RECLAMACIONES IMPUTABLES A UN POSIBLE FRAUDE

2011-2017 (primer trimestre)

Con base en las reclamaciones con impacto monetario presentadas por los clientes de la Banca en México

Elaborado por CONDUSEF a partir de información de la CNBV

SHCP
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

CONDUSEF
Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros

Julio, 2017

ANTECEDENTES A NIVEL MUNDIAL

80 millones

REDES SOCIALES

De **Perfiles Falsos** en Facebook, Twitter e Instagram*

1,590 millones de usuarios activos

(*) Fuente: El Pulso del cibercrimen 2016 EASY SOLUTIONS

4 de 5 USUARIOS DE GOOGLE

CONTAMINACIÓN DE ANUNCIOS EN MOTORES DE BUSQUEDA

Usan los resultados de Adwords*

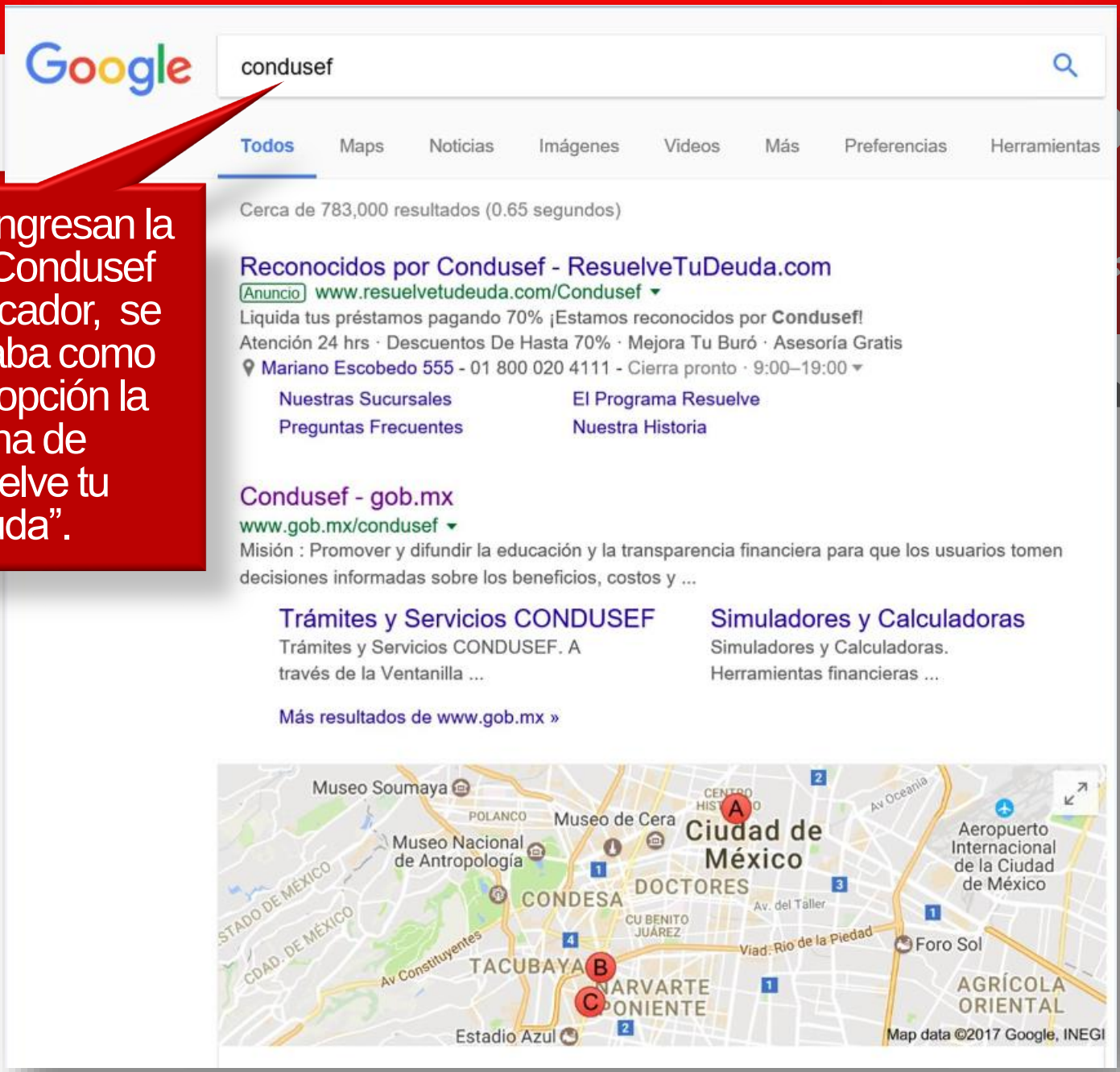
Los cibercriminales están aprovechando los avisos pagados en buscadores para dirigir los usuarios a sitios de phishing.

Ejemplo Condusef

(*) Fuente: El Pulso del cibercrimen 2016 EASY SOLUTIONS

4d

Cuando ingresan la palabra Condusef en el buscador, se desplegaba como primera opción la página de "Resuelve tu Deuda".



(*) Fuente: El Pulso del cibercrimen 2016 EASY SOLUTIONS

3.3 MILLONES

APLICACIONES MÓVILES FALSAS

Aplicaciones de **Android** fueron clasificadas como **malware***

Las tiendas de aplicaciones no oficiales carecen de fuertes controles de seguridad y hay millones de aplicaciones falsas que pueden robar credenciales e instalar malware.

(*) Fuente: El Pulso del cibercrimen 2016 EASY SOLUTIONS

127%
Ha crecido

RANSOMWARE
ha sido el incremento de los ataques de ransomware durante el último año*

Los cibercriminales infiltran los sistemas de una organización o de una persona para tomar datos sensibles como "rehenes" hasta que se les pague un rescate. **El rescate debe ser pagado en una moneda específica: los bitcoins.**

(*) Fuente: El Pulso del cibercrimen 2016 EASY SOLUTIONS

689 MILLONES DE USUARIOS

USUARIOS AFECTADOS (21 países)

Afectados por el cibercrimen en el último año*

(Existen 3 mil millones de internautas en el mundo)

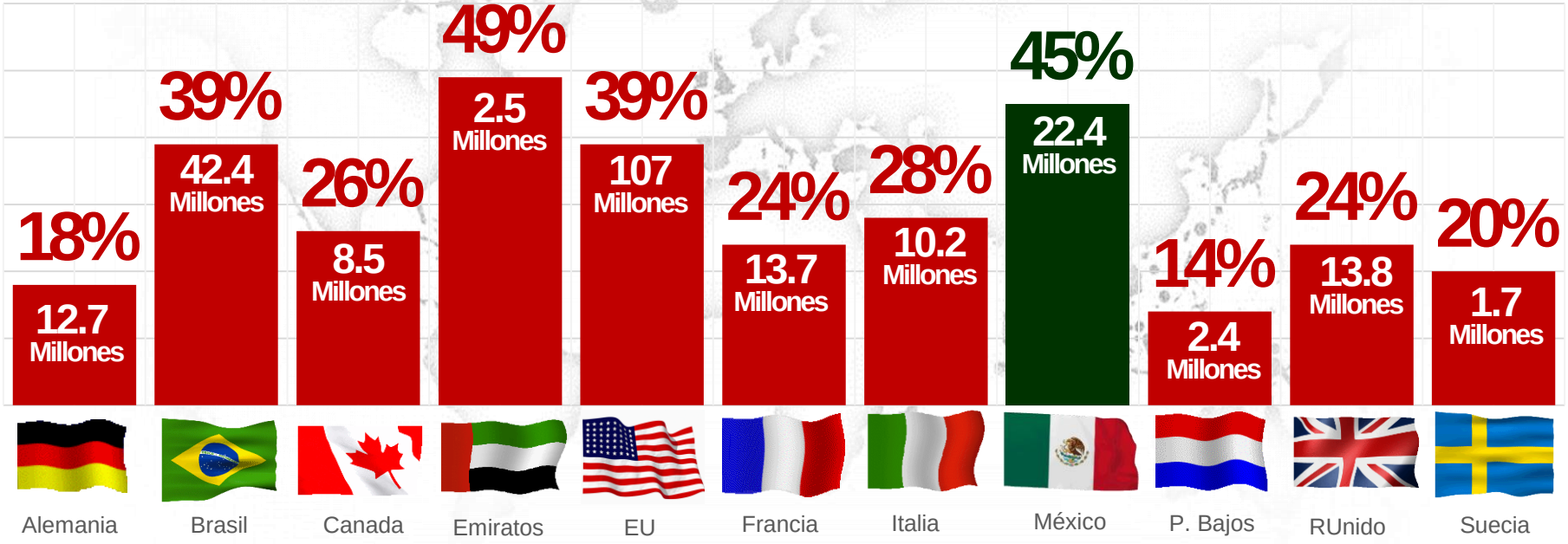
(*) Informe de Norton sobre ciberseguridad 2016

689 MILLONES DE USUARIOS

PORCENTAJE DE AFECTADOS
Comparativo 11 países

Usuarios afectados *VS* **Usuarios internautas**

En 2016, el 45% de los internautas de México fueron afectados por el cibercrimen.



(*) Informe de Norton sobre ciberseguridad 2016

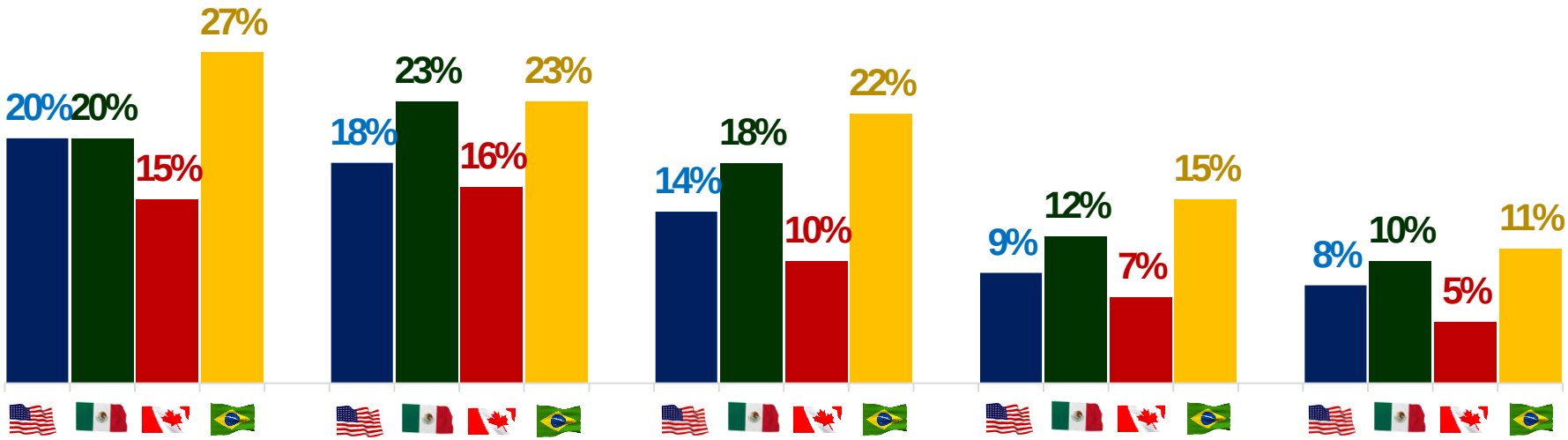
Evolución del fraude

A nivel mundial

	1980	1990	2000	2010	2015
Criminales	Operaban de manera **Individual**	**Equipos** de criminales en ciertos países.	**Redes de crimen local** en ciertos países	**Redes de crimen global hackers**	**Redes de crimen global con organizaciones descentralizadas y hackers**
Blanco Objetivo	Consumidores	Pequeños comerciantes	Grandes comerciantes	Procesadores de la banca	Toda la Industria del pago
Principal tipo de fraude	Plásticos extraviados, robados o interceptados (TDC y TDD).	Falsificación / clonación.	Falsificación / clonación. Phishing, robo de datos financieros en la basura.	Falsificación / clonación. Skymmer Phishing, robo de datos financieros en la basura, alteración de cajeros, robo de identidad.	Falsificación / clonación. Skymmer Phishing, robo de datos en la basura, alteración de cajeros, robo de identidad. Pharming, Hacking
Tecnología	**APARECE:** • En 1969 la TDC • En 1970 la TPV • En 1972 el ATM • En 1980 la TDD	En 1988 aparece la Banca Por Teléfono	En 1999 aparece la Banca Por Internet	En 2011 aparece la Banca Móvil	Auge del Comercio Electrónico, Pagos por Celular, Dinero móvil, moneda virtual y Fintech

Comportamiento de las personas:

Las personas deben fortalecer sus acciones de prevención, lo que constituye una forma de protegerse a sí mismos.



No bloquear el teléfono inteligente al dejar de usarlo

Tirar a la basura papeles o Documentos con números de cuentas

Usar la banca en línea o comprar en Internet sin un software de seguridad o en café internet

Anotar el PIN y llevarlo consigo o guardarlo junto con la tarjeta

Responder e-mails o llamadas telefónicas y proporcionar datos de cuentas bancarias

(*) Fuente: Estudio de ACI Worldwide 2016

RECLAMACIONES IMPUTABLES A UN POSIBLE FRAUDE

MÉXICO

Reclamaciones imputables a un posible fraude

- Robo o extravío del plástico
- Clonación de la banda magnética
- Compras remotas (ventas por teléfono e internet)
- Transferencias electrónicas no reconocidas
- Robo de identidad o falsificación de datos personales
- Prácticas engañosas para obtener datos en cajeros automáticos.

22.2 millones

CIFRAS ACUMULADAS

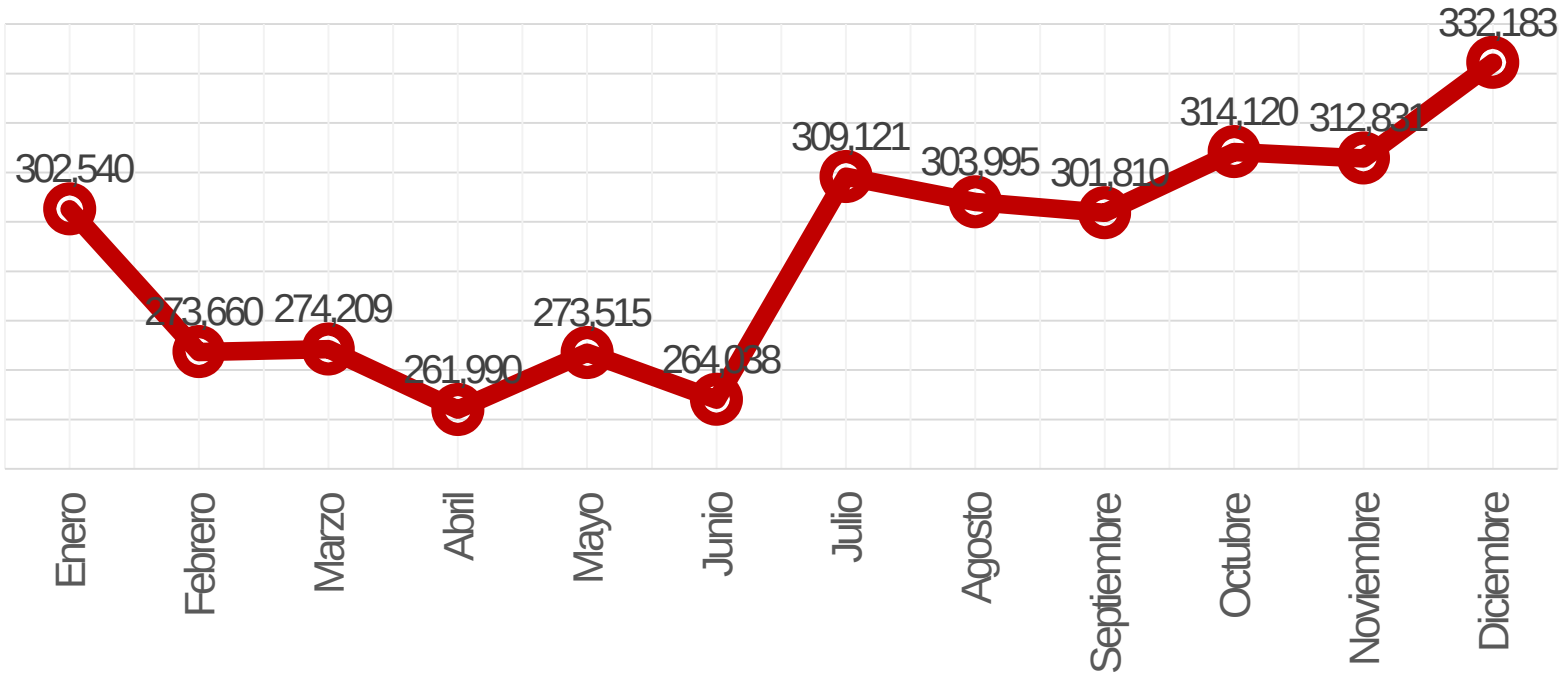
Reclamaciones imputables a un posible fraude
Desde el año 2011 al primer trimestre de 2017

22.2 millones

¿Cuándo se originaron los Fraudes?

Con base en la FECHA DE SUCESO, se obtuvo el mes con mayor incidencia de fraudes.

En promedio, **DICIEMBRE** es el mes con mayor número de fraudes originados.

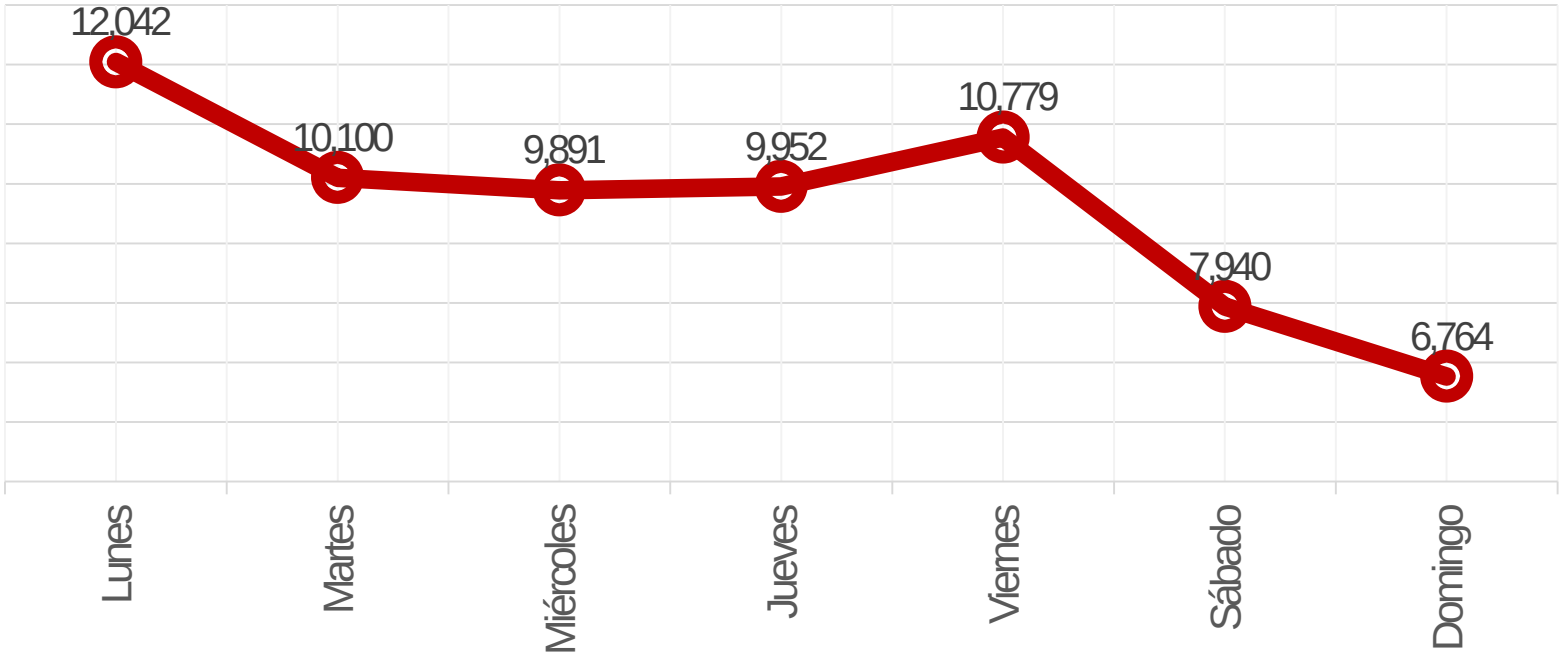


22.2 millones

¿Cuándo se originaron los Fraudes?

Con base en la FECHA DE SUCESO, se obtuvo el día de la semana con mayor incidencia de fraude.

En promedio, **LOS LUNES** es el día con mayor número de fraudes originados.

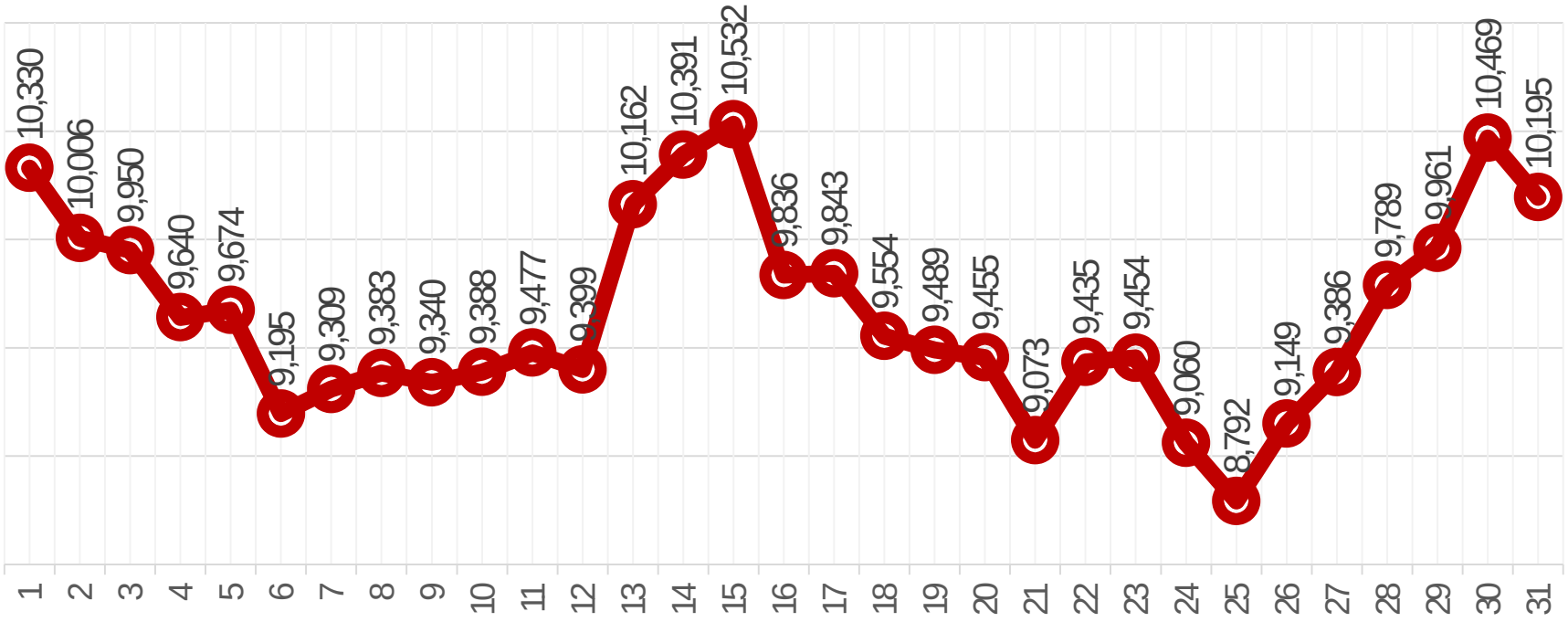


22.2 millones

¿Cuándo se originaron los Fraudes?

Con base en la FECHA DE SUCESO, se obtuvo el día del mes con mayor incidencia de fraude.

En promedio, **LOS DÍAS 15 Y 30** son los días con mayor número de fraudes originados.

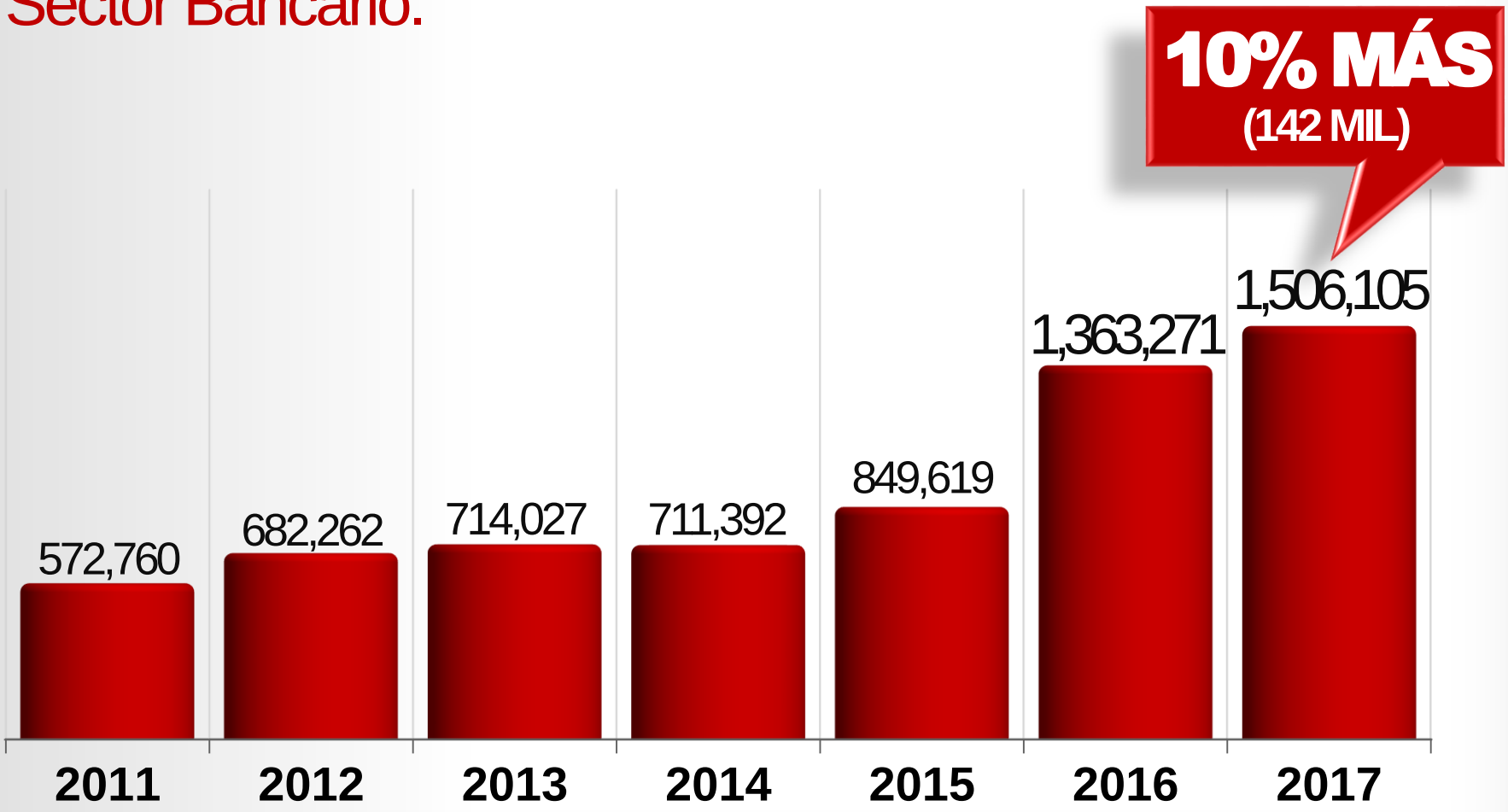


RECLAMACIONES FRAUDES

Primer trimestre 2011-2017

En el T1-2017, se registraron **1.5 MILLONES**.

- Prácticamente 18 mil reclamaciones por día al Sector Bancario.



Reclamaciones Fraudes por Banco

El **28% de las reclamaciones de fraude son de Bancomer**, CitiBanamex 22% y Santander 19%.

27 de 31 Bancos registran incrementos.

BANCO	Cifras enero-marzo			
	2016	2017	P(%)	VAR (%)
BBVA Bancomer	316,135	424,263	28.2	34
CitiBanamex	296,885	333,204	22.1	12
Banco Santander	217,655	292,346	19.4	34
Banorte IXE	75,909	145,670	9.7	92
Banco Inbursa	44,413	83,821	5.6	89
HSBC México	48,640	59,241	3.9	22
Banco Azteca	264,089	56,499	3.8	-79
Scotiabank Inverlat	22,490	43,386	2.9	93
American Express	20,737	22,753	1.5	10
BanCoppel	37,752	21,819	1.4	-42
Banco Invex	7,368	7,202	0.5	-2
Banca Afirme	2,936	4,962	0.3	69
Banregio	2,844	4,194	0.3	47
Banco del Bajío	2,986	3,083	0.2	3
Banco Ahorro Famsa	1,149	1,329	0.1	16
Banco Monex	26	743	0.0	2758
Consubanco	114	398	0.0	249
Cibanco	145	251	0.0	73
Banca Mifel	120	249	0.0	108
Banco Multiva	695	232	0.0	-67
Banco Compartamos	62	163	0.0	163
Intercam Banco	33	130	0.0	294
Bansi	22	53	0.0	141
Bankaool	14	41	0.0	193
Banco Autofin	23	27	0.0	17
Banco Actinver	8	17	0.0	113
Banco Ve Por Más	-	11	0.0	-
Fundación Dondé	11	8	0.0	-27
Volkswagen Bank	6	7	0.0	17
Interacciones	1	2	0.0	100
Investa Bank	-	1	0.0	-
Total	**1,363,271**	**1,506,105**	**100.0**	**10**

Afectación monetaria a los Usuarios y resolución

RECLAMACIONES FRAUDES

Monto reclamado, abonado y resolución

En el primer trimestre de 2017, los usuarios reclamaron $3,244 millones de pesos.

- Únicamente se abonó el 53%
- 8 de cada 10 asuntos se resuelven a favor del usuario.

	2016 T1	2017 T1
Posible Fraude	**1,363,271**	**1,506,105**
$ Monto Reclamado Total (mdp)	**$3,072**	**$3,244**
$ Monto Reclamado asuntos concluidos (mdp)	**$3,068**	**$2,671**
$ Monto Abonado (mdp)	**$1,596**	**$1,424**
% de abono	**52%**	**53%**
% de resolución Favorable	**82%**	**82%**

RECLAMACIONES FRAUDES

Monto reclamado y abonado 2017 T1

El Banco que más bonifica a los usuarios es Banorte IXE con el 85.6%. El que menos abona es Banco Azteca (33%).

	Reclamación (Número)	Monto reclamado (mdp)		Monto abonado* (mdp)	Abono (%)
		TOTAL	CONCLUIDO		
	1,506,105	**$3,244.2**	**$2,670.9**	**$1,423.5**	**53.3%**
BBVA Bancomer	424,263	1,058.4	964.6	357.1	37.0
CitiBanamex	333,204	758.6	639.2	363.4	56.8
Banco Santander	292,346	510.5	326.4	198.7	60.9
Banorte IXE	145,670	262.6	230.5	197.3	85.6
Banco Inbursa	83,821	159.3	116.2	71.0	61.1
HSBC México	59,241	205.1	190.3	139.5	73.3
Banco Azteca	56,499	40.0	37.1	12.5	33.8
Scotiabank Inverlat	43,386	130.0	86.5	33.7	38.9
American Express	22,753	44.7	27.0	21.7	80.3
BanCoppel	21,819	23.5	17.5	11.7	66.9
Otros	23,103	51.5	35.6	16.8	

Mutación del fraude

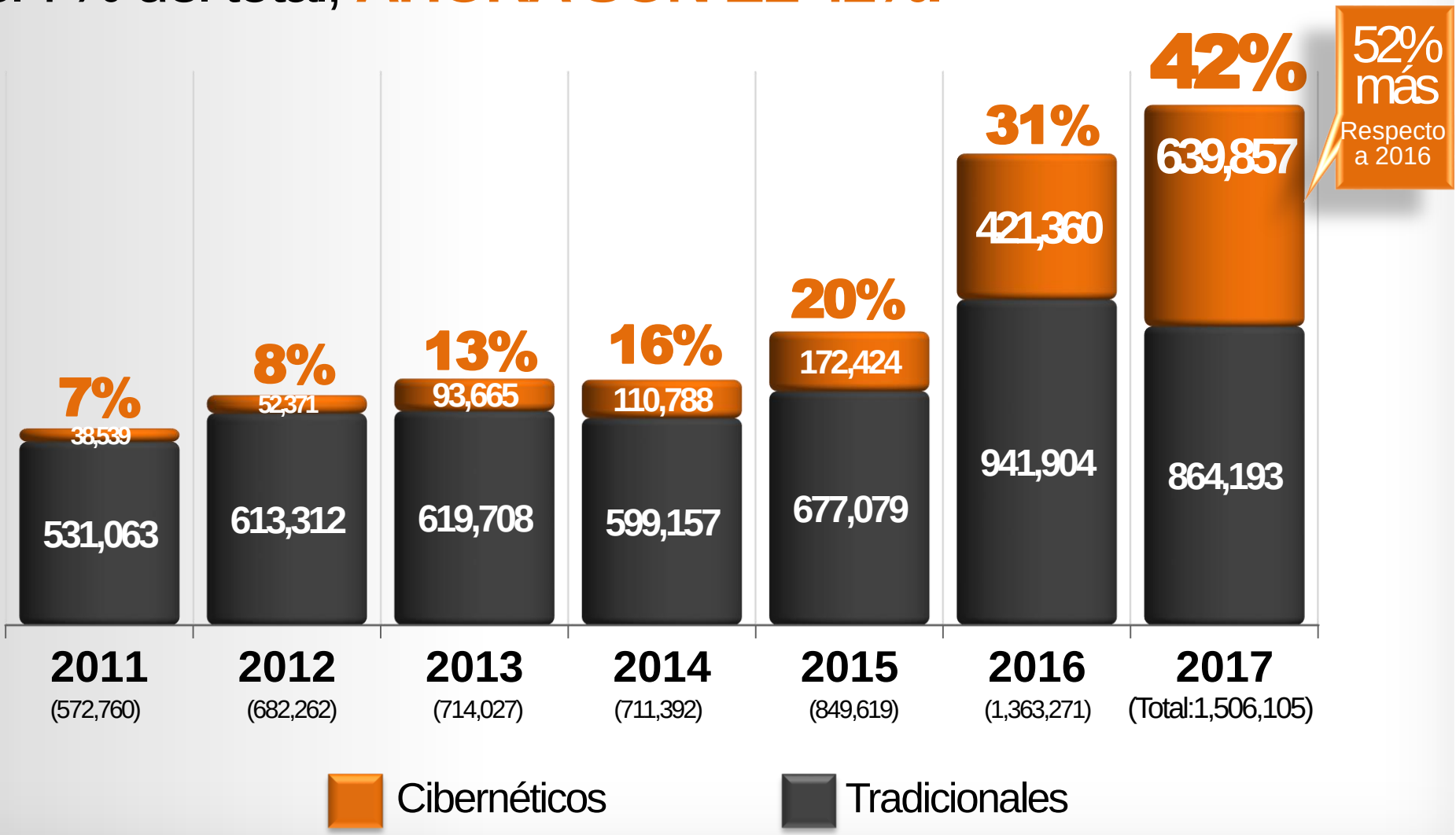
Tradicional

Cibernético

RECLAMACIONES FRAUDES

Primer trimestre 2011-2017

Antes, los **FRAUDES CIBERNÉTICOS** representaban el 7% del total, **AHORA SON EL 42%.**



FRAUDES CIBERNÉTICOS

Monto reclamado, abonado y resolución

En el T12017, los usuarios reclamaron por fraudes cibernéticos $1,167 millones de pesos.

- En este tipo de quejas se abona el 53%
- 9 de cada 10 asuntos se resuelven a favor del usuario.

	2016 T1	2017 T1
Fraude cibernético	**421,360**	**639,857**
$ Monto Reclamado Total (mdp)	**$894**	**$1,167**
$ Monto Reclamado asuntos concluidos (mdp)	**$893**	**$994**
$ Monto Abonado (mdp)	**$392**	**$523**
% de abono	**44%**	**53%**
% de resolución Favorable	**90%**	**90%**

FRAUDES CIBERNÉTICOS

Monto reclamado y abonado 2017 T1

4 Bancos concentran casi el 90%. CitiBanamex con mayor número de fraudes cibernéticos (28%).

	Reclamos (número)	Part. %	Monto reclamado (mdp)	Monto abonado* (mdp)	Abono (%)	Fav (%)
	639,857	**100**	**$1,167**	**$523**	**53**	**90**
CitiBanamex	177,516	28	378.9	167.1	51	93
Banco Santander	140,285	22	217.3	80.9	60	89
BBVA Bancomer	124,254	19	371.0	122.3	35	84
Banorte IXE	118,822	19	102.8	97.6	97	99
Banco Inbursa	19,769	3	15.1	8.2	69	83
Banco Azteca	18,325	3	10.0	5.1	54	72
American Express	12,877	2	14.0	9.7	87	91
BanCoppel	10,968	2	11.1	6.4	86	79
HSBC México	6,060	1	25.2	18.9	81	90
Scotiabank	5,416	1	10.0	2.1	52	84
Otros	5,565	1	12.3	4.5	-	-

CANAL POR DONDE SE DAN LOS FRAUDES CIBERNÉTICOS

FRAUDES CIBERNÉTICOS

Canal transaccional

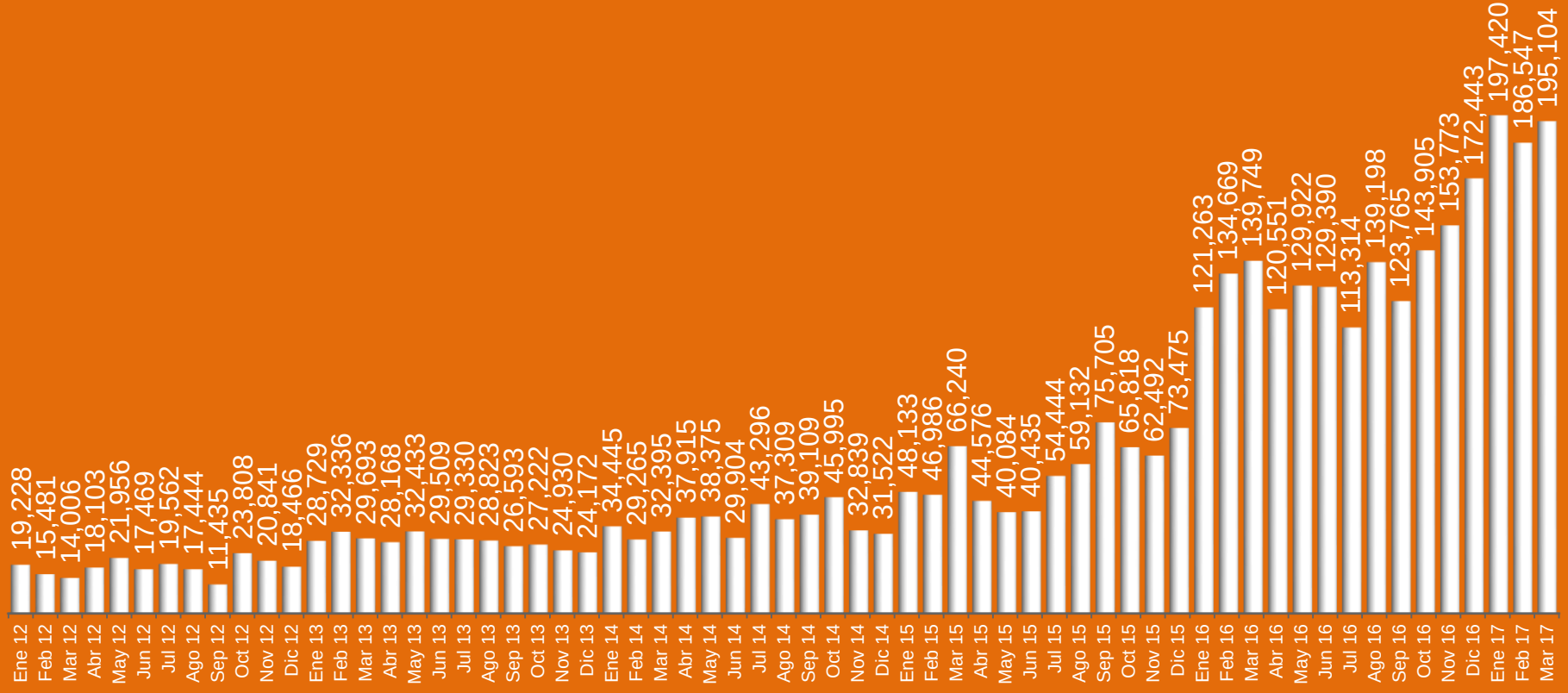
El 91% fueron por comercio electrónico. Destaca el incremento de las operaciones por internet PF y de Banca Móvil (167% y 74% respectivamente)

	2016 T1	2017 T1					
	Total	Total	Part. %	Var. %	Monto reclamado (mdp)	% abono	% Fav
	421,360	639,857	100	52	$1,167	53	90
Comercio por Internet	395,681	579,071	91	46	$662	85	93
Op. por Internet P Físicas	18,553	49,449	8	167	$281	26	82
Banca Móvil	5,139	8,938	1	74	$101	11	15
Op. por Internet P Morales	1,025	1,365	0	33	$123	2	22
Pagos por Celular	962	1,034	0	7	$1.6	6	1

FRAUDES CIBERNÉTICOS EN COMERCIO ELECTRÓNICO

COMPORTAMIENTO MENSUAL 2012-2017

En 2017, el **PROMEDIO MENSUAL ES DE 193 MIL**; hace un año era de 131 mil y en 2012 18 mil.

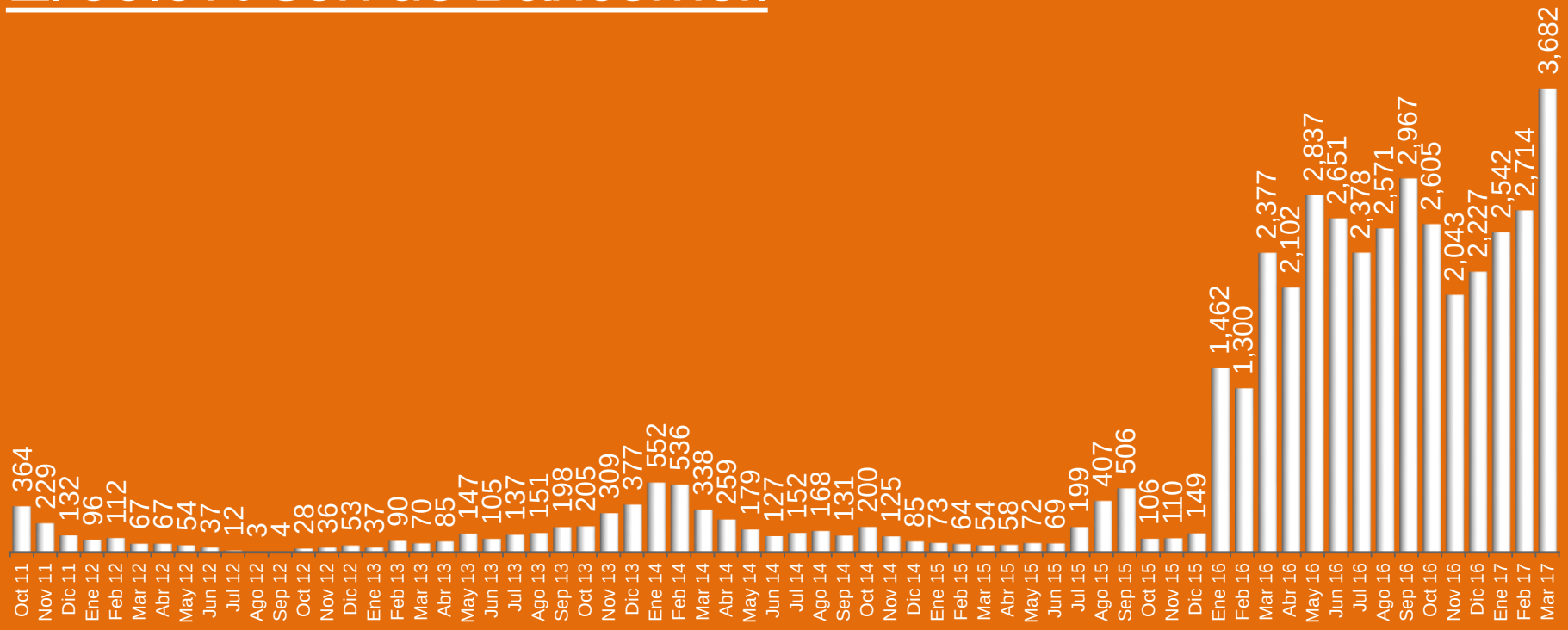


FRAUDES CIBERNÉTICOS EN BANCA MÓVIL

COMPORTAMIENTO MENSUAL 2011-2017

Preocupa la **TENDENCIA A LA ALZA**; en el mes de marzo se presentó cifra histórica con 3,682 casos.

El 99.9% son de Bancomer.



Por todo lo anterior, la CONDUSEF sugiere tomar en cuenta las siguientes recomendaciones para evitar ser víctima de un fraude ya sea tradicional o cibernético:

RECOMENDACIONES
A LOS USUARIOS DE SERVICIOS FINANCIEROS

1. Evita realizar compras o transferencias electrónicas **en computadoras de uso público** o compartido.

2. Realiza tus compras seguras por internet, verificando que el sitio cuente con el **protocolo de seguridad** "https://" y un candado cerrado en la barra de direcciones.

3. No respondas ningún mensaje de **correo sospechoso**, de remitentes desconocidos o aquellos que te dicen haber ganado un premio, viaje o sorteo, te pedirán tus datos personales.

4. Ten en cuenta que ni las entidades financieras, ni VISA o MasterCard u otro operador de tarjetas, solicitan **datos personales** a sus clientes o verificación de sus cuentas, mediante correo electrónico.

RECOMENDACIONES
A LOS USUARIOS DE SERVICIOS FINANCIEROS

5 **Nunca ingreses tus contraseñas**, sobre todo bancarias, a algún sitio al que se llegó por un correo electrónico o chat. Ingresa a la dirección oficial de la institución financiera.

6 Procura no apartarte de la computadora cuando tengas **abierta una sesión de banca por internet**, ni dejar el token a la mano.

7 No des a conocer a nadie tu **Número de Identificación Personal (NIP)** y cambia tus contraseñas de acceso con frecuencia.

8 Al realizar un pago, nunca pierdas de vista la **Terminal Punto de Venta (TPV)**, así evitarás un doble cargo o que tu tarjeta sea clonada.

RECOMENDACIONES
A LOS USUARIOS DE SERVICIOS FINANCIEROS

9 Utiliza tu tarjeta en sitios comerciales debidamente establecidos y **guarda tus vouchers** para posibles aclaraciones por cargos no reconocidos.

10 Antes de **tirar a la basura algún documento** que tenga información personal o financiera, destrúyelo por completo y verifica que ningún dato pueda ser extraído.

11 Revisa las terminales y cajeros, ya que la **presencia de aparatos añadidos** pueden delatar un duplicador de bandas magnéticas.

12 No permitas **ayuda de extraños** en Cajeros Automáticos.

RECOMENDACIONES
A LOS USUARIOS DE SERVICIOS FINANCIEROS

13 Si acudes a algún centro vacacional, cuida de **no dar datos de tus tarjetas** cuando te ofrecen tiempos compartidos o periodos vacacionales a lo largo del año, ya que al entregar la información de tu Tarjeta de Crédito o Débito, puedes estar aceptando cargos que se reflejarán en tu próximo estado de cuenta.

14 Recuerda que también existe el **Phishing telefónico (vishing)**, en donde los delincuentes simulan ser funcionarios bancarios y te piden otorgar datos de tus cuentas, generalmente aducen que tus cuentas están registrando cargos irregulares. Evita proporcionarles tus datos y llama directamente a la institución bancaria.

ACCIONES REALIZADAS POR CONDUSEF:

1. Se realizó una **CAMPAÑA DE DIFUSIÓN NACIONAL** sobre Robo de Identidad.
2. Se crearon **3 MICROSITIOS** informativos (Robo de Identidad, Comercio Electrónico y Educa tu Cartera).
3. Se implementó el **PROTOCOLO DE ATENCIÓN PORI** (Robo de Identidad).
4. Se actualizó en 4 ocasiones el BEF con información relevante de reclamaciones: **posible fraude, robo de identidad, fraude cibernético y banca móvil.**
5. **NUEVO CUADERNILLO DE FRAUDES FINANCIEROS**

Próximamente campaña de **Fraude Cibernético** en redes sociales y medios digitales.

Proyecto de Resolución que Modifica las Disposiciones de Carácter General aplicables a las Instituciones de Crédito en materia de Robo de Identidad (CNBV):

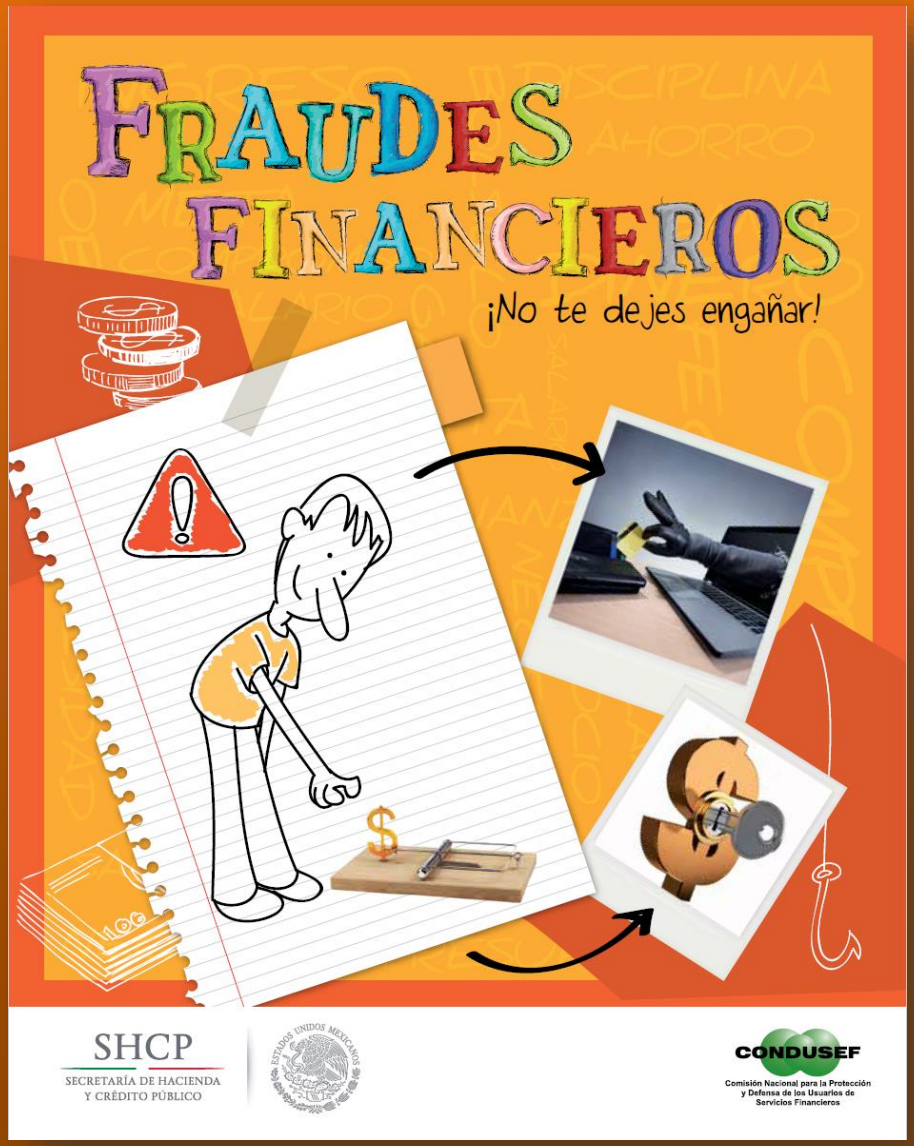
- Fortalecer los procedimientos y mecanismos que los bancos utilizan para **IDENTIFICAR A LA PERSONA QUE CONTRATA CON ELLAS,** con el fin de coadyuvar a prevenir, inhibir y, en su caso, detectar la suplantación de identidad;
- Verificar **LA VIGENCIA, INFORMACIÓN Y DOCUMENTACIÓN** para cerciorarse de la identidad de la persona: INE, pasaporte y CURP;
- Definir la forma y mecanismos para otorgar **CERTEZA EN LA CONTRATACIÓN "SIN PRESENCIA FÍSICA"**.
- Establecer la obligación de que los bancos cuenten con un **REGISTRO DE RECLAMACIONES** de sus clientes.
- Obtener el número de teléfono móvil o email del cliente a fin de **RECIBIR LAS NOTIFICACIONES Y ALERTAS**.
- Brindar a las IF la posibilidad para que generen una **BASE DE DATOS DE HUELLAS DACTILARES.**

Evita sorpresas, ¡mejor infórmate!

Contiene información de:

- ✓ Créditos exprés
- ✓ Pirámides
- ✓ Alteración de cheques
- ✓ Tallado
- ✓ Phishing
- ✓ Pharming
- ✓ Clonación de tarjetas
- ✓ Fraudes en internet

Además, te da tips para **evitar ser parte de la estadística** de posibles fraudes y robos de identidad.



CASOS PRÁCTICOS DE FRAUDE FINANCIERO

SHCP
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

CONDUSEF
Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros

CASO 1: FACEBOOK

- El Usuario consultó su Reporte de Crédito Especial, advirtiendo que en los registros existía un préstamo personal que no reconocía, por la cantidad de $2,174.00.
- Se procesó la queja dentro del Protocolo PORI con la Institución Financiera.
- La I.F. presentó su informe, con los requisitos para el otorgamiento del crédito, del que se desprendió lo siguiente:

1. Para el otorgamiento del crédito se creó un perfil falso de Facebook.
2. Todo el proceso de contratación del crédito se realiza en línea.
3. Se proporcionó una credencial para votar apócrifa del usuario.
4. El registro de la solicitud y la autenticación de la información proporcionada se realiza a través de la cuenta de Facebook.

- Resultado: Se lograron conciliar los intereses a favor del Usuario a través del protocolo de atención especial PORI, al advertirse que se presentó una identificación apócrifa.

SHCP
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

CONDUSEF
Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros

CASO 2: BANCA MÓVIL

- El cajero automático retuvo la tarjeta del Usuario, al tratar de reportarla le indicaron que ya había sido cancelada, hecho que el Usuario no realizó. Al acudir a la sucursal, a solicitar los movimientos, se percató de lo siguiente:
  1. El alta en el sistema de alertas de la Institución Financiera con un número de celular y un correo electrónico que desconoce.
  2. El alta en el servicio de Banca Móvil, a través del número de celular que desconoce.
  3. De la disposición de los recursos existentes en su cuenta, incluyendo los depositados en una cuenta de inversión inmediata.
- Se inició procedimiento de Conciliación con la Institución Financiera, la cual presentó su informe, indicando el procedimiento para la contratación del servicio; por el cual esta Comisión Nacional advirtió lo siguiente:

  1. Para la contratación del servicio de Banca Móvil, se requiere contar con un teléfono celular "inteligente", sin embargo, el Usuario es una persona de la tercera edad que no utiliza dicha tecnología.
  2. La Institución Financiera no acreditó el canal por medio del cual se contrató el servicio de alertas y de Banca Móvil.
  3. La Institución Financiera refiere que el número telefónico registrado para la operación de Banca Móvil, no necesariamente debe ser el mismo que el Usuario registró ante la Institución Financiera al aperturar sus cuentas, ya que para la operación de Banca Móvil puede dar de alta uno distinto.
  4. La Institución Financiera no verificó que el número de teléfono celular dado de alta en Banca Móvil, se encontrara a nombre del Usuario.
  5. El número de teléfono celular registrado en Banca Móvil hace las veces de token virtual, con lo que se tiene acceso a la operación las 24 horas, los 7 días de la semana.
  6. A través de Banca Móvil accedieron a los recursos del Usuario, incluyendo aquéllos depositados en su cuenta de inversión, sin que existiera constancia física de la compra venta de títulos, ya que las instrucciones de venta se realizan a través de Banca Móvil sin que dicha aplicación generara documento alguno al respecto.
- Resultado: Se lograron conciliar los intereses a favor del Usuario, al advertirse las inconsistencias antes descritas.

SHCP
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

CONDUSEF
Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros

CASO 3: PHISHING

- El Usuario revisó el estado de cuenta y tuvo conocimiento de que se le realizaron movimientos que no reconoce a través de transferencias electrónicas.

- Se llevó a cabo el procedimiento de Conciliación con la Institución Financiera.

- La I.F. presentó su informe, manifestando que el usuario expuso sus datos personales y de acceso a banca electrónica a un tercero distinto, con lo que se comprometió la seguridad de su cuenta y argumenta que no solicitan vía correo electrónico o llamada telefónica, datos personales, claves de acceso, NIP'S o contraseñas, números de token.

- Resultado: No se conciliaron los intereses. Se dejaron a salvo los derechos de las partes para hacerlos valer ante la autoridad judicial, emitiendo el Dictamen Técnico Favorable, al considerar que se cuenta con elementos para suponer la procedencia de la reclamación del Usuario, ya que al presentarse movimientos inusuales en la cuenta, la Institución Financiera debió advertir de esta situación a través del área de prevención de fraudes.

SHCP
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

CONDUSEF
Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros

CASO 4: CHEQUES

- El 12 de abril de 2016 el Usuario giró un cheque al portador por la cantidad de $1,200.00, al encontrar mucha gente en la fila del banco, accedió a que se lo cambiara otro cliente de la Institución Financiera. Posteriormente, el usuario acudió a un cajero de la Institución Financiera percatándose de un movimiento raro en su saldo, procediendo a preguntar a su asesor, quien le indicó que el cheque fue cobrado por $100,200.00 y no estaba al portador sino a nombre de Laura Borja Pérez “nombre ficticio”.

- Se inició procedimiento de Conciliación con la Institución Financiera.

- La I.F. presentó su informe, manifestando que no es posible formular una propuesta conciliadora, toda vez que el cheque fue negociado de forma correcta, pues dicho documento al momento de ser presentado para su pago cumplía con todos los requisitos establecidos, anexando copia del cheque. En el cual se advierte la alteración de la cantidad, de $1,200.00 por $100,200.00, y en la palabra Portador la dividieron convirtiendo la primera parte “Porta” en Borja y sin espacio “dor” Pérez, generando el nombre ficticio de “Laura Borja Pérez”. Asimismo el cheque fue endosado en propiedad, por “Laura Borja Pérez” nombre ficticio, a favor de un tercero para abono en cuenta.

- Resultado: No se conciliaron los intereses. Se dejaron a salvo los derechos de las partes, para hacerlos valer ante la autoridad judicial.