Instituto Nacional de Transparencia, Acceso a la información y Protección de Datos Personales

RESILIENCIA CIBERNÉTICA EN EL SISTEMA FINANCIERO

Banco Mundial y el Centro de Estudios Monetarios Latinoamericanos (CEMLA)

CONTEXTO INTERNACIONAL DE CIBERSEGURIDAD

CONVENIO DE BUDAPEST

Convenio sobre la ciberdelincuencia

Consejo de Europa

2001

Único tratado internacional vinculante en la materia que constituye una especie de guía, “ley modelo” o “acuerdo marco”

CIBERSEGURIDAD EN LATINOAMÉRICA Y EL CARIBE

*De acuerdo con el Reporte “Estado de la Ciberseguridad en el Sector Bancario en América Latina y El Caribe”, revela los siguientes datos en 2018:

- ✓ al menos 9 de cada 10 entidades bancarias sufrieron incidentes cibernéticos en el último año.
- ✓ el 37% de los bancos de la Región fueron víctimas de ataques que resultaron efectivos.
- ✓ el 39% de los incidentes no son reportados, dato que en el caso de las entidades bancarias de mayor tamaño baja hasta el 19%.
- ✓ 6 de cada 10 usuarios que no utilizan servicios de banca digitales lo hace por desconfianza sobre la seguridad de las transacciones.

*Disponible en: http://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

inai
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

CIBERSEGURIDAD EN CONTEXTO

Se estima que el costo total anual de respuesta y de recuperación ante incidentes de seguridad digital de las entidades bancarias de la región América Latina para 2017 fue de USD$ 809 millones aproximadamente.

México ocupa el segundo lugar en América Latina en vulnerabilidad a ciberataques relacionados con piratería informática, robo de identidad y fraude en tarjetas de crédito, de acuerdo con la consultora de información estratégica LexisNexis Risk Solutions.

El estudio también revela que 49% de pérdidas por fraude en México proviene del robo de identidad, y 45% anual por medio de transacciones de crédito, seguido de 31% por medio de gestiones de débito.

CIBERSEGURIDAD EN MÉXICO

El Poder Ejecutivo, en el marco de la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE), acordó, por unanimidad, la creación de la Subcomisión de Ciberseguridad en octubre de 2017, la cual está presidida por la Secretaría de Gobernación a través de la entonces denominada Comisión Nacional de Seguridad (CNS). Entre otras tareas, la Subcomisión de Ciberseguridad se encargará de dar seguimiento y coordinar la implementación de la Estrategia Nacional de Ciberseguridad (ENC).

La ENC establece 8 ejes transversales:

1. Cultura de ciberseguridad
2. Desarrollo de capacidades
3. Coordinación y colaboración
4. Investigación, desarrollo e innovación en TIC
5. Estándares y criterios técnicos
6. Infraestructuras críticas
7. Marco jurídico y autorregulación
8. Medición y seguimiento.

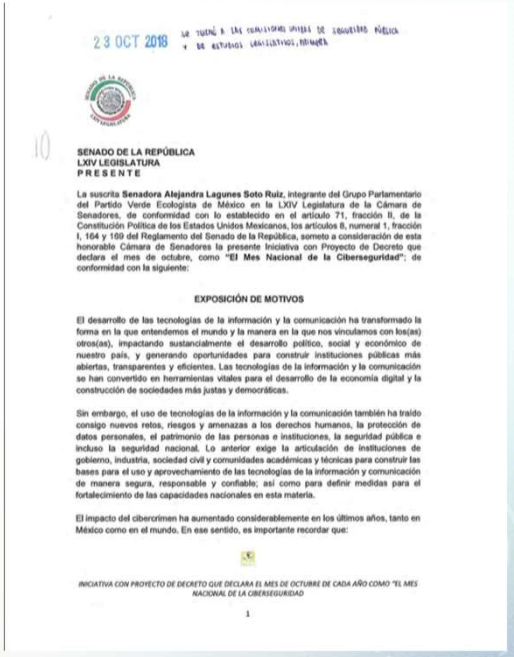
CIBERSEGURIDAD EN MÉXICO

Senado de la República - Iniciativa con proyecto de decreto. Octubre 2018.

En 2019…

- El Senado de la República aprobó declarar la primera semana del mes de octubre, como la “Semana Nacional de la Ciberseguridad".

Con el propósito de concientizar a la ciudadanía sobre los riesgos del uso del ciberespacio y la cultura de la prevención ante el avance y alcance de las tecnologías de la información y comunicación (TIC), y para brindar mayor protección y seguridad a los usuarios de los aparatos cibernéticos.



23 OCT 2018

SENADO DE LA REPÚBLICA
LXIV LEGISLATURA
PRESENTE

La suscrita **Senadora Alejandra Lagunes Soto Ruiz**, integrante del Grupo Parlamentario del Partido Verde Ecologista de México en la LXIV Legislatura de la Cámara de Senadores, de conformidad con lo establecido en el artículo 71, fracción II, de la Constitución Política de los Estados Unidos Mexicanos, los artículos 8, numeral 1, fracción I, 164 y 169 del Reglamento del Senado de la República, someto a consideración de esta honorable Cámara de Senadores la presente Iniciativa con Proyecto de Decreto que declara el mes de octubre, como **"El Mes Nacional de la Ciberseguridad"**; de conformidad con la siguiente:

EXPOSICIÓN DE MOTIVOS

El desarrollo de las tecnologías de la información y la comunicación ha transformado la forma en la que entendemos el mundo y la manera en la que nos vinculamos con los(as) otros(as), impactando sustancialmente el desarrollo político, social y económico de nuestro país, y generando oportunidades para construir instituciones públicas más abiertas, transparentes y eficientes. Las tecnologías de la información y la comunicación se han convertido en herramientas vitales para el desarrollo de la economía digital y la construcción de sociedades más justas y democráticas.

Sin embargo, el uso de tecnologías de la información y la comunicación también ha traído consigo nuevos retos, riesgos y amenazas a los derechos humanos, la protección de datos personales, el patrimonio de las personas e instituciones, la seguridad pública e incluso la seguridad nacional. Lo anterior exige la articulación de instituciones de gobierno, industria, sociedad civil y comunidades académicas y técnicas para construir las bases para el uso y aprovechamiento de las tecnologías de la información y comunicación de manera segura, responsable y confiable; así como para definir medidas para el fortalecimiento de las capacidades nacionales en esta materia.

El impacto del cibercrimen ha aumentado considerablemente en los últimos años, tanto en México como en el mundo. En ese sentido, es importante recordar que:

INICIATIVA CON PROYECTO DE DECRETO QUE DECLARA EL MES DE OCTUBRE DE CADA AÑO COMO "EL MES NACIONAL DE LA CIBERSEGURIDAD

1

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

CIFRAS EN MÉXICO

México cuenta con 74.3 millones de usuarios de Internet de seis años o más, que representan el 65.8% de la población en ese rango de edad. Se observa un crecimiento de 4.2 puntos porcentuales respecto a lo reportado en 2017, cuando se registraron 71.3 millones de usuarios.

*Se estima que el costo total anual de respuesta y de recuperación ante incidentes de seguridad digital de las entidades e instituciones financieras en México en 2018 fue de USD$ 107 millones aproximadamente.

CONDUSEF

Señala que durante el primer trimestre de 2019, las quejas por fraudes cibernéticos crecieron 35% respecto de 2018.

	2015	2016	2017	2018	2019	VAR. (2019 vs 2018)
TOTALES	1,683,661	2,674,023	3,345,664	3,515,712	4,318,853	
CIBERNÉTICOS	304,256	836,532	1,578,000	2,074,554	2,807,819	35%
	18%	31%	47%	59%	65%	-
TRADICIONALES	1,379,287	1,835,409	1,762,805	1,441,115	1,511,022	5%
	82%	69%	53%	41%	35%	-
Por definir	118	2,082	4,859	43	12	-

CIFRAS EN MÉXICO

El monto reclamado de los fraudes cibernéticos ascendió a $5908 mdp; se bonifico sólo el 42% y 87 de cada 100 fraudes cibernéticos se resolvieron a favor del usuario.

En el primer semestre de 2019, los RI (Robo de Identidad) cibernéticos aumentaron 217% respecto del mismo periodo del 2018.

Primer semestre 2019	Reclamaciones Iniciadas	Monto Reclamado (mdp)	Monto Reclamado Concluido (mdp)	Monto Abonado (mdp)	% de abono	% de resolución Favorable
TOTAL DE FRAUDES	**4,318,853**	**$11,689**	**$10,363**	**$4,344**	**42**	**78**
Comercio por Internet	2,679,492	$2,761	$2,490	$2,007	81	91
Banca Móvil	95,648	$1,181	$1,051	$123	12	9
Operaciones por Internet P. Físicas	30,816	$1,770	$1,627	$106	6	16
Operaciones por Internet P. Morales	1,754	$193	$175	$16	9	16
Pagos por Celular	109	$1	$1	$0	2	1
SUBTOTAL CIBERNÉTICO	**2,807,819**	**$5,908**	**$5,344**	**$2,252**	**42**	**87**
Terminal Punto de Venta	845,592	$2,079	$1,788	$737	41	54
Comercio por Teléfono	449,598	$546	$428	$334	78	90
Cajeros Automáticos	170,183	$544	$473	$112	24	22
Sucursales	44,009	$2,506	$2,234	$868	39	33
Otros Bancos	645	$65	$64	$30	46	50
Movimiento generado por el Banco	544	$25	$18	$4	25	30
Banca por Teléfono	284	15	$12	$8	61	40
Corresponsales	167	$0	$0	$0	37	20
SUBTOTAL TRADICIONAL	**1,511,022**	**$5,780**	**$5,019**	**$2,092**	**42**	**60**
Por Definir	12	$1	$0	$0	56	86

	2015	2016	2017	2018	2019	VAR. (2019 Vs 2018)
TOTALES	**50,911**	**32,719**	**39,775**	**33,136**	**40,928**	
CIBERNÉTICOS	**982**	**768**	**2,960**	**1,180**	**3,737**	**217%**
	1.9%	**2.3%**	**7.4%**	**3.6%**	**9.1%**	-
TRADICIONALES	**49,811**	**31,786**	**36,395**	**31,956**	**37,179**	**16%**
	97.8%	**97.1%**	**91.5%**	**96.4%**	**90.8%**	-
Por definir	118	165	420	-	12	-

De las Reclamaciones de Posible Robo de Identidad en 2019:

Enero – Junio 2019	Reclamaciones	$Monto Reclamado (mdp)	$Monto Reclamado Concluido (mdp)	$Monto Abonado (mdp)	% de abono	% de resolución Favorable
TOTAL DE FRAUDES	**40,928**	**$2,216.1**	**$2,042.7**	**$831.1**	**41**	**44**
Banca Móvil	2,270	$144.8	$123.9	$15.8	13	11
Comercio por Internet	959	$2.3	$1.9	$1.3	69	75
Operaciones por Internet P. Físicas	504	$102.9	$99.5	$33.9	34	31
Operaciones por Internet P.Morales	4	$1.4	$1.4	$1.4	100	100
SUBTOTAL CIBERNÉTICO	**3,737**	**$251.3**	**$226.7**	**$52.4**	**23**	**31**
Sucursales	28,307	$1,816.9	$1,678.5	$688.9	41	41
Terminal Punto de Venta	7,031	$80.9	$77.3	$54.0	70	61
Cajeros Automáticos	956	$43.0	$40.3	$26.5	66	78
Movimiento generado por el Banco	382	$11.5	$9.1	$2.3	25	36
Comercio por Teléfono	209	$0.7	$0.7	$0.3	37	14
Corresponsales	166	$0.4	$0.4	$0.2	37	21
Banca por Teléfono	128	$10.5	$9.6	$6.5	67	62
SUBTOTAL TRADICIONAL	**37,179**	**$1,964.1**	**$1,815.9**	**$778.6**	**43**	**45**
Por Definir	12	$0.7	$0.1	$0.0	56	86

inai
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

CIBERSEGURIDAD EN EL SISTEMA FINANCIERO MEXICANO [OEA/2019*]

Gráfica 14. Procesos / programas respecto a la seguridad digital implementados actualmente por las entidades e instituciones financieras

Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

FUENTE: http://www.oas.org/es/sms/cicte/documents/informes/Estado-de-la-Ciberseguridad-en-el-Sistema-Financiero-Mexicano.pdf

inai
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Protección de Datos Personales y Ciberseguridad en México

De acuerdo con la LFPDPPP, se debe abordar los principios y deberes de seguridad para las finalidades determinadas, además de ser correctos y actualizados y sujetos a tratamiento mientras sea necesario para la finalidad para la que se recabaron, pero no más allá.

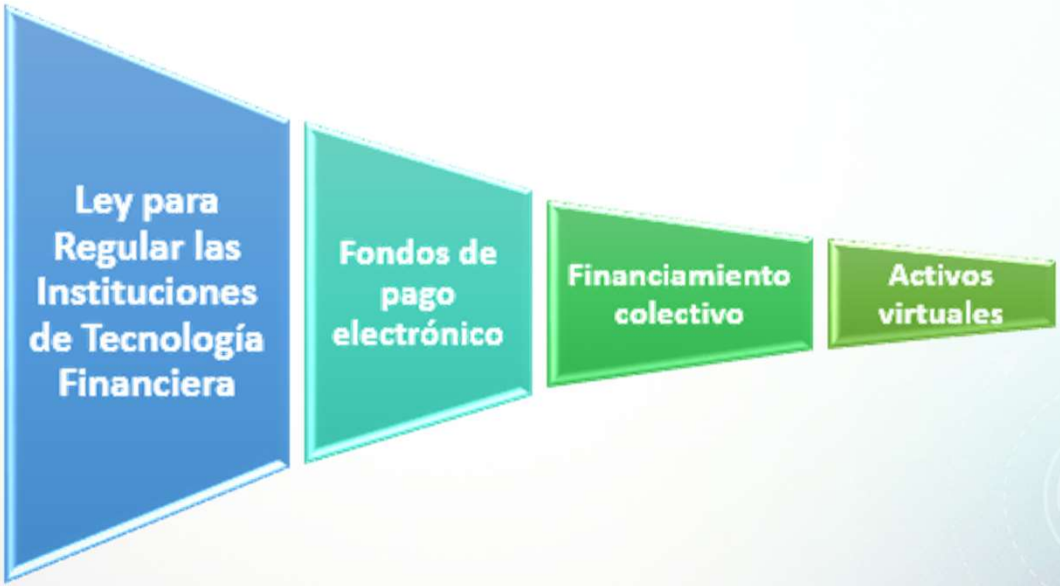
La ciberseguridad busca mejorar la calidad, el control y la privacidad de la información personal. Nunca hay un riesgo cero en esta materia, la llegada de los ciberataques solo es cuestión de tiempo, como consecuencia de la adaptación tecnológica en casi todos las actividades del ser humano.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

LEGISLACIÓN FINTECH

FINTECH
MÉXICO

Marzo de 2018



OPEN BANKING

Ley para Regular las Instituciones de Tecnología Financiera (Ley Fintech)

En México, el 9 de marzo de 2018, fue publicada la Ley para Regular las Instituciones de Tecnología Financiera, mejor conocida como Ley Fintech.

Artículo 76.

- ✓ Establece la obligación de implementar interfaces de programación de aplicaciones informáticas estandarizadas (API) para posibilitar la conectividad y acceso de otras interfaces desarrolladas o administradas por las entidades establecidas en la ley y terceros especializados en tecnologías de la información.
- ✓ Incluye los datos financieros, agregados y transaccionales como aquellos que serán compartidos en el esquema de open banking.
- ✓ Instituye como base legal para el uso de estos datos, la autorización de los clientes.
- ✓ Brinda la posibilidad de que los titulares retiren su consentimiento dado siempre que haya vulnerabilidades que pongan en riesgo la información de sus clientes o el tercero incumpla con los términos y condiciones pactados para el intercambio de información.

TRATAMIENTO DE DATOS PERSONALES EN EL SECTOR FINANCIERO

Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento

- Todo tratamiento de datos personales estará sujeto al consentimiento de su titular.
- En el tratamiento de datos patrimoniales y financieros, se requerirá el consentimiento expreso.
- Consentimiento escrito mediante mecanismos convencionales y digitales

ACTIVOS VIRTUALES Y SUS RIESGOS

Activos Virtuales:

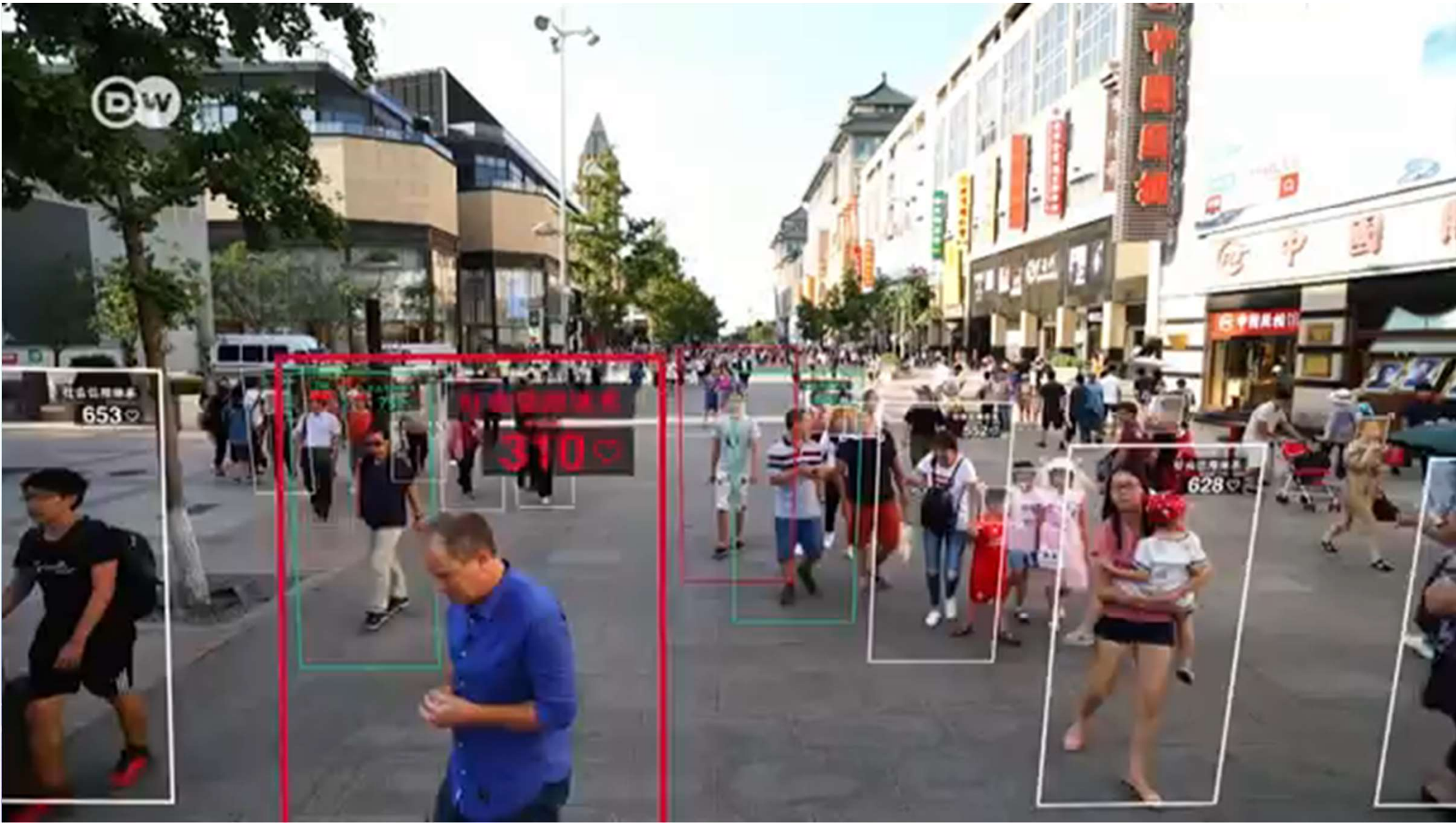
Representación de valor registrada electrónicamente y utilizada entre el público como medio de pago para todo tipo de actos jurídicos y cuya transferencia únicamente puede llevarse a cabo a través de medios electrónicos.

La **volatilidad** es uno de los riesgos del uso de criptomonedas debido a que las grandes fluctuaciones de los precios pueden traer pérdidas de miles de dólares.

A pesar del valor que se le asigna pese a su popularidad, aún hay **incertidumbre** sobre su futuro.

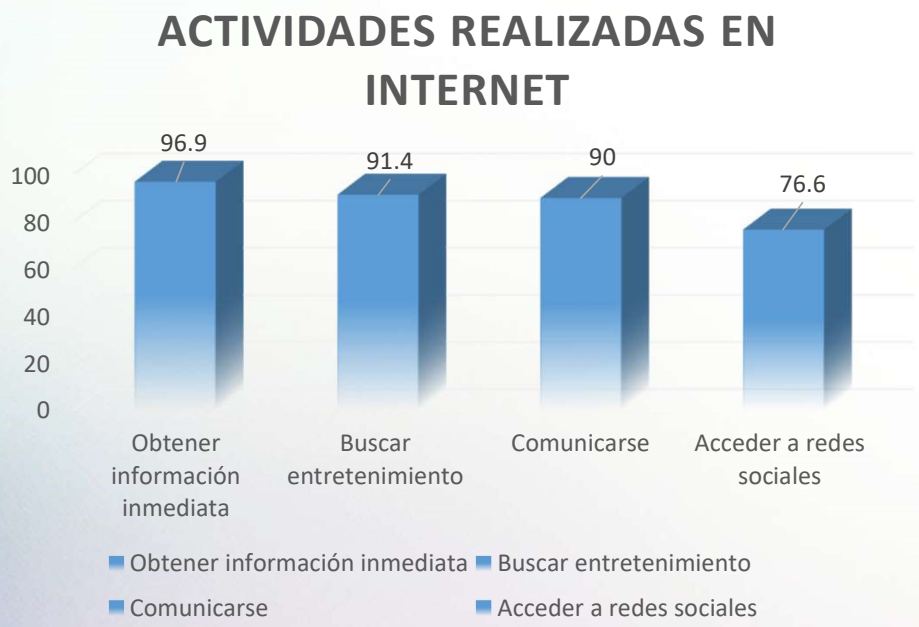
No hay forma de **proteger el fallo de la persona**, el fallo técnico o el fraude. Es decir, no hay un sistema implantado para compensar las pérdidas.

De momento, las criptomonedas están libres de carga sobre la **regulación**, pero si empiezan a regularse, muchas divisas tradicionales podrían verse afectadas.


653
310
628

SERVICIOS DIGITALES FINANCIEROS

En México existen 71.3 millones de usuarios activos que se conectan regularmente a Internet.



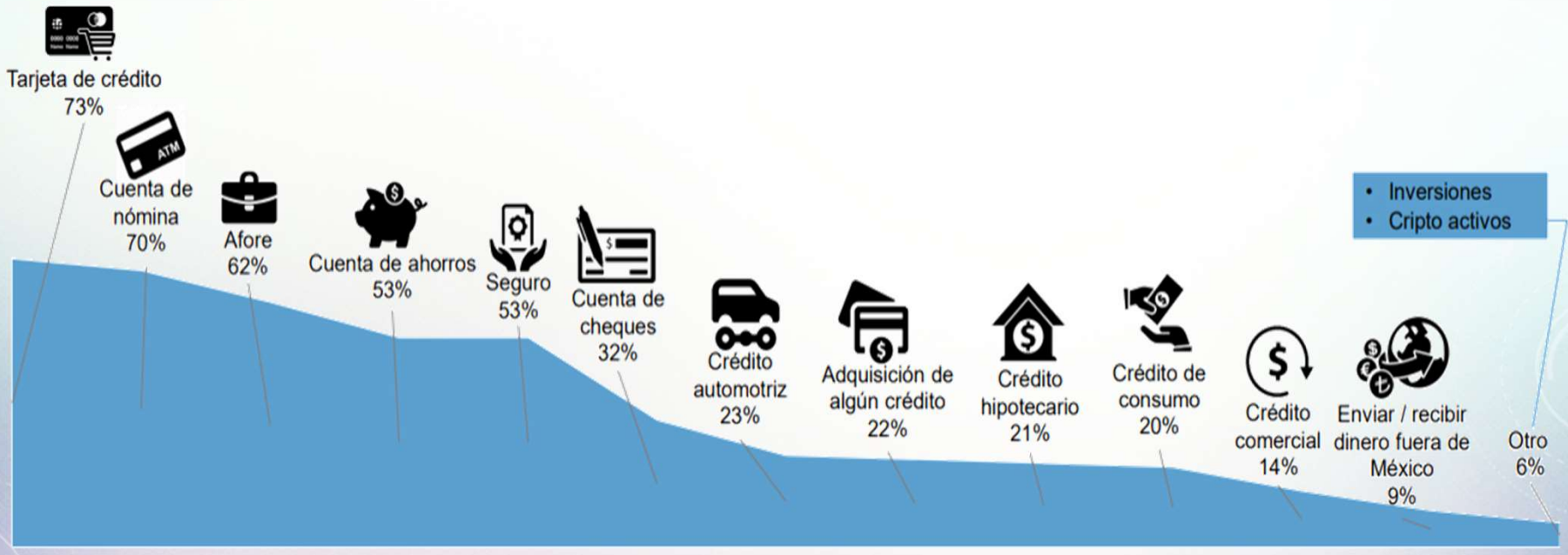
El número de usuarios con servicio de telefonía celular es de 80.7 millones.

Del 73.5% de la población de seis años o más, ocho de cada diez se conectan a Internet desde un celular inteligente (smartphone).

Fuente ENDITH 2018:https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2019/OtrTemEcon/ENDUTIH_2018.pdf

SERVICIOS DIGITALES FINANCIEROS

De acuerdo al *Estudio sobre los Servicios Financieros de los Usuarios de Internet en México 2019,* el **75% de usuarios de Internet poseen algún servicio financiero**.



Fuente ESFU 2019: https://www.asociaciondeinternet.mx/es/component/remository/Banca-por-Internet/Estudio-sobre-los-Servicios-Financieros-de-los-Usuarios-de-Internet-en-Mexico-2019/lang,es-es/?Itemid=

PLATAFORMAS TIPO CODI

CoDi® es una plataforma desarrollada por Banco de México para facilitar las transacciones de pago y cobro a través de transferencias electrónicas, de forma rápida, segura y eficiente, a través de teléfonos móviles.

CoDi® usa la tecnología de los códigos QR y NFC, para facilitar que tanto comercios como usuarios, puedan realizar transacciones sin dinero en efectivo.

VENTAJAS

- Formalizar las actividades de comercio.
- Velocidad de transacciones.
- No hay comisiones adicionales.
- Mayor control de las finanzas personales.
- Baja probabilidad de fraude.
- Reducir la producción de moneda en efectivo.

PLATAFORMAS TIPO CODI – POSIBLES RIESGOS

Código malicioso insertado en un código QR	Hay un riesgo latente acerca de la creación de códigos QR malintencionados, la ejecución de estos surge cuando una persona escanea códigos de este tipo desde la cámara de su celular cada vez que se encuentra uno en la calle.
Amenazas de Ciberseguridad	La información de las transacciones se manda vía Internet, con lo cual se está expuesto al filtrado de datos personales o ataques de malintencionados u otras amenazas presentes en el ciberespacio.
Problemática con el acceso a una cuenta bancaria	En México el acceso a una cuenta bancaria aun es complejo, el 32% de la población de 18 a 70 años no cuenta con algún producto financiero.
Fallas Operativas	Otra gran inquietud es la posibilidad de enfrentar fallas eléctricas o del servidor. Con lo cual la plataforma quedaría inhabilitada por un tiempo indefinido y sería imposible realizar transacciones en ese lapso.
Catástrofes	En que ocurra un desastre natural y este afecte a los servidores de la plataforma, los usuarios no podrán realizar ningún tipo de transacción.
Brecha Generacional	Es necesario tener en cuenta que el uso de las tecnologías para sectores de la población adulta mayor o grupos poblacionales vulnerables, en zonas rurales o con poco acceso a Internet se verá limitado
Posibles ataques en el futuro	Al ser una tecnología emergente, su seguridad es la óptima actualmente, pero en el futuro cuando la plataforma sea más utilizada por un mayor número de usuarios, la probabilidad de que haya ataques a la seguridad puede aumentar.

PLATAFORMAS TIPO CODI – RECOMENDACIONES

a) Analizar las actividades realizadas con el dispositivo móvil.
b) Se recomienda no descargar programas de tiendas no oficiales, debido a que todas las aplicaciones sin importar la institución financiera se encuentran disponibles en las tiendas oficiales para sistemas operativos Android e iOS.
c) Antes de realizar alguna transacción es recomendable instalar un antivirus en el dispositivo que se utilizará.
d) Utilizar contraseñas robustas, que tengan una combinación de caracteres en mayúsculas y minúsculas, números y caracteres especiales.
e) Habilita el doble factor de autenticación en las apps que esté disponible.
f) Existen varias aplicaciones que validan si un código QR es auténtico y puede utilizarse antes de realizar la transacción a través de CoDi.
g) Activar las notificaciones que ofrece la plataforma para poder estar al tanto de los movimientos bancarios que se realizaron.
h) Limita el valor de tus transacciones de pagos.

GRACIAS

Mtro. Jonathan Mendoza Iserte

@JonnhyMendoza

Secretario de Protección de Datos Personales

Instituto Nacional de Transparencia, Acceso a la información y Protección de Datos Personales