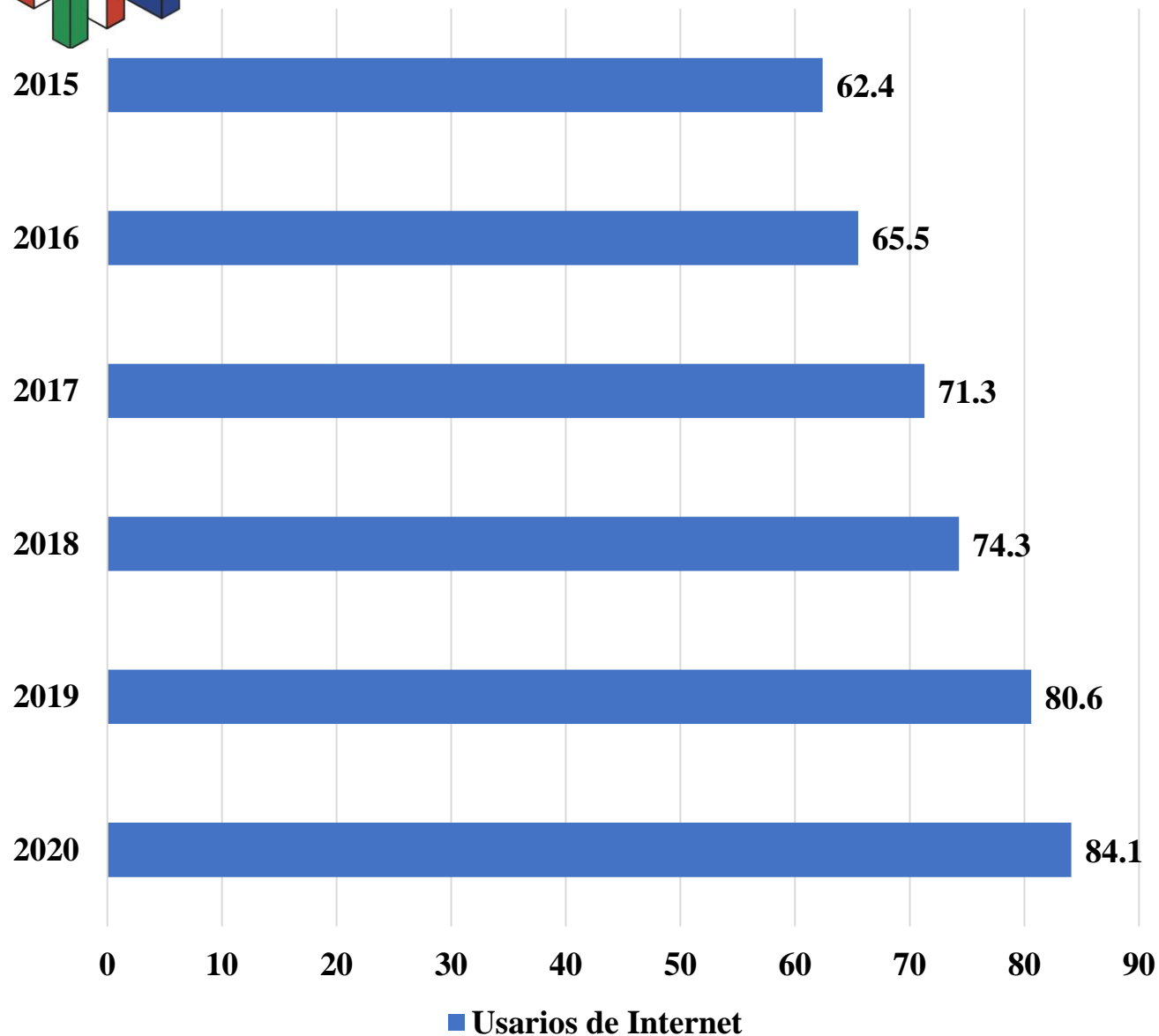
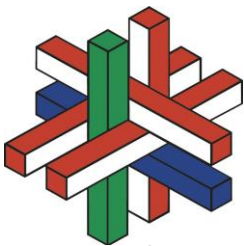
**3. Relaciones públicas:** El gobierno permite al sector privado aportar ideas a nuevas leyes y trabajar en conjunto para desarrollar estrategias nacionales de ciberseguridad, promoviendo el networking y el intercambio de conocimientos.

**4. Intereses sociales:** Se busca discutir ampliamente temas de ciberseguridad a nivel estatal y darles prioridad política, mientras que la industria busca promover la ciberseguridad en general para permitir un mercado sin interrupciones.

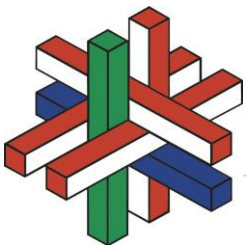
GOBIERNO DE  
**MÉXICO**



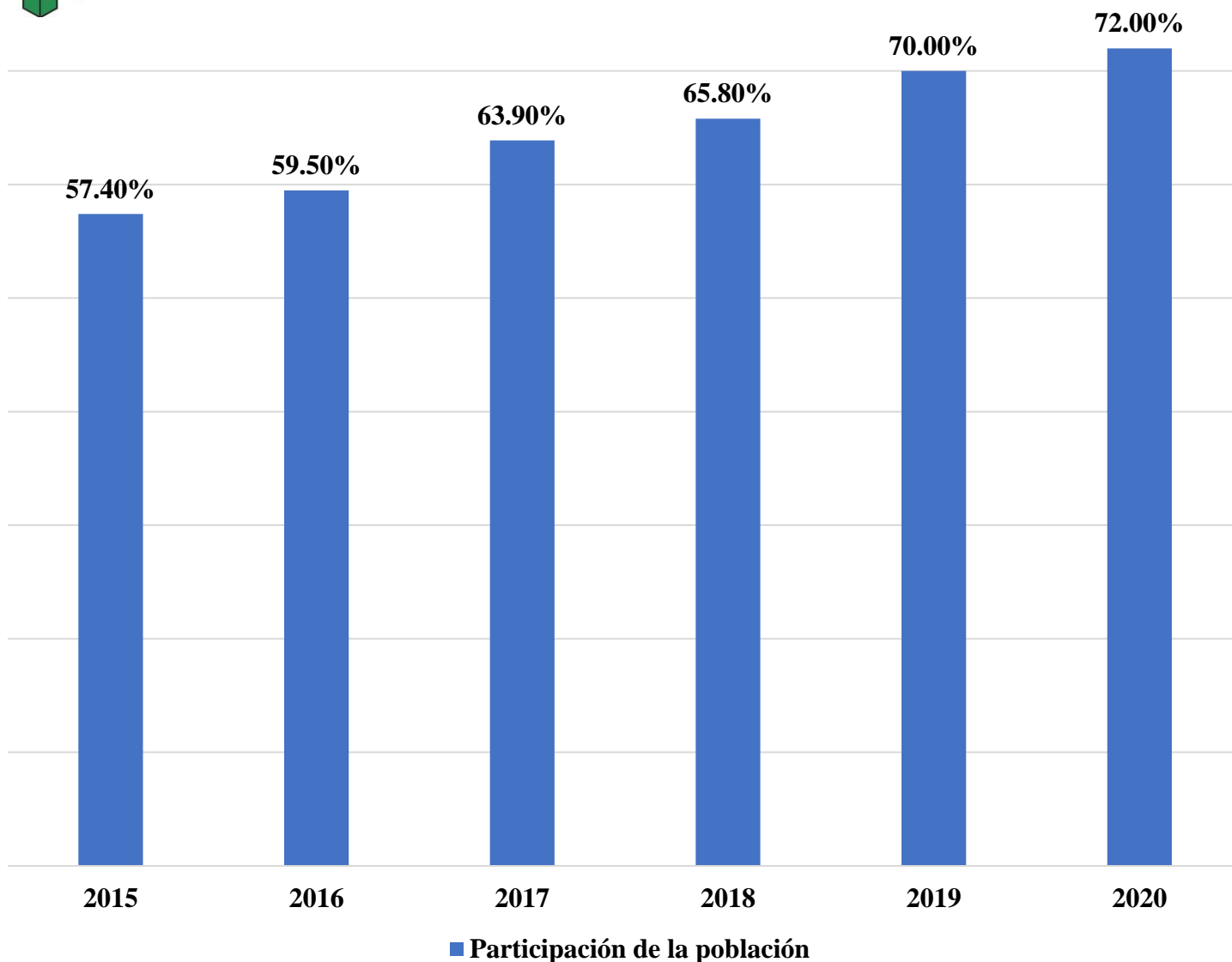
# Brecha digital en México



- La ENDUTIH 2020 del INEGI estima que 78.3% de la población ubicada en áreas urbanas son usuarios.
- Mientras que en el área rural la proporción es de 50.4 por ciento.

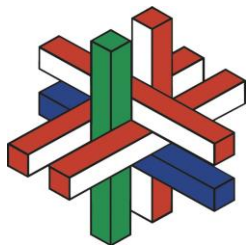


# Brecha digital en México



- En 2020 los usuarios en zonas urbanas se estimaron en 76.6% y en zonas rurales la estimación fue de 47.7 por ciento.





# La necesidad de un enfoque multistakeholder para una estrategia nacional de ciberseguridad



**2017**

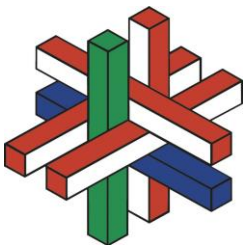


**2018**



**2021-2014**





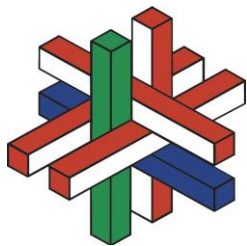
# Instituciones en México para combate ciberdelincuencia



---

**FGR**  
FISCALÍA GENERAL  
DE LA REPÚBLICA

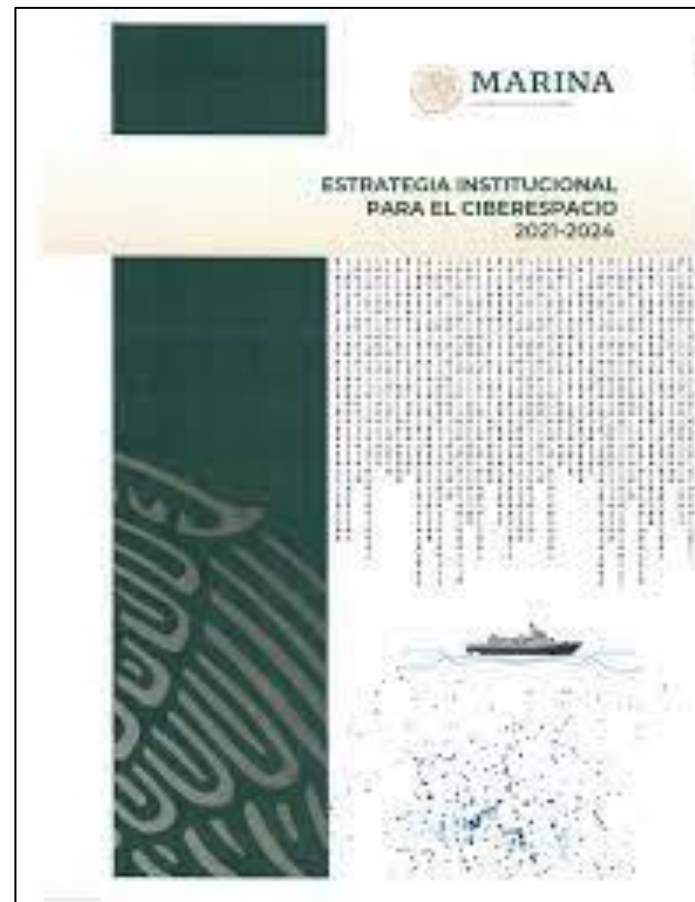
---



## La necesidad de un enfoque multistakeholder para una estrategia nacional de ciberseguridad

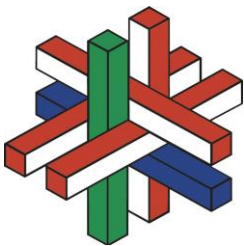


**Glosario de Términos SEDENA-Marina en materia de seguridad en el ciberespacio (2021)**

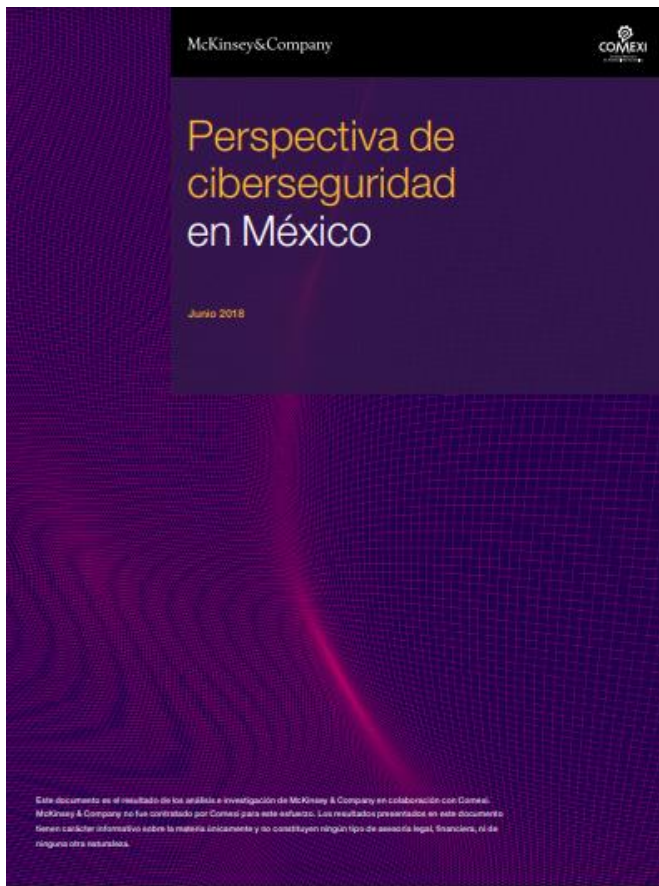


**Estrategia Institucional para el Ciberespacio (2021-2024)**

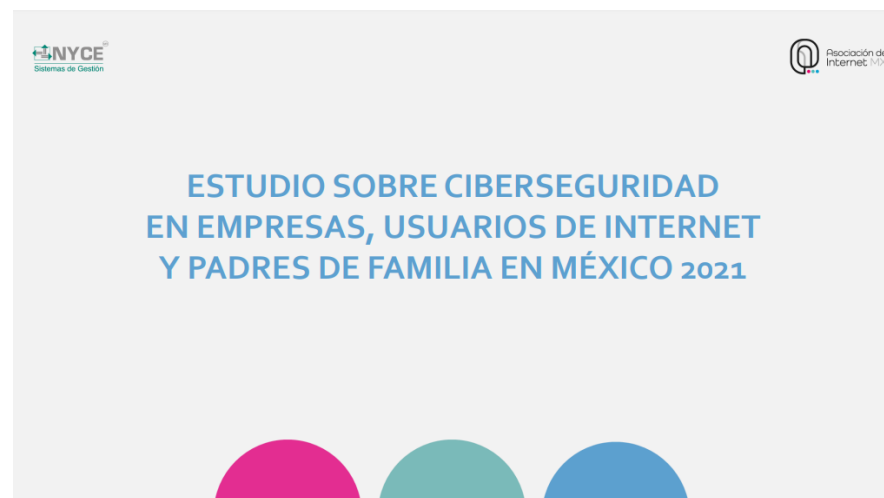




# La necesidad de un enfoque multistakeholder para una estrategia nacional de ciberseguridad



**Perspectiva de ciberseguridad en México 2018 (Mc Kinsey Company y COMEXI)**



**Estudio sobre ciberseguridad en empresas, usuarios de internet y padres de familia en México 2021 (AIMX)**

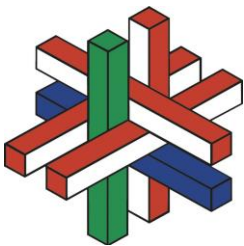


**El Estado de la Ciberseguridad en México (2021)**



# Iniciativa de Ley Nacional de Ciberseguridad o Ciberdelicuencia

<b>No.</b>	<b>CÁMARA</b>	<b>LEGISLATURA</b>	<b>FECHA DE PRESENTACIÓN</b>	<b>AUTOR(ES)</b>
1	Senadores	LXIV	23/10/2018	Alejandra Lagunes Soto Ruíz (PVEM)
2	Diputados	LXIV	08/04/2019	José Salvador Rosas Quintanilla (PAN)
3	Diputados	LXIV	29/10/2019	Javier Salinas Narváez (MORENA)
4	Diputados	LXIV	05/11/2019	Enviada por la Cámara de Senadores
5	Diputados	LXIV	08/01/2020	María Eugenia Hernández Pérez (MORENA)
6	Diputados	LXIV	12/08/2020	María Eugenia Hernández Pérez (MORENA)
7	Senadores	LXIV	02/09/2020	Miguel Ángel Mancera Espinosa (PRD)
8	Senadores	LXIV	04/11/2020	José Ramón Enríquez Herrera (MORENA)
9	Senadores	LXIV	06/04/2021	Jesús Lucía Trasviña Waldenrath (MORENA)
10	Senadores	LXV	14/10/2021	Jesús Lucía Trasviña Waldenrath (MORENA)
11	Diputados	LXV	15/12/2021	Lidia García Anaya (MORENA)
12	Senadores	LXV	25/04/2023	Javier López Casarín (PVEM)



## La necesidad de un enfoque multistakeholder para una estrategia nacional de ciberseguridad



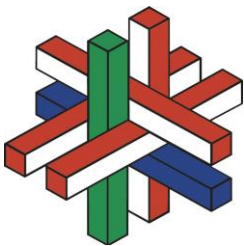
**AMCID** Academia Mexicana  
de Ciberseguridad  
y Derecho digital



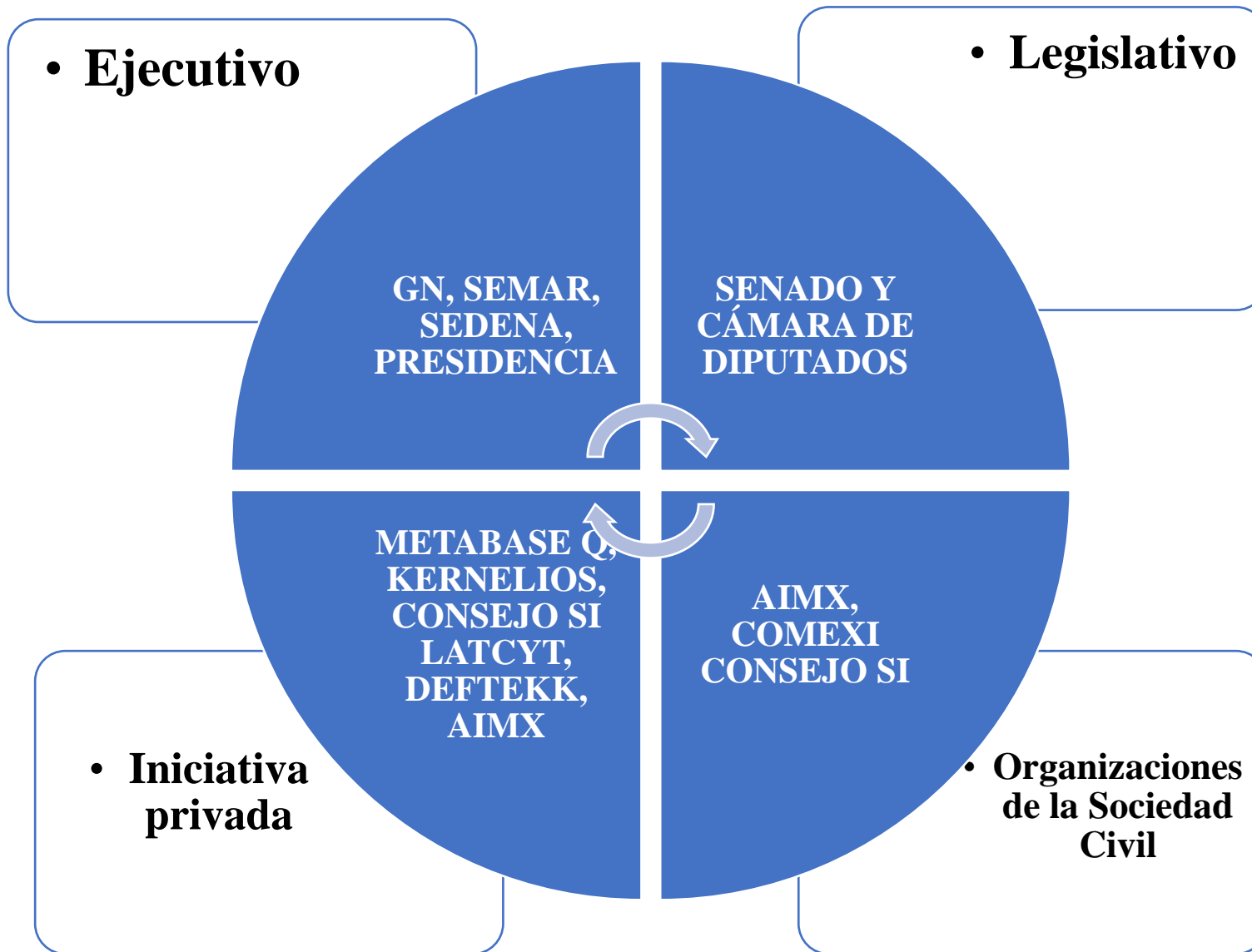
**METABASE Q**

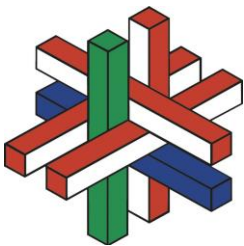
**DEFTEKK**  
CYBERSECURITY





# La necesidad de un enfoque multistakeholder para una estrategia nacional de ciberseguridad





# Un ejemplo de interrelación de APP en materia ciberseguridad

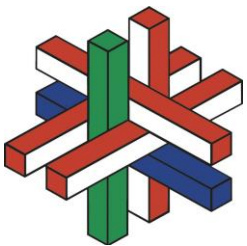
Recientemente en México se crearon las legislaciones de tipo **Ley Olimpia** es la denominación que adquiere un conjunto de reformas legislativas en distintos estados de México.

Estas leyes están encaminadas a reconocer la violencia digital y sancionar los delitos que violen la intimidad sexual de las personas a través de medios digitales, también conocida como ciber violencia o violencia digital.



Entidad Federativa	Regulación	Sanción	Fecha de publicación
Aguascalientes	Código Penal para el estado de Aguascalientes <b>Artículo 181 b</b>	<b>1 a 4 años de prisión</b> 300 a 600 días multa, así como al pago total de la reparación de los daños y perjuicios ocasionados	28 de noviembre de 2019
Baja California	Código Penal para el estado de Baja California <b>Artículo 175 sexties</b>	<b>1 a 6 años de prisión</b> Multa de 500 a 1500 veces la unidad de medida y actualización	Aprobada (pendiente de publicar)
Baja California Sur	Código Penal para el estado libre y soberano de Baja California Sur <b>Artículo 183 Quáter</b>	<b>3 a 6 años de prisión</b> Multa de 1000 a 2000 días multa al momento de que se cometa el delito	20 de junio de 2019
Chiapas	Código Penal para el estado de Chiapas <b>Artículo 343 Bis</b>	<b>3 a 5 años de prisión</b> 100 a 200 días multa	5 de marzo de 2019
Ciudad de México	Código penal para el Distrito Federal <b>Artículos 181 Quintus, 209 y 236</b>	<b>4 a 6 años de prisión</b> Multa de 500 a 1000 unidades de medida y actualización	22 de enero del 2020
Coahuila	Código Penal de Coahuila de Zaragoza <b>Artículo 236, fracción III</b>	<b>3 a 6 años de prisión</b> Multa de 1000 a 2000 unidades de medida y actualización	12 de julio de 2019
Durango	Código Penal para el estado libre y soberano de Durango <b>Artículo 182 ter</b>	<b>4 a 8 años de prisión</b> Multa de 288 a 566 unidades de medida y actualización	29 de diciembre de 2019
Guanajuato	Código Penal del Estado de Guanajuato <b>Artículo 187-e</b>	<b>2 a 4 años de prisión</b> 20 a 40 días multa	19 de junio de 2019
Guerrero	Código Penal para el estado libre y soberano de Guerrero <b>Artículo 187</b>	<b>3 a 6 años de prisión</b> Multa de 200 hasta 1000 veces el valor diario de la Unidad de Medida y Actualización	8 de noviembre de 2019
Estado de México	Código Penal del Estado de México <b>Artículos 211 Ter y 211 Quater</b>	<b>1 a 5 años y de 3 a 7 años de prisión</b> Multa de 200 a 500 y de 200 a 400 unidades de medida y actualización	5 de septiembre de 2019

Entidad Federativa	Regulación	Sanción	Fecha de publicación
Jalisco	Código Penal del Estado de Jalisco <b>Artículo 176 Bis 1 y 176 Bis 2</b>	<b>1 a 8 años de prisión</b> Multa de 1000 a 2000 unidades de medida y actualización	19 de septiembre de 2020
Michoacán	Código Penal para el estado de Michoacán de Ocampo <b>Artículos 195 y 195 bis</b>	<b>4 a 8 años de prisión</b> Multa de 1000 a 2000 veces el valor diario de la Unidad de Medida y Actualización y desde 1000 hasta 2000 veces el valor diario de la Unidad de Medida y Actualización por concepto de reparación del daño	13 de enero de 2020
Nuevo León	Código Penal para el estado de Nuevo León <b>Artículo 271 bis 5</b>	<b>6 meses a 4 años de prisión</b> Multa de 800 a 200 cuotas	19 de diciembre de 2018
Oaxaca	Código Penal para el estado libre y soberano de Oaxaca <b>Artículo 249</b>	<b>4 a 8 años de prisión</b> Multa de 1000 a 2000 veces el valor diario de la unidad de medida y actualización vigente al momento de que se cometa el delito	24 de agosto de 2019
Puebla	Código Penal del estado libre y soberano de Puebla <b>Artículo 225</b>	<b>3 a 6 años de prisión</b> Multa de 1000 a 2000 veces la unidad de medida y actualización al momento de que se cometa el delito	10 de diciembre de 2018
Querétaro	Código Penal para el estado de Querétaro <b>Artículos 167 Quáter y 167 Quinquies</b>	<b>3 a 6 años de prisión</b> 1000 a 2000 veces el valor diario de la UMA, y desde 1000 hasta 2000 veces el valor diario de la UMA por concepto de reparación del daño	12 de julio de 2019
Veracruz	Código Penal para el estado libre y soberano de Veracruz de Ignacio de la Llave <b>Artículos 190 Quincecies, 190 Sexdecies y 190 Septendecim</b>	<b>4 a 8 años de prisión</b> Multa de 1000 hasta 2000 Unidades de Medida y Actualización, al momento de que se cometa el delito	4 de junio de 2019
Yucatán	Código Penal del estado de Yucatán <b>Artículo 243 bis 3 y 243 bis 4</b>	<b>1 año a 5 años y de 6 meses a 4 años de prisión</b> Multa de 100 a 400 y de 200 a 500 unidades de medida y actualización	22 de junio de 2018
Zacatecas	Código Penal para el estado de Zacatecas <b>Artículo 232 Ter</b>	<b>4 a 8 años de prisión</b> Multa de 100 a 200 veces el valor diario de la Unidad de Medida y Actualización	31 de agosto de 2019



# Oportunidad de APP en materia ciberseguridad



**Desinformación**



**Nuevas  
Tecnologías**



**Actividad  
criminal en el  
internet**