Delitos cibernéticos

Esther Elizabeth Albarrán Martínez[a]

Resumen / *Abstract*

La sofisticación en los delitos de la mano con la tecnología marcha a una velocidad vertiginosa, hacerle frente tanto en la legislación como en la división de funciones de las autoridades y en las estrategias de prevención y combate es un arduo desafío en el país. La coordinación y trabajo en conjunto del sector privado con el público es un factor clave en esta tarea. La ciberseguridad y la protección de datos personales juegan roles importantes para conseguir las metas deseadas, pues contar con estrategias bien trazadas para evitar vulneraciones e intrusiones a los sistemas informáticos auxiliará a reforzar la defensa ante posibles ataques cibernéticos. Capacitar y concientizar tanto a empresas, servidores públicos y sociedad no solo en ciberseguridad y protección de datos personales es crucial para reducir los delitos informáticos y contar con un ciberespacio más seguro.

Palabras clave: fraudes, internet, delitos cibernéticos, datos personales, ciberseguridad.

The sophistication in the crimes of the hand with the technology marches to a vertiginous speed, to face it as much in the legislation as in the division of functions of the authorities and in the strategies of prevention and combat is an arduous challenge in the country. The coordination and joint work of the private sector with the public sector is a key factor in this task. Cybersecurity and personal data protection play important roles to achieve the desired goals, since having well-defined strategies to avoid violations and intrusions to computer systems will help strengthen the defense against possible cyber attacks. Training and raising awareness of companies, public servants and society, not only in cyber security and personal data protection, is crucial to reduce computer crimes and have a safer cyberspace.

Keywords: *fraud, internet, cybercrime, personal data, cybersafety.*

a. Maestrante en materia de Transparencia y Datos Personales en la Universidad de Guadalajara y Licenciada en Derecho por la UNAM.

INTRODUCCIÓN

La tecnología y su constante actualización han traído diversos beneficios para la humanidad. Hoy en día podemos comunicarnos en tiempo real con personas que se encuentran en otros países; la investigación y tratamientos médicos han mejorado al punto de prevenir y eliminar enfermedades que antes eran mortales; el uso del internet ha facilitado el teletrabajo desde casa o *home office*, el uso del cómputo en la nube, de redes sociales para dar opiniones y mantenernos informados; asimismo ha sido una herramienta clave para afrontar la contingencia sanitaria que enfrentamos actualmente, entre otros tantos beneficios. En resumen, la tecnología, específicamente el internet, ha proporcionado las herramientas necesarias para hacer que las personas tengan una vida más productiva, cómoda, entretenida e informada.

El Plan Nacional de Desarrollo 2019-2024 prevé cobertura de internet para todo el país, por lo que se estima que para el año 2025 existan más de 300 millones de dispositivos con acceso a las redes en México, 70% más de los 180 millones que ya existen (McKinsey & Company en colaboración con el Colegio Mexicano de Asuntos Internacionales, 2018, pág. 13).

Sin embargo, su potencialidad nos obliga a un planteamiento clave: ¿qué sucede cuando la tecnología es usada para sacar provecho de unos cuantos y en detrimento de los usuarios? Día a día dependemos más de la misma para realizar nuestras actividades cotidianas, pero esto tiene consecuencias, sobre todo cuando no se usa de manera informada y responsable.

Esta situación se refleja en el aumento de "crímenes cibernéticos" durante la época de la pandemia causada por el virus SARS COV 2. La propia Secretaria General Adjunta de Asuntos de Desarme de la ONU, Izumi Nakamitsu, advirtió en mayo pasado durante una reunión informal del Consejo de Seguridad del probable aumento al 600% de ataques en la red.

A finales de 2019, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financiero (CONDUSEF) informó del aumento del 36% de fraudes cibernéticos respecto del año anterior, llegando a un estimado de 5.8 millones de fraudes cibernéticos durante 2019[1].

Estos datos reflejan que los delitos van aumentando no solamente en cantidad, sino que los métodos y modalidades en que los mismos se efectúan van de la mano con la actualización de la tecnología. Es por ello que, desde hace años, han surgido nuevos tipos penales y se han sofisticados delitos previamente existentes.

Estos delitos son conocidos como delitos cibernéticos, delitos informáticos o ciberdelitos, en los cuales los criminales utilizan las computadoras como medio o fin para cometerlos

1 Estadísticas sobre el comercio electrónico que pueden ser consultadas en el siguiente vínculo: https://www.condusef.gob.mx/?p=estadisticas

(Nava, 2015). Lo anterior, quiere decir que estas conductas pueden cometerse bajo diversas modalidades, utilizando las tecnologías de la información como medio o fin en sí mismo; para encontrar víctimas, para acceder, alterar o destruir información, entre otros.

Cualquier persona que utilice internet puede ser víctima: tanto ciudadanos, como pequeñas y medianas empresas, corporaciones trasnacionales, así como gobiernos pueden ser afectados por este tipo de ilícitos, incluso al grado de poner en riesgo la seguridad nacional. Sin embargo, las personas físicas recienten directamente los efectos y pérdidas en sus derechos y bienes jurídicos más preciados.

Esto quiere decir que actualmente, con el uso desmedido de los dispositivos inteligentes y el internet, ya no existe un hombre que "reina" gracias a la tecnología inventada por él, sino más bien un hombre sometido a la tecnología, dominado por sus máquinas, como alertaba Sartori (2019, pág. 141).

SOBRE LOS DELITO INFORMÁTICOS EN MÉXICO

A pesar de ser una situación mundial que afecta más a determinados países, México se encuentra dentro de los primeros lugares pues de acuerdo con datos del mapa en tiempo real de Kaspersky[2], México es el décimo país a nivel mundial más atacado cibernéticamente.

No obstante, actualmente el país no cuenta con un catálogo específico en materia de delitos cibernéticos, sino que estas conductas se encuentran tipificadas alrededor de diferentes códigos y leyes tanto federales como locales, por lo que las conductas y las penas pueden variar desde pornografía infantil, fraude, robo de identidad y robo de datos, entre otros.

En este tipo de conductas, el sujeto activo (es decir, la persona que efectúa la conducta) cuenta con conocimientos avanzados en tecnología (no es indispensable ser un genio, basta con tener conocimientos superiores a la mayoría de la población) y se aprovecha del desconocimiento o vulnerabilidad de personas, empresas y/o instituciones para acceder a sistemas ajenos, extraer información, causar daños, pérdidas o alteraciones en los mismos.

En la doctrina, terminología para referirse a cada uno de los atacantes es variada y depende del tipo de conducta que realicen:

- *Hacker:* Personas que acceden de manera no autorizada a sistemas informáticos, no necesariamente con la finalidad de causar un daño.
- *Cracker:* Personas que acceden de manera no autorizada a sistemas informáticos. A diferencia de los hackers, los crackers si tienen la intención de causar daños y/o pérdidas al sistema. También conocidos como piratas informáticos.

2 El mapa en tiempo real puede ser consultado en el siguiente hipervínculo: https://cybermap.kaspersky.com/es

- *Hactkvista:* Combinación entre hacker y activista. La persona demuestra su disgusto ante organizaciones públicas o privadas mediante el aprovechamiento de la vulneración de sus sistemas informáticos.
- *Phreaker:* Son crackers de sistemas telefónicos.

Como mencioné anteriormente, en México no se cuenta con un catálogo o capítulo específico. No obstante, a nivel federal el Código Penal Federal tipifica las siguientes conductas que pueden realizarse a través de medios electrónicos:

- Comunicación de Contenido Sexual con Personas Menores de Dieciocho Años de Edad o de Personas que no tienen Capacidad para comprender el Significado del Hecho o de Personas que no tienen la Capacidad para Resistirlo (Título Séptimo, art. 199 Bis);
- Revelación de secretos (Título Noveno, art. 210-211 Bis);
- Acceso ilícito a sistemas y equipos de informática (Título Noveno, art. 210-211 Bis);
- Pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo (Título Octavo, Capítulo 2, art. 202)

Sin embargo, las conductas van más allá, pues los tipos penales anteriormente mencionados pueden englobar las siguientes acciones:

- *Phising:* A través del engaño, se hace creer al usuario que el delincuente es otra persona o institución con la finalidad de robar información.
- *Ataques de malware o código malicioso:* Programas que se mantienen ocultos en algún dispositivo tecnológico. Virus informático, spyware, troyanos, gusanos.
- *Espionaje informático:* Acceso no autorizado de intrusos para conocer la información de otros usuarios.
- *Spam:* Envío no autorizado de mensajes o correos electrónicos para ingresar a la información de los usuarios.
- *Negación de servicios:* Se impide la visita a una página electrónica específica, a través de la saturación de la misma.

SOBRE LA COMPETENCIA DE LAS AUTORIDADES ANTE LOS DELITOS INFORMÁTICOS

A su vez, la competencia de las autoridades es un tema por resolver. Actualmente la Policía Federal cuenta con el Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX) y la Secretaría de Seguridad Pública y Protección Ciudadana cuenta con el Centro Nacional de Inteligencia (CNI), anteriormente CISEN. Organismos cuyas facultades son la prevención e investigación de delitos, entre los cuales se ubican los delitos cibernéticos.

Ante estas lagunas, se han presentado proyectos como la iniciativa de Ley de Seguridad Informática[3] presentada por la senadora Lucía Trasviña Waldenrath, tiene como fin crear una ley especializada en materia de ciberdelitos y propone la creación de una Agencia Nacional de Seguridad Informática como la encargada de coordinar la política en la materia.

Por otra parte, en 2017 el gobierno de México emitió la Estrategia Nacional de Ciberseguridad en coordinación con la OEA, sin embargo, dicho documento se encontraba centrado en el Plan Nacional de Desarrollo 2013-2018, sin actualizarse con el Plan de la nueva administración, además de no consolidar los principios establecidos por la misma.

LA VULNERACIÓN DE LOS DERECHOS HUMANOS ANTE LOS DELITOS CIBERNÉTICOS

Retomando el punto de los delitos informáticos, la consecución de estas conductas delictivas lleva consigo transgresiones a bienes jurídicos como el patrimonio, la privacidad de la información sexual, y la propia seguridad nacional, entre otros. No obstante, no solo bienes jurídicos tutelados por el derecho penal son vulnerados, sino que los derechos humanos también se ven mermados ante estas acciones, como la privacidad y la protección de los datos personales.

LA PRIVACIDAD

Isaiah Berlin definió la privacidad (Escalante, 2004, pág. 17) como "libertad negativa", es decir, la ausencia de obstáculos o coacciones para que cada persona pueda obrar como mejor le parezca. O sea, la privacidad es el espacio en el cual la autonomía y la libertad individual imperan sobre las decisiones de la colectividad.

En este tenor, "el derecho a la privacidad podría definirse como aquél que todo individuo tiene a separar aspectos de su vida privada del escrutinio público" como establece García Ricci (2013). Esto quiere decir que la privacidad es la esfera del ser humano concerniente únicamente al individuo mismo, en la que la libertad personal marca las pautas de acción, sin vulnerar las libertades y esferas de los demás.

Por lo anterior, es preciso señalar que penetrar la esfera de lo privado conlleva un riesgo inminente a la salvaguarda de los derechos de la persona, por lo que dicho conceptos necesita la protección de la ley para evitar abusos en contra de los individuos. Es así que, al resguardar el ámbito privado se garantiza el ejercicio de otros derechos fundamentales, necesarios para el desarrollo personal.

---

3 Misma que puede consultarse en la siguiente liga: https://infosen.senado.gob.mx/sgsp/gaceta/64/1/2019-03-27-1/assets/documentos/Inic_MORENA_Seguridad_Informatica.pdf

LA PROTECCIÓN DE DATOS PERSONALES

Por su parte, la protección de datos personales es un derecho de reciente aparición cuya finalidad es brindar un tratamiento efectivo de la información personal que recaban tanto empresas como instituciones gubernamentales.

Un dato por sí solo no es susceptible de protección, sino que a quien se protege es al titular del dato. Por lo tanto, los datos que circulan en la red corren riesgos, sumado a problemas de jurisdicción del internet, como sucede en México.

Aunado a lo anterior, a nivel global aún no se cuenta con estándares o normatividad de manera uniformada sobre el tema, lo cual dificulta la cooperación internacional. A pesar de ello, existe normatividad regional o sectorial como la establecida por la Unión Europea, de la cual México podría aprender.

En México, este derecho se encuentra plasmado en los artículos 6o., Base A y 16, segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), que establece la protección a la vida privada y los datos personales, la cual deberá realizarse mediante la expedición de leyes secundarias.

De esta manera, los particulares se rigen por la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP) de 2010, por su parte las instituciones públicas se rigen por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) publicada en 2017, así como por las leyes locales en la materia.

Cada una de estas normas constriñe a las responsables del tratamiento de datos, a proteger y salvaguardar la información personal que recaban a través de medidas de seguridad que pueden ser administrativas, técnicas y físicas, con la finalidad de evitar vulneración a la privacidad de los titulares de los datos.

Una medida de seguridad es un instrumento, política o herramienta que en cierta medida crea confianza y certidumbre en usuarios informáticos sobre el resguardo y protección de información.

El objetivo de implementar medidas de seguridad es que cada una de ellas ayude a reducir el riesgo de que se materialice un incidente y sus consecuencias desfavorables. Las medidas de seguridad también ayudan a que, en caso de que se presente un incidente, se reduzca el daño a los titulares y a la empresa u organización (INAI, 2005, pág. 6).

Hacer uso adecuado de los datos recabados es esencial en entes públicos como privados así como contar con las medidas necesarias para evitar vulneraciones, ya que muchos de ellos resguardan información personal de clientes y usuarios que van desde datos de identificación (nombre, domicilio, teléfono, correo electrónico), datos patrimoniales (información fiscal y financiera, cuentas bancarias, créditos) datos sensibles (información de salud, ideología), a datos biométricos (iris, huellas dactilares, ADN).

En palabras de Mendoza Enríquez (2018), "factores como el uso indebido de la información o la vulneración de medidas de seguridad de la misma, ponen en riesgo la reputación de las empresas, y las podrían hacer acreedoras de sanciones, por lo que resulta necesario estudiar el tema desde una perspectiva regulatoria, que incluya: legislación, normas sectoriales y buenas prácticas".

Esta evolución continua de la informática que se refleja en la sofisticación de los ataques cibernéticos y en la vulneración de los sistemas informáticos tanto de particulares como de entes públicos, obliga a generar medidas de seguridad informáticas que evolucionen constantemente para resguardar la información contenida.

De igual manera, la capacitación en materia de protección de datos personales frente al personal de las instituciones es sumamente importante, ya que el conocimiento sobre el tema hará más fácil el cumplimiento de las obligaciones establecidas por las normas de protección de datos personales y evitará las prácticas desleales como la venta de bases de datos de manera ilegal.

Por su parte el Programa Nacional de Protección de Datos Personales 2018-2022 (PRONADATOS), establecido por el Sistema Nacional de Transparencia, establece las estrategias, objetivos, líneas de acción y líneas estratégicas que el Sistema implementará en materia de protección de datos personales en el país, mismos que se actualizarán y evaluarán de manera anual. Entre las estrategias a implementar se encuentran las siguientes:

- Realizar análisis de brechas entre las medidas de seguridad establecidas y las faltantes.
- Registro de los medios de almacenamiento de los datos personales.
- Efectuar acciones correctivas y preventivas para mejorar medidas de seguridad.
- Implementar avisos de privacidad visuales o sonoros, con los ajustes razonables necesarios para personas con discapacidad.
- Elaborar políticas y programas de privacidad.
- Desarrollar sistemas de vigilancia internos.
- Rastrear datos personales durante el tiempo que dure su tratamiento (trazabilidad).

Sin embargo, contar con medidas de seguridad en materia de protección de datos personales no es la única solución. Para evitar y contrarrestar ataques cibernéticos, así como para hacer frente a estos eventuales riesgos, es necesario contar con estrategias y políticas de ciberseguridad.

SOBRE LA CIBERSEGURIDAD

La ciberseguridad es el conjunto de acciones tomadas por organizaciones e individuos para mitigar los riesgos que enfrentan en el ciberespacio, con el propósito de disminuir la probabilidad de sufrir un ciberataque (McKinsey & Company en colaboración con el Colegio Mexicano de Asuntos Internacionales, 2018, pág. 21). Este tipo de herramientas

es de vital importancia dentro de empresas y organizaciones públicas en materia de telecomunicaciones, seguridad, salud, energía, finanzas, laborales, protección de derechos humanos, entre otros.

Esto quiere decir que es imprescindible contar con políticas de seguridad para evitar la comisión de actos ilícitos que afecten directamente a las personas y a su vez, estos planes deben contener mecanismos de identificación de riesgos y programas de protección ante los mismos.

Estas estrategias de ciberseguridad, deben estar estrechamente ligadas con la protección de los datos personales y la privacidad de las personas, así como el uso del internet en la vida cotidiana de las personas, al momento de su planeación, implementación y actualización continua.

El desarrollo de un plan de prevención de seguridad de información y un plan de atención a crisis, también es una medida importante en cualquier institución, para conocer los procedimientos y pasos a seguir ante cualquier tipo de vulneración de los sistemas.

A pesar de que muchos de los responsables de tratamiento de datos personales, ante posibles incidentes, cuentan con medidas de seguridad similares, es necesario establecer los supuestos ante los cuales las organizaciones pueden estar en riesgo y de manera particular instaurar las medidas de seguridad, dependiendo del tipo de vulneración a la cual se debe hacer frente.

Conocer las fortalezas y debilidades de los sistemas informáticos de cada institución o empresa, así como los posibles riesgos a los cuales se está expuesto, es de suma importancia para analizar las repercusiones y tomar decisiones adecuadas sobre las medidas de seguridad más adecuadas para cada caso en concreto, siempre con miras de prevención.

Lo anterior de conformidad con lo argumentado por Calderón Martínez (2013, p. 1), “el objetivo es encontrar los mecanismos para garantizar la seguridad de los sistemas de cómputo, en virtud de que se han convertido en un pilar para la seguridad nacional y el éxito económico de las naciones.”

Sin embargo, para implementar estas medidas, planes y protocolos es sumamente necesario analizar caso por caso qué tipo de información recaba cada organización, para qué se utiliza, en dónde se almacena tanto física como virtualmente, quiénes tienen acceso a la misma y las obligaciones con las que cuentan al respecto.

Esta información servirá para poder implementar un plan adecuado a las características particulares de cada institución y no correr el riesgo de ser víctima de un evento inesperado o la actuación de personas ajenas a la organización que traiga como consecuencia pérdidas económicas, conflictos legales e incluso pérdida de confianza por parte de la sociedad.

Dentro de cada institución pública u organización privada es de vital importancia contar con un plan que involucre procedimientos y herramientas de respaldo de la información, así como los procedimientos necesarios a implementar en caso que ocurra un desastre. De esta

manera, los encargados de cada área podrán contar con la seguridad que la información que guardan en sus archivos electrónicos no se perderá y podrán seguir utilizándola en el futuro.

Es así que algunas de las herramientas y estrategias en materia de seguridad con la que cada entidad pública y privada debe contar, son las siguientes:

- Cifrado de datos.
- Uso de redes privadas virtuales (VPN´S).
- Procedimientos de eliminación de datos de manera segura, cuando los mismos ya no sean necesarios o termine su tratamiento.
- Procedimientos de autenticación e identificación de usuarios internos.
- Contar con un sistema de detección de intrusos, con la finalidad de detectar intromisiones no autorizadas, asegurar el sistema de un posible ataque y/o crear distracciones para engañar y controlar atacantes.
- Concientización y capacitación continua al personal con la finalidad de que conozcan el tipo de amenazas ante las cuales es posible enfrentarnos y conocer los protocolos de actuación para evitar y enfrentar un ataque a la seguridad o pérdida de información.
- Creación y actualización continua de contraseñas.
- Contar con un control de acceso para la aprobación o negación del paso a personas no autorizadas a lugares físicos o tecnológicos con parámetros de seguridad actuales.

Adquisición de paquete de software antivirus y eliminadores de malwareLas anteriores acciones son estrategias que tanto el sector público como el sector privado pueden ejercer para proteger sus sistemas informáticos y con ello, la información personal de millones de ciudadanos. Pero, ¿qué pueden hacer los ciudadanos para evitar ser víctimas de estos ilícitos?

DE LOS USOS Y COSTUMBRES DE LOS CIBERNAUTAS EN MÉXICO, APUNTES FINALES

La sociedad mexicana, si bien utiliza en gran medida las tecnologías de la información realizando transacciones, compras y transferencias bancarias, también es cierto que muy poco porcentaje sabe cómo utilizar responsablemente esta tecnología. A su vez, el conocimiento de la protección de datos personales y el ejercicio de los derechos ARCO por parte de la sociedad es mínimo.

Según datos del Censo Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales Federal de 2017 efectuado por el INEGI, 21 mil 727 solicitudes de acceso a la información y protección de datos personales recibidas por los órganos garantes federal y locales durante 2016, únicamente el 2.2% de las mimas correspondieron a solicitudes de protección de datos personales.

A nivel local, en la Ciudad de México, el órgano garante local informó que del periodo comprendido del 1° de enero al 30 de septiembre de 2018 se recibieron 6 mil 121 solicitudes de derechos ARCO.

Esta situación refleja el desconocimiento por parte de la población de la existencia de la protección de su información personal, el desconocimiento del significado de un aviso de privacidad y de las medidas de seguridad con las que cada institución debe contar para el resguardo de dichos datos, así como de la importancia que tienen sus datos y el valor que pueden tener en el mercado.

Es por ello, que los órganos garantes cuentan con mayor obligación que nunca de difundir, socializar y concientizar a la población sobre este derecho tan importante en la era digital que vivimos hoy en día.

CONCLUSIONES

México aún cuenta con áreas de oportunidad para hacer frente a la ciberdelincuencia, comenzando por una adecuada definición y concentración de la tipificación normativa de los delitos informáticos, la coordinación de competencias entre autoridades sobre la materia, la homologación entre las diferentes normas al respecto, entre las que se encuentran la normatividad penal y en materia de protección de datos personales, la creación y actualización de estrategias de ciberseguridad y la concientización de la ciudadanía sobre la importancia de ser cibernautas responsables y resguardar su información personal.

No basta con abastecer al país con servicios tecnológicos, sino que la importancia radica en ofrecer y garantizar acceso seguro a las tecnologías de la información, previniendo cualquier afectación a la vida privada y bienes de las personas.

REFERENCIAS

Calderón Martínez, Alfredo, Coordinador (2013). El Derecho en la era digital. Internet, firma electrónica, protección de datos, delitos informáticos, comunicaciones, redes sociales, preservación de evidencia. México: Editorial Porrúa.

García Ricci, Diego (2013) Artículo 16 Constitucional Derecho a la privacidad. Instituto de Investigaciones Jurídicas de la UNAM, Recuperado el 07 de septiembre de 2019 de: https://archivos.juridicas.unam.mx/www/bjv/libros/8/3567/39.pdf

Inai. (2005). Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas. Noviembre 12, 2015, de inai Sitio web: http://inicio.ifai.org.mx/DocumentosdeInteres/Manual_Seguridad_Mipymes(Julio2015).pdf.

McKinsey & Company en colaboración con el Colegio Mexicano de Asuntos Internacionales, 2018, pág. 13 Pag. 13 consejo mexicano https://consejomexicano.org/multimedia/1528987628-817.pdf

Mendoza Enríquez, Olivia Andrea. (2018). Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento en Protection of Personal Data in Companies Established in Mexico. Revista IUS vol.12 no.41 Puebla ene./jun. 2018. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100267

Sartori, Giovanni, (2019).Homo videns La sociedad teledirigida, México, Debolsillo, Octava reimpresión.

LEGISLACIÓN

Código Penal Federal publicado en el Diario Oficial de la Federación el 14 de agosto de 1931. Última reforma publicada el 1 de julio de 2020 en el Diario Oficial de la Federación. Disponible en: http://www3.contraloriadf.gob.mx/prontuario/index.php/normativas/Template/ver_mas/67414/12/2/0

PÁGINAS ELECTRÓNICAS

Kaspersky, mapa en tiempo real https://cybermap.kaspersky.com/es
CONDUSEF https://www.condusef.gob.mx/?p=estadisticas

ESTHER ELIZABETH ALBARRÁN MARTÍNEZ. Maestrante en materia de Transparencia y Datos Personales en la Universidad de Guadalajara y Licenciada en Derecho por la UNAM.