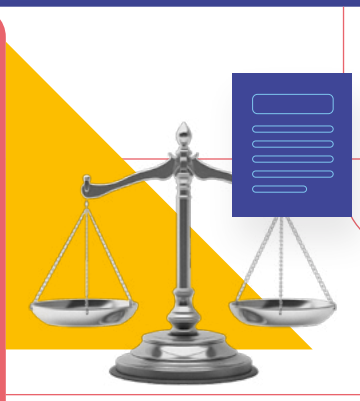
ift INSTITUTO FEDERAL DE TELECOMUNICACIONES

ESTUDIO DEL SIM SWAPPING EN MÉXICO

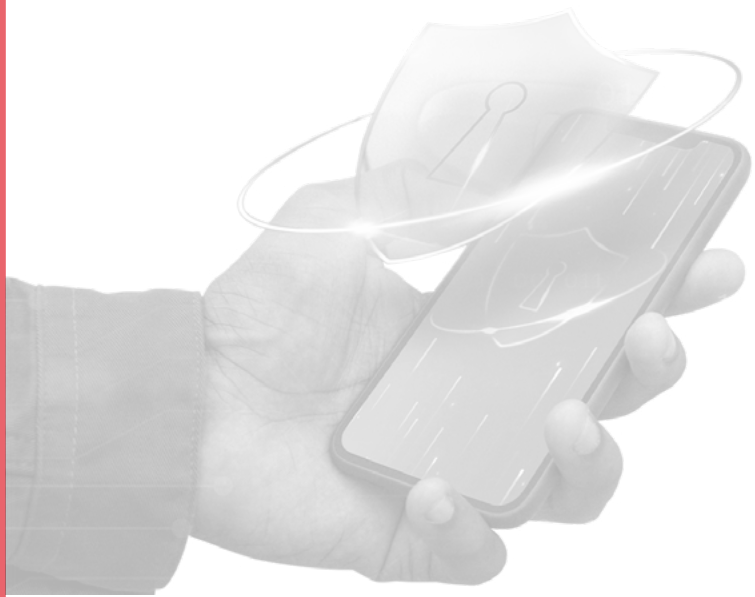


LEGALES

La Coordinación General de Política del Usuario publica el presente Estudio sobre el SIM Swapping en México, con fundamento en el Estatuto Orgánico del IFT que le otorga la atribución de diseñar mecanismos de información y comunicación que permitan informar a los usuarios de servicios de telecomunicaciones, de manera clara y objetiva, sus derechos y la manera de garantizarlos, así como proveer a los usuarios de información transparente y oportuna relacionada con las características de los servicios de telecomunicaciones, como es la calidad y la cobertura de estos. (Estatuto Orgánico del IFT, Artículo 71º Fracción IV, IFT, 2018)

El contenido, las opiniones y las conclusiones o recomendaciones vertidas en el documento no refleja la postura institucional ni es vinculante para el Pleno del Instituto Federal de Telecomunicaciones, ni para los concesionarios o autorizados para prestar servicios públicos de telecomunicaciones.

ÍNDICE



1. INTRODUCCIÓN

Durante los últimos años, el acceso de la población a internet y a las Tecnologías de la Información y Comunicación (TIC) ha incrementado considerablemente, así como los trámites y servicios habilitados a través de dichos medios. De acuerdo con la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH), la población de 6 o más años usuaria de internet ha pasado del 57.4% en 2015 al 81.2% en 2023[1]. Asimismo, para el año 2023 el 81.4% de la población era usuaria de teléfono móvil, de la cual el 95.5% usa un celular inteligente (smartphone).[2]

De la misma forma, los datos de la ENDUTIH muestran que, en el año 2023, el 31.9% de los usuarios de teléfono celular inteligente usan aplicaciones en sus dispositivos para acceder a la banca móvil, 3.4% más que en 2022.

De acuerdo con el sistema de información económica de Banco de México (BANXICO) al primer trimestre de 2024, existían 82,308,499 usuarios de banca por internet, de los cuales 383,577 realizan transferencias bancarias por teléfono móvil.

Con estas cifras se evidencia positivamente el aumento constante del uso del acceso a internet y de los usos productivos que la población está realizando, como es acceder a trámites y servicios, y a los servicios financieros a través de la banca en línea.

La población con acceso a internet se ha visto beneficiada por la disminución de las barreras de comunicación, la reducción de los tiempos y costos para acceder a información, servicios, trámites, entre otros. Sin embargo, negativamente también hay diversos datos que muestran que se han incrementado y actualizado las amenazas en el ciberespacio y las posibilidades de ser víctima de un delito cibernético.

Los delincuentes han aprovechado las vulnerabilidades para atacar las redes, infraestructuras y sistemas informáticos, lo cual ha tenido un impacto significativo en la economía y la sociedad a nivel global, afectando tanto a gobiernos como a empresas y particulares[3].

A medida que avanza la tecnología, también lo hacen las tácticas que los delincuentes utilizan para atacar a las personas y apoderarse de los datos personales de sus víctimas y usurpar su identidad, generando diversas afectaciones, como son las patrimoniales[4].

[1] INEGI (2024). Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares. Disponible en: https://www.inegi.org.mx/programas/endutih/2023/

[2] Ídem.

[3] INTERPOL (s.f.) La ciberdelincuencia traspasa fronteras y evoluciona a gran velocidad. Disponible en: https://www.interpol.int/es/Delitos/Ciberdelincuencia

[4] Universidad Siglo 21 (22 de diciembre de 2022). El auge de la Cibercriminalidad: Desafíos y soluciones en la Era Digital. Disponible en: https://21.edu.ar/identidad21/el-auge-de-la-cibercriminalidad-desafios-y-soluciones-en-la-era-digital/

En este sentido, diversas aplicaciones y plataformas han implementado métodos de autenticación de dos factores como medidas de seguridad para proteger las cuentas de las personas usuarias[5], recibiendo en el equipo terminal móvil un mensaje corto de texto (SMS) con un código de verificación para iniciar sesión, recuperar cuentas o contraseñas en caso de olvido.

Lo anterior, si bien son medidas en beneficio de las personas usuarias para proteger su información y acceso a las plataformas, también le ha conferido una gran importancia al número telefónico, ya que éste actúa como llave de acceso a su información y cuentas personales.

Por ello, cuando un atacante tiene en su poder una tarjeta SIM con el número telefónico de la víctima, este puede acceder a gran parte de su información, cambiar contraseñas y apoderarse de las cuentas asociadas a las plataformas digitales que tengan habilitada la autenticación de dos factores por medio del servicio móvil de telefonía o mensajes cortos.

En este contexto, en el que las personas utilizan su número telefónico como mecanismo de autenticación para acceder a sus cuentas de redes sociales, banca digital, correo electrónico y diversas aplicaciones, surge el SIM SWAPPING como una nueva técnica de ataque a las personas usuarias.

Esta técnica implica que el atacante, habiendo obtenido previamente información personal de su víctima por medio de ingeniería social u otra técnica, se haga pasar por esta para solicitar al concesionario o autorizado que transfiera el número telefónico a una nueva tarjeta SIM. Con ello, el atacante puede acceder a las cuentas y aplicaciones asociadas al número telefónico de la víctima, comprometiendo la seguridad de la persona usuaria, poniendo en riesgo sus datos personales, contenido multimedia, cuentas bancarias, contactos y cualquier otra información almacenada en las plataformas digitales.

En los últimos años, el SIM SWAPPING ha ganado popularidad a nivel global, afectando a un número creciente de personas, generando pérdidas financieras y daños sociales a las víctimas. En México, si bien no se tiene una cifra exacta del número de víctimas de esta práctica, algunos casos se han presentado ante las autoridades, exponiendo de esta forma el *modus operandi* de los atacantes, así como las afectaciones que se pueden ocasionar a las víctimas.

Lo anterior, evidencia la necesidad de abordar esta problemática, haciéndola de conocimiento público, difundiendo las medidas de prevención y a través de la emisión de normativas que puedan contribuir a la mitigación de esta.

Para contribuir con estas acciones, el presente estudio tiene como objetivo ampliar el conocimiento disponible respecto al SIM SWAPPING en México, para ello se realizó una investigación para exponer en qué consiste esta práctica, su incidencia en nuestro país, las acciones implementadas por los organismos reguladores de otros países para combatirla, los mecanismos de protección implementados por los concesionarios o autorizados, y se emiten algunas conclusiones orientadas a la prevención del SIM SWAPPING y para proteger a las personas usuarias.

Finalmente, se realizan recomendaciones para prevenir y mitigar el impacto del SIM SWAPPING, dirigidas a las personas usuarias, concesionarios y autorizados para prestar servicios de telecomunicaciones, autoridades y otras partes interesadas.

[5] Fernández Yúbal (6 de octubre de 2021). Verificación en 2 pasos o 2FA: qué es, para qué sirve y qué métodos existen. Xataca. Disponible en: https://www.xataka.com/basics/verificacion-dos-pasos-2fa-que-sirve-que-metodos-existen

2. SIM SWAPPING Y SUS GENERALIDADES

2.1. ¿Qué es?

De acuerdo con la Secretaría de Seguridad Ciudadana de la Ciudad de México (SSC), se reconoce al "SIM SWAPPING" como la duplicación de la tarjeta SIM con la intención de suplantar la identidad de clientes de instituciones bancarias por medio del número telefónico y, de esta forma, acceder a las cuentas bancarias ligadas al dispositivo móvil[6].

Asimismo, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) señala que el SIM SWAPPING es una modalidad de fraude, ya que roba la identidad del usuario para que el delincuente pueda tener acceso a las claves o datos confidenciales de las cuentas bancarias de las personas usuarias[7].

La Alianza para Soluciones de la Industria de las Telecomunicaciones (ATIS, por sus siglas en inglés)[8], define al SIM SWAPPING como un fraude, una forma avanzada de robo de identidad que aprovecha las debilidades en los procesos de autenticación de los proveedores de telefonía móvil. En este tipo de fraude, se señala que el número de teléfono del usuario se transfiere sin autorización a una nueva tarjeta SIM o SIM integrada (eSIM) controlada por un individuo malintencionado.

Asimismo, se destaca que, aunque esta acción pueda parecer simple, sus repercusiones son significativas, ya que le permite al individuo malintencionado acceder a los mensajes de texto entrantes, llamadas e incluso evadir las medidas de seguridad de autenticación de dos factores (2FA)[9].

Los estafadores suelen utilizar la ingeniería social[10] en los ataques de SIM SWAPPING para recopilar información personal de la persona usuaria, por ejemplo a través de correos electrónicos (phishing) y llamadas engañosas (vishing) en las que se hacen pasar por personal de servicio al cliente[11].

Las implicaciones del SIM SWAPPING son diversas e incluyen pérdidas financieras, acceso a cuentas bancarias y usurpación de identidad. Además, comprometen la comunicación personal y comercial, reparar el daño puede ser un proceso largo y difícil para las víctimas.

[6] SSC (29 de octubre de 2020). Policía Cibernética de la SSC alerta a la ciudadanía sobre nueva modalidad de fraude denominada "SIM SWAPPING" O "Duplicación de Sim". Gobierno de la Ciudad de México. Disponible en: https://www.ssc.cdmx.gob.mx/comunicacion/nota/2191-policia-cibernetica-de-la-ssc-alerta-la-ciudadania-sobre-nueva-modalidad-de-fraude-denominada-sim-swapping-o-duplicacion-de-sim

[7] CONDUSEF (2024). Modalidad de fraude también conocido como SIM SWAPPING. Disponible en: https://www.condusef.gob.mx/?p=contenido&idc=1594&idcat=3

[8] ATIS es una organización líder en tecnología y desarrollo de soluciones, la cual reúne a las principales empresas de TIC a nivel mundial para promover las prioridades comerciales de la industria.

[9] ATIS (marzo de 2024). Enhancing Telecom Security through Self-Sovereign Identity: A Solution to SIM Swap Fraud. Resources, White Papers, pp. 4 y 5. Disponible en: https://atis.org/resources/enhancing-telecom-security-through-self-sovereign-identity-a-solution-to-sim-swap-fraud/

[10] Técnica de estafa basada en cómo piensan y actúan las personas, que tiene la finalidad de engañar y manipular al usuario, para que, aprovechándose del error humano, se acceda a información privada, se obtenga acceso a sistemas u objetos de valor. Kaspersky (s.f.) ¿Qué es la ingeniería social? Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

[11] Ídem

2.2. ¿Cómo se lleva a cabo esta práctica?

La CONDUSEF ha descrito el *modus operandi* de esta práctica, destacando las siguientes fases[12]:

1. Un tercero solicita a la compañía telefónica el cambio de tarjeta SIM, alegando un presunto daño o pérdida.
2. Una vez concretado este proceso, el supuesto titular de la línea acude con una identificación falsa para recoger la tarjeta SIM y con ello tener acceso a números telefónicos, cuentas bancarias, información en la nube, entre otros datos.
3. Con la tarjeta SIM en su poder, los defraudadores pueden iniciar sesión en cuentas que utilizan los SMS como método de autenticación, ya que reciben los mensajes con los códigos de verificación.
4. Este tipo de fraude no se limita al robo de información bancaria, ya que también permite el acceso a sus contactos e información.

En el año 2020, la SSC publicó la nota informativa 2191[13] mediante la cual informa a la población la forma bajo la cual se realiza el SIM SWAPPING, destacando lo siguiente:

> *"Consiste en llamar a la compañía telefónica de un ciudadano haciéndose pasar por él para pedir la cancelación y reposición de su SIM. De este modo, el delincuente accede a las cuentas bancarias ligadas al teléfono.*
>
> *Cabe mencionar que, el número telefónico no basta para tomar la posesión de la banca electrónica. Por ello, los cibercriminales obtienen datos por medio de ingeniería social, a través de internet y redes sociales, con lo que complementan la información de autenticidad.*
>
> *A través de la línea telefónica, el defraudador valida aplicaciones y activa servicios que le permiten obtener claves de desbloqueo de la banca electrónica, para tener el control de ellas.*
>
> *Es así como las Instituciones financieras reciben las llamadas telefónicas y no detectan ninguna anomalía, ya que no tienen la capacidad de identificar que quien posee el control de esa línea telefónica no es el cliente registrado, por lo tanto, brinda servicios de manera normal.*
>
> *Esta modalidad de "SIM SWAPPING" también puede afectar las comunicaciones, ya que hoy en día aplicaciones de mensajería instantánea como WhatsApp, Telegram, Messenger entre otras, ocupan el sistema de verificación en dos pasos que incluye el envío de un código por SMS al número telefónico."*

[12] CONDUSEF (s.f). Modalidad de fraude también conocido como SIM Swapping. Disponible en: https://www.condusef.gob.mx/?p=contenido&idc=1594&idcat=3

[13] SSC, op. cit.

Por su parte, ATIS describe el proceso de SIM SWAPPING de la siguiente manera:

Diagrama 1.
Proceso del SIM SWAPPING

Fuente: ATIS. *Enhancing Telecom Security through Self-Sovereign Identity: A Solution to SIM Swap Fraud*, 2024.

Finalmente, también es importante destacar que, durante el proceso de portabilidad numérica, en caso de efectuarse una portabilidad no consentida, el atacante podría tener acceso a una tarjeta SIM con el número telefónico de la víctima, cuando se hace pasar como el legítimo propietario del número telefónico portado ante el concesionario o autorizado receptor.

3. EL SIM SWAPPING EN EL MARCO JURÍDICO MEXICANO

La SSC ha identificado al "SIM SWAPPING" o "duplicación de SIM" como una nueva modalidad de fraude, en el que los delincuentes suplantan la identidad de la víctima para solicitar la duplicación de su tarjeta SIM para posteriormente utilizarla para acceder a toda clase de información ligada a su línea telefónica, siendo su principal objetivo las cuentas bancarias[14].

Asimismo, la Fiscalía General del Estado de Michoacán señala que el SIM SWAPPING no se encuentra tipificado como delito, sin embargo, en caso de que se iniciara carpeta de investigación se establecería lo mencionado en el artículo 301 Bis del Código Penal para el Estado de Michoacán, el cual establece:

> *"Artículo 301 bis. Usurpación de Identidad. Se impondrán de dos a cinco años de prisión y de doscientos a quinientos días de multa, a quien sin la autorización previa de quien pueda otorgarla, utilice datos personales, para realizar actos jurídicos o de cualquier otra índole, con la finalidad de obtener beneficios para sí o para otro o con el fin de perjudicar de algún modo al usurpado."*

Por su parte, la Fiscalía General del Estado de Quintana Roo cuenta con 2 carpetas de investigación relacionadas con suplantación de identidad, para investigar el SIM SWAPPING.

Es importante destacar que actualmente, de acuerdo con la Guardia Nacional, 30 entidades federativas en México han tipificado la suplantación de identidad en sus legislaciones, abordando esta problemática de manera general.

Con lo anterior, se puede advertir que, si bien no existe un tipo penal que lo contemple, el SIM SWAPPING ha sido investigado por algunas de las Fiscalías Generales de los Estados como fraude, suplantación de identidad y robo de identidad.

Adicionalmente, se considera oportuno destacar que durante la ejecución del SIM SWAPPING, se podrían estar materializando delitos en materia de datos personales.

Lo anterior, en virtud de que de acuerdo con el Diccionario de Protección de Datos Personales del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), un delito en materia de datos personales es:

> *"Aquella acción llevada a cabo y contraria a lo establecido por los ordenamientos legales en la materia —que contraviene a la dignidad de la persona— específicamente respecto del tratamiento indebido de información de carácter personal y cuya garantía prevé una sanción que puede ser agravada, respecto de condicionantes como las veces que se ha cometido la falta, la gravedad y trascendencia de la falta o el tratamiento indebido de datos personales sensibles."*[15]

De lo anterior, podemos observar que la vulneración de los datos personales constituye un elemento fundamental para la ejecución del SIM SWAPPING, en virtud de que el tratamiento no autorizado por parte de los titulares de los datos personales y la vulneración de su seguridad son consecuencias de esta práctica.

[14] Ídem

[15] Alday, Barco, Carbonell et. al. (2019). Diccionario de Protección de Datos Personales. Conceptos fundamentales. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), Primera edición, México, pág. 240, ISBN: 978-607-98648-3-5. Disponible en: https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/DICCIONARIO_PDP_digital.pdf

4. DATOS ESTADÍSTICOS DE SIM SWAPPING EN MÉXICO

Actualmente, no existe información estadística exacta sobre la incidencia del SIM SWAPPING en México, toda vez que no existe un tipo penal que identifique y sancione específicamente esta práctica. Sin embargo, como se ha mencionado, por sus características se ha clasificado como fraude, suplantación de identidad y robo de identidad; por ello, los casos presentados se podrían estar registrando dentro de dichas estadísticas de incidencia delictiva.

Al investigar la incidencia delictiva, encontramos que, según las estadísticas del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP), no existe un registro desglosado que permita identificar mensualmente y a nivel estatal o municipal la incidencia del SIM SWAPPING. Sin embargo, se consideran estadísticas de todo tipo de fraudes y no se especifica cuáles se cometieron por medio del SIM SWAPPING o la duplicidad de tarjetas SIM.

Ante la falta de estadísticas sobre la incidencia del SIM SWAPPING en México, este Instituto realizó sendos requerimientos de información a las siguientes autoridades:

- Guardia Nacional.
- 32 Fiscalías Generales de los Estados.
- Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros.
- Comisión Nacional Bancaria y de Valores.
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Dentro de la información solicitada se encuentra la estadística de casos relacionados con el SIM SWAPPING y registrados en los estados durante los años 2021 a 2023, así como las disposiciones legales existentes para perseguir y sancionar dicha práctica.

Asimismo, se realizó una búsqueda en las inconformidades que las personas usuarias de servicios de telecomunicaciones han presentado en contra de concesionarios o autorizados a través de la plataforma “Soy Usuario”, a fin de poder detectar posibles casos asociados al SIM SWAPPING.

A continuación, se muestran la información reportada por las autoridades en atención a las solicitudes formuladas y los hallazgos de la revisión a la plataforma “Soy Usuario”.

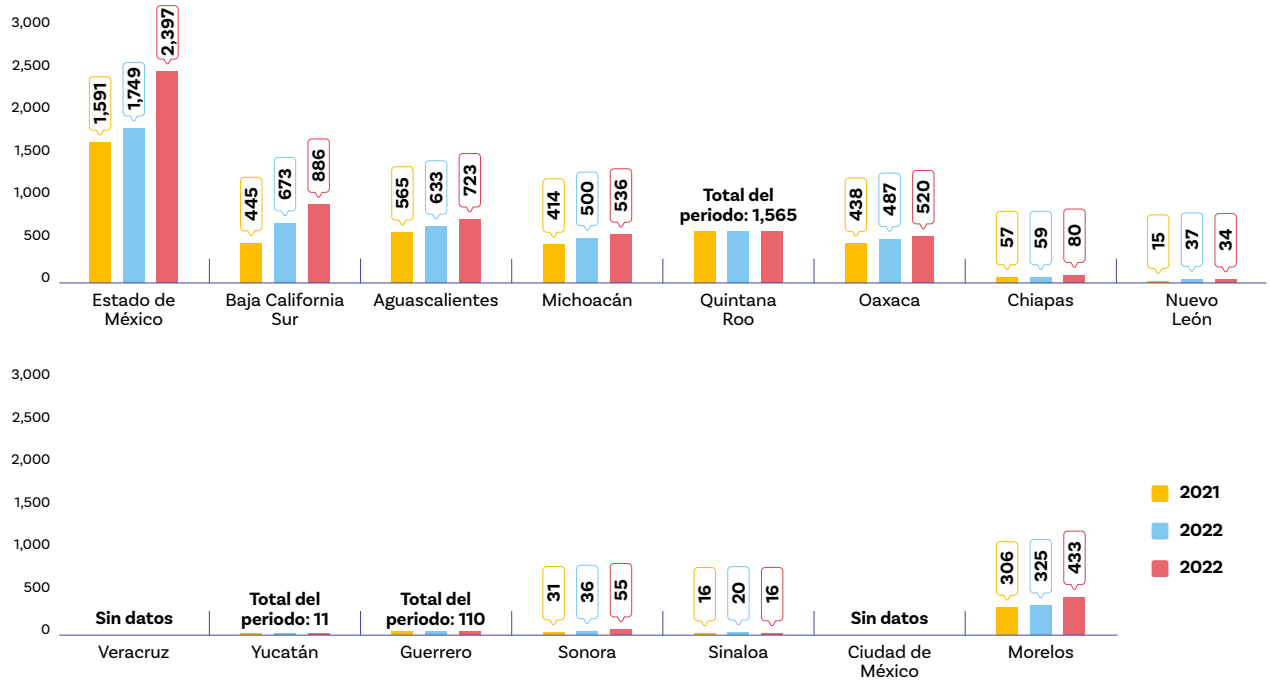
4.1. Fiscalías Generales de los Estados

De las solicitudes de información formuladas a las 32 Fiscalías Generales de los Estados, únicamente se recibió respuesta por parte de 15 fiscalías, de las cuales, solo la Fiscalía General del Estado de Quintana Roo informó contar con información específica sobre la incidencia de esta práctica.

No obstante lo anterior, se destaca que las demás Fiscalías Generales de los Estados, proporcionaron información sobre casos relacionados con incidentes cibernéticos, debido a que, dadas las características del SIM SWAPPING, existe la posibilidad de que este delito haya sido registrado como un delito cibernético.

En la **Gráfica 1** se muestran las estadísticas de carpetas de investigación iniciadas por las Fiscalías Generales de los Estados por incidentes cibernéticos. Como se observa en la gráfica, de los estados que atendieron la solicitud de información, la entidad con las cifras más altas es el Estado de México, mientras que Nuevo León es la entidad con la menor incidencia. En el caso de Veracruz y Ciudad de México, no se cuenta con información sobre estos delitos y la cifra proporcionada por la Fiscalía General del Estado de Quintana Roo corresponde al total de casos registrados entre los años 2021 a 2023, sin contar con un dato exacto para cada año.

Gráfica 1.
Casos registrados por las Fiscalías Generales de los Estados relacionados con incidentes cibernéticos de 2021 a 2023.

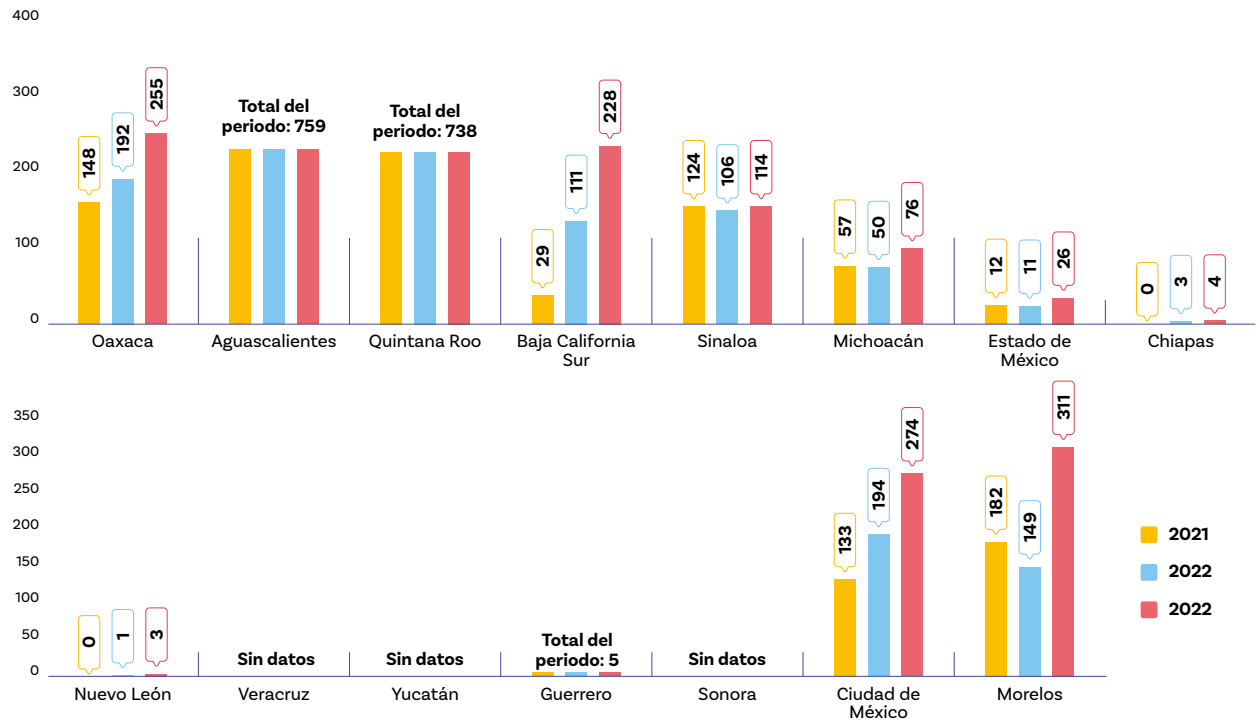


Fuente: Elaboración propia con base en la información proporcionada por las Fiscalías Generales de los Estados.

A fin de poder aproximarse a los posibles casos de SIM SWAPPING, se solicitó información sobre cuántos de estos casos, estaban relacionados con la suplantación de identidad.

En este sentido, en la **Gráfica 2** se presenta la información proporcionada por las Fiscalías Generales de los Estados respecto a los casos de delitos cibernéticos en los que se suplantó la identidad de las víctimas. Como se observa, Oaxaca, Morelos y Ciudad de México reportaron las cifras más altas de este delito, mientras que Nuevo León fue la entidad con la menor cifra registrada. Por su parte, Veracruz, Yucatán y Sonora no cuentan con información sobre esta clasificación de los delitos. Cabe mencionar que Aguascalientes y Quintana Roo reportaron la cifra correspondiente al total de casos registrados de los años 2021 a 2023, sin especificar la cifra exacta para cada año.

Gráfica 2.
Casos registrados por las Fiscalías Generales de los Estados relacionados con suplantación de identidad de 2021 a 2023.



Fuente: Elaboración propia con base en la información proporcionada por las Fiscalías Generales de los Estados.

Posteriormente, se solicitó de forma específica a las Fiscalías que proporcionaran información sobre los casos de SIM SWAPPING de los que tuvieran registro; no obstante, únicamente la Fiscalía General del Estado de Quintana Roo, manifestó contar con dos carpetas de investigación abiertas sobre casos de SIM SWAPPING, sin especificar el periodo en el cual fueron iniciadas.

Asimismo, cada una de las Fiscalías Generales de los Estados que atendieron el requerimiento, informaron sobre las acciones que ejecutan para mitigar los delitos cibernéticos y la suplantación de identidad.

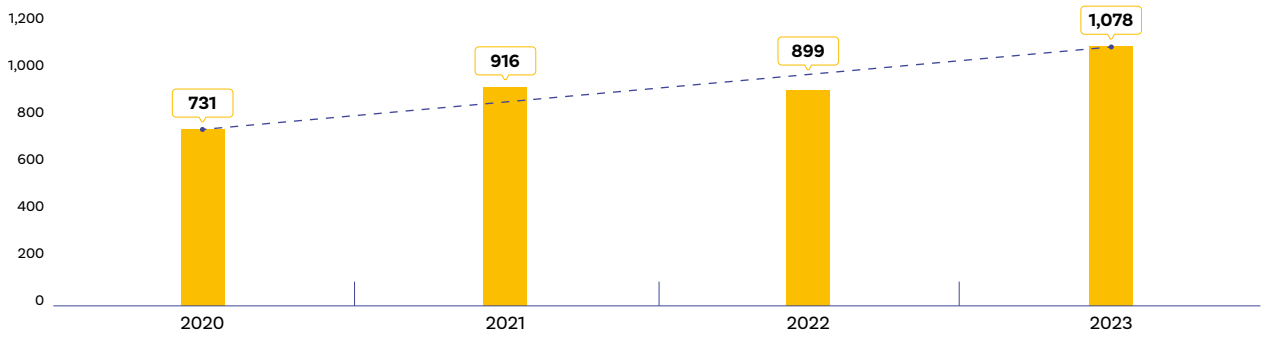
Es importante destacar que para dar un seguimiento a la evolución y la incidencia del SIM SWAPPING en México, así como a los delitos relacionados con este, resulta relevante contar con información estadística para poder mitigar dicha problemática.

4.2. Guardia Nacional

En atención al requerimiento de información efectuado a la Guardia Nacional se informó que se registraron 916 incidentes de suplantación de identidad durante el año 2021, 899 incidentes durante el año 2022 y 1078 incidentes durante el año 2023. Esta cifra se obtuvo a través de su portal electrónico, el cual puede consultarse en el siguiente enlace:

https://www.gob.mx/guardianacional/documentos/estadistica-de-reportes-ciudadanos-y-mandamientos-ministeriales-y-judiciales

Gráfica 3.
Reportes ciudadanos de suplantación de identidad recibidos en la Dirección General Científica de la Guardia Nacional de 2020 a 2023.



Fuente: Elaboración propia con base en la información de Estadística de Reportes Ciudadanos y mandamientos ministeriales y judiciales de la Guardia Nacional.

El portal contiene información estadística sobre reportes ciudadanos recibidos por la Dirección General Científica desde el 1 de enero de 2020 hasta el 31 de marzo de 2024. Sin embargo, no se cuenta con información relacionada con delitos cibernéticos para los años 2020, 2021, 2022, 2023 ni 2024.

No obstante, en cuanto a datos específicos sobre SIM SWAPPING, la Guardia Nacional indicó que no dispone de un desglose detallado que permita identificar incidentes de suplantación de identidad mediante la duplicación de tarjetas SIM.

Esta limitación se debe a que, según lo informado, la institución coadyuva bajo la dirección del Ministerio Público, quien determina los actos de investigación necesarios. Por lo tanto, recomendó redirigir consultas sobre carpetas de investigación relacionadas con SIM SWAPPING a las autoridades competentes.

Asimismo, se señaló que 30 entidades federativas en México han tipificado la suplantación de identidad en sus legislaciones, abordando esta problemática de manera general.

Con la información proporcionada por la Guardia Nacional podemos observar que el SIM SWAPPING es una práctica que puede estar siendo clasificada por los Ministerios Públicos como suplantación de identidad.

4.3. Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF)

Actualmente, algunas instituciones bancarias utilizan los números telefónicos asociados a sus usuarios como un medio para el envío de información sobre sus cuentas y como un mecanismo de autenticación para la recuperación de usuarios o contraseñas. Por ello, cuando un atacante cuenta con datos personales, incluyendo datos sensibles como son los financieros (números de cuenta, usuarios, contraseñas) y, adicionalmente tiene en su posesión una tarjeta SIM con el número telefónico de la víctima, este podría tener acceso y control de la banca en línea y realizar transacciones no consentidas, generando con esto un daño patrimonial.

Resulta relevante retomar la información estadística con la que cuenta la CONDUSEF sobre las quejas presentadas por fraudes asociados a accesos no autorizados a la banca en línea.

Con este fin, se consultaron los Anuarios Estadísticos sobre Reclamaciones Monetarias de la Banca, en los cuales se incluyen los casos en los que los usuarios acuden a la CONDUSEF o a las instituciones financieras para reportar problemas o solicitar aclaraciones relacionadas con algún producto o servicio financiero.

Dentro del total de estas reclamaciones, para aquellas en las que la problemática se desprenda de un posible caso de robo de identidad, desde el año 2016 la CONDUSEF ha implementado un procedimiento especial de atención a usuarios para casos de posible robo de identidad (PORI). El objetivo de este procedimiento es enfrentar las problemáticas de robo de identidad, orientando a la víctima para que presente una denuncia ante el Ministerio Público y proporcionando un seguimiento especial a estos casos.

En este sentido, CONDUSEF informó que durante el año 2019 se presentó un total de 6,575 reclamaciones iniciadas dentro del procedimiento PORI, las cuales en el año 2020 disminuyeron considerablemente a 2,383, para incrementarse ligeramente en 2021, pasando a un total de 2,841; y, en el año 2022 nuevamente se redujeron a un total de 2,383 de reclamaciones.

Por otra parte, como se muestra en el **Cuadro 1**, respecto al peso relativo de este tipo específico de reclamaciones frente al total de reclamaciones monetarias de la banca presentadas en la CONDUSEF, se observa una tendencia a la baja de las reclamaciones PORI en términos relativos frente al total.

Cuadro 1.
Evolución del total de las reclamaciones monetarias de la Banca y las reclamaciones con procedimiento por posible robo de identidad ante la CONDUSEF (2019-2022).

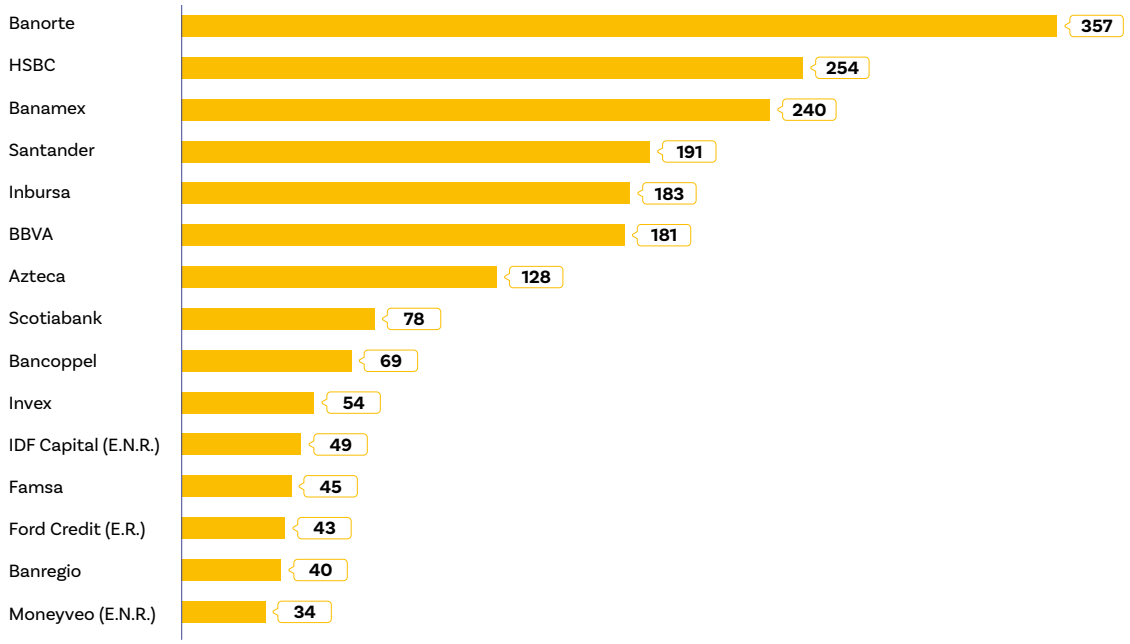
Reclamaciones monetarias de la Banca iniciadas en la CONDUSEF	2019	2020	Variación anual (%)	2021	Variación anual (%)	2022	Variación anual (%)
Total de Reclamaciones	310,200	192,345	-38	252,170	31.1	230,698	-8.5
Reclamaciones con procedimiento PORI	6,575	2,383	-63.8	2,849	19.6	2,325	-18.4
Peso relativo Reclamaciones PORI	2.1	1.2		1.1		1	

Fuente: Elaboración propia con base en información del Anuario Estadístico 2020, 2021 y 2022 de la CONDUSEF.

En cuanto a las reclamaciones iniciadas en el protocolo PORI, de la **Gráfica 4** a la **Gráfica 6**, se presenta la evolución de los casos presentados ante la CONDUSEF por institución financiera. En dichos gráficos podemos observar que Banorte en los años 2020 y 2021 se mantuvo como la institución que concentró el mayor número de reclamos y, en el año 2022 fue la segunda institución con más reclamos, solo detrás de Banco Azteca, y junto a HSBC y BBVA se posicionaron entre las instituciones que ocuparon las primeras posiciones.

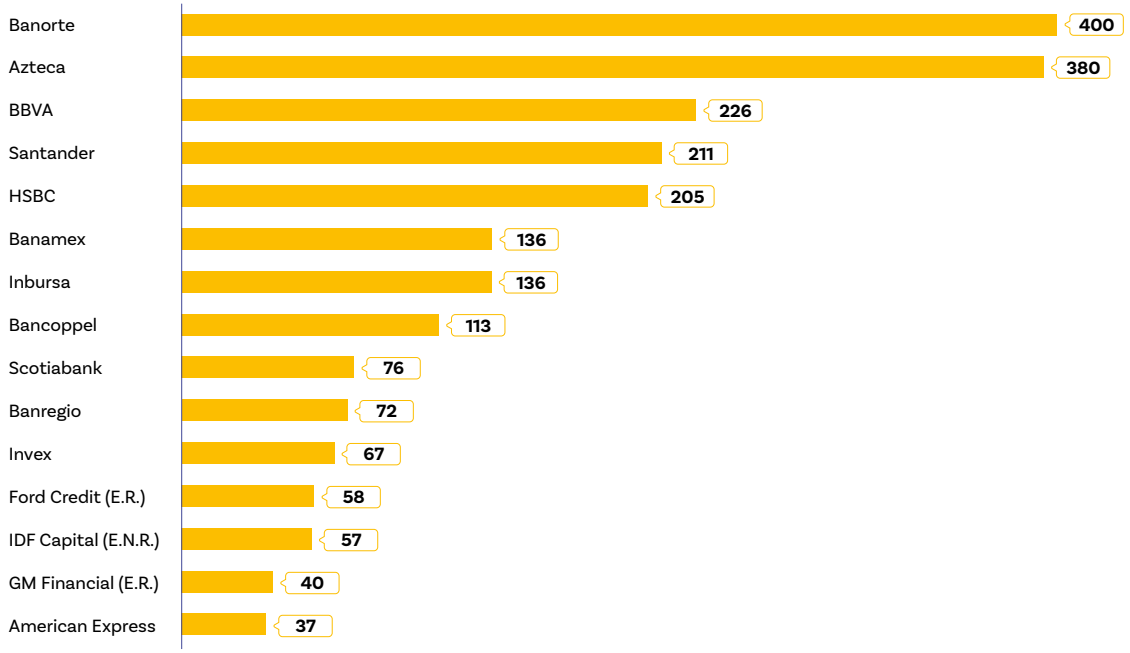
Lo anterior, es relevante ya que se considera que una política que pretenda hacer frente al SIM SWAPPING y sus consecuencias negativas para los usuarios de la banca, debe considerar como principal punto de acción un fortalecimiento de los protocolos de verificación de identidad de acuerdo a la incidencia particular.

Gráfica 4.
Principales instituciones financieras con reclamaciones por Protocolo PORI ante la CONDUSEF en 2020.



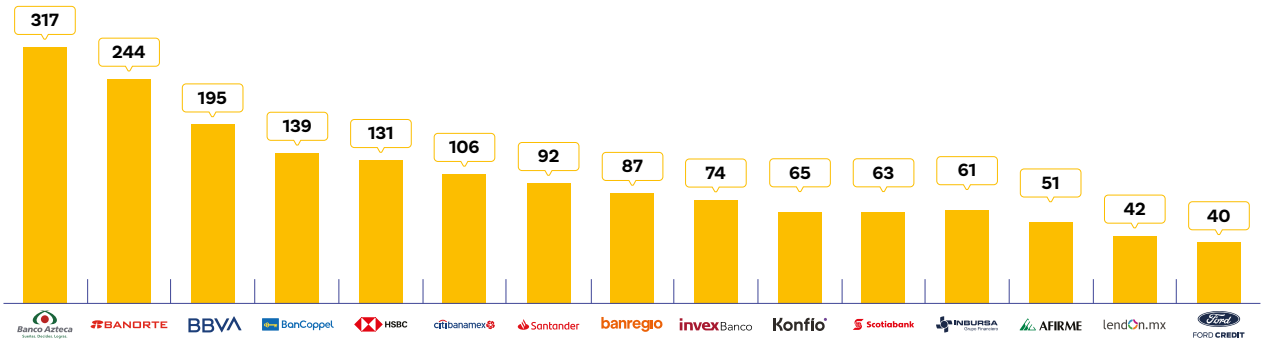
Fuente: Anuario Estadístico de la CONDUSEF 2020.

Gráfica 5.
Principales instituciones financieras con reclamaciones por Protocolo PORI ante la CONDUSEF en 2021.



Fuente: Anuario Estadístico de la CONDUSEF 2020.

Gráfica 6.
Principales instituciones financieras con reclamaciones por Protocolo PORI ante la CONDUSEF en 2022.



Fuente: Anuario Estadístico de la CONDUSEF 2022.

Por su parte, respecto a las causas por las que se presentaron las reclamaciones bajo el protocolo PORI, en el **Cuadro 2** y **Cuadro 3** observamos que los créditos no reconocidos en el historial crediticio, así como los créditos, tarjetas de crédito o cuentas otorgadas sin ser solicitados ni autorizados por el usuario, cliente y/o socio, son las principales razones por las que las personas acuden ante la CONDUSEF. Este dato resulta relevante, ya que permite identificar cuáles podrían ser los trámites con mayor probabilidad de que se realicen derivado de un robo de identidad.

Cuadro 2.
Reclamaciones por protocolo PORI, por causa, 2019-2020.

Causa	2019	2020	Part. (%)	Var. (%)
Total	6,575	2,383	100	-63.8
Crédito no reconocido en el historial crediticio	2,117	1,289	54.1	-39.1
Crédito, TDC o cuenta otorgados sin ser solicitados ni autorizados por el Usuario, cliente y/o socio	2,280	440	18.5	-80.7
El Usuario, cliente y/o socio, no reconoce haber celebrado contrato con la Institución (crédito o depósito)	852	239	10	-71.9
Emisión de tarjeta de crédito sin solicitud	694	206	8.6	-70.3
Disposición de efectivo en ventanilla y/o sucursal no reconocida por el Usuario, cliente y/o socio	413	137	5.7	-66.8
Inconformidad con el cobro de productos o servicios no contratados por el Usuario, cliente y/o socio	201	66	2.8	-67.2
Rectificación resultante de PORI*	18	6	0.3	-66.7

*Son todas aquellas causas que inician registro en el SIO como PORI, pero al avanzar el trámite se determina que no provienen de un robo de identidad.

Fuente: Anuario Estadístico de la CONDUSEF 2020.

Cuadro 3.
Reclamaciones por protocolo PORI, por causa, 2021-2022.

Reclamaciones por causa	Enero-Diciembre			
Causa	2021	2022	Part. (%)	Var. (%)
Total	**2,849**	**2,325**	**100**	**-18.4**
Crédito no reconocido en el historial crediticio	**1,724**	**1,443**	**62.1**	**-16.3**
El Usuario, cliente y/o socio no reconoce haber celebrado contrato con la Institución (crédito o depósito)	375	345	14.8	-8
Crédito, TDC o cuenta otorgados sin ser solicitados ni autorizados por el Usuario	437	291	12.5	-33.4
Disposición de efectivo en ventanilla y/o sucursal no reconocida por el Usuario	130	126	5.4	-3.1
Emisión de tarjeta de crédito sin solicitud	134	80	3.4	-40.3
Inconformidad con el cobro de productos o servicios no contratados por el Usuario	42	33	1.4	-21.4
Rectificación resultante de PORI*	7	7	0.3	-

*Son todas aquellas causas que inician registro en el SIO como PORI, pero al avanzar el trámite se determina que no provienen de un robo de identidad.

Fuente: Anuario Estadístico de la CONDUSEF 2022.

Además de lo anterior, durante el período de febrero de 2022 a junio de 2024, un total de 211,673 usuarios de bancos presentaron una Queja Electrónica a través del Portal de Queja Electrónica de CONDUSEF. De estos usuarios, el 31.3% (66,229) completaron voluntariamente una encuesta al finalizar el proceso de la queja.

En la encuesta, el 46.4% de los usuarios asociaron el posible fraude con sus cuentas de depósito a la vista, mientras que el 33.3% lo asociaron con operaciones de crédito en cuenta corriente.

Respecto a los tipos de fraude identificados, el 35.8% de los usuarios consideraron haber sido engañados a través de llamadas telefónicas que aparentaban provenir de su banco, un 22.2% mencionó que recibieron mensajes SMS o WhatsApp solicitando datos de sus cuentas bancarias bajo el pretexto de cargos sospechosos, y un 18.9% indicó haber ingresado a un portal que parecía ser de su institución, pero resultó ser falso. Estas tres modalidades suman el 76.9% del total de los cinco tipos de fraudes considerados en la encuesta.

En cuanto a las tendencias, se observa que el 43.2% de los fraudes en banca electrónica están relacionados con llamadas telefónicas que se hacen pasar por comunicaciones del banco. Además, los fraudes a través de celulares han crecido en participación, alcanzando un aumento del 15.1% y superando en un 60% los reportados entre febrero y diciembre de 2022 en comparación con el mismo período en 2023.

Finalmente, el 29.7% de los usuarios que reportaron haber sido víctimas de fraude virtual presentaron su queja en alguna de las tres unidades de Atención a Usuarios de la Ciudad de México. Por entidad federativa, el Estado de México superó ligeramente a la Ciudad de México con un 18.5% frente al 17.9%, seguido de Jalisco con un 8.4%.

Lo anterior cobra relevancia si consideramos que las llamadas telefónicas fraudulentas, los mensajes SMS/WhatsApp y el acceso a portales falsos son métodos comunes para obtener la información necesaria para llevar a cabo el SIM SWAPPING. Además, el crecimiento en los fraudes relacionados con el celular refuerza la relevancia de este tipo de ataque en el panorama actual de fraudes bancarios en México.

4.4. Instituto Federal de Telecomunicaciones

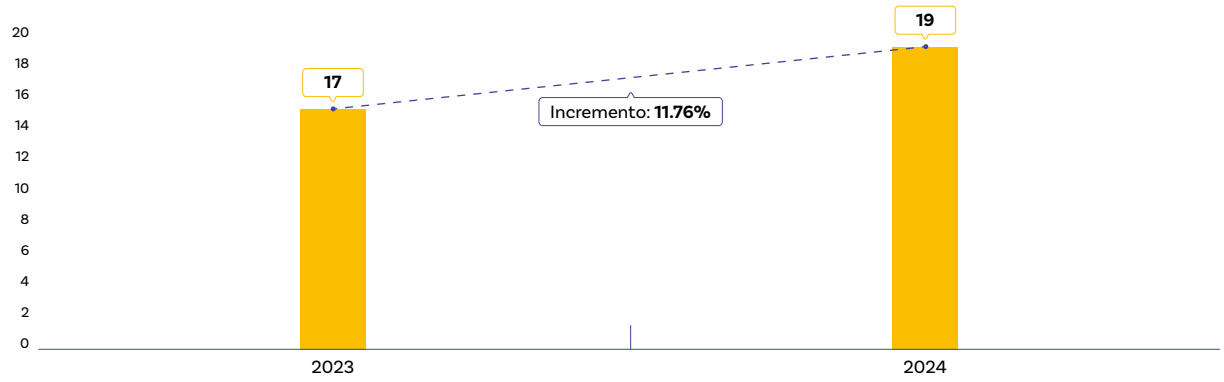
El IFT ha puesto a disposición de la población el portal "Soy Usuario", el cual es una herramienta electrónica que permite a las personas usuarias de servicios públicos de telecomunicaciones interponer inconformidades cuando consideran que se han vulnerado sus derechos[16].

A través de este portal el IFT gestiona las inconformidades presentadas por las personas usuarias por diversos motivos; siendo esta una fuente valiosa y confiable que nos permite identificar y conocer, a través de la información proporcionada por las personas, aquellos casos posiblemente asociados al SIM SWAPPING.

Por tal motivo, se han identificado aquellas inconformidades que, conforme a la narrativa de las personas, podrían estar relacionadas con un caso de SIM SWAPPING, toda vez que, de su lectura se advierte que, sin el consentimiento de la persona, su tarjeta SIM fue cambiada y utilizada indebidamente por un tercero.

De acuerdo con la información de la herramienta Soy Usuario, como se muestra en la ***Gráfica 7,*** tan sólo del mes de enero a octubre de 2024 se han registrado 19 casos de SIM SWAPPING, mientras que en el año 2023 se tuvo un registro de 17 casos, lo que representa un incremento del 11.76%.

Gráfica 7.
Casos de SIM SWAPPING registrados por año en el portal Soy Usuario.

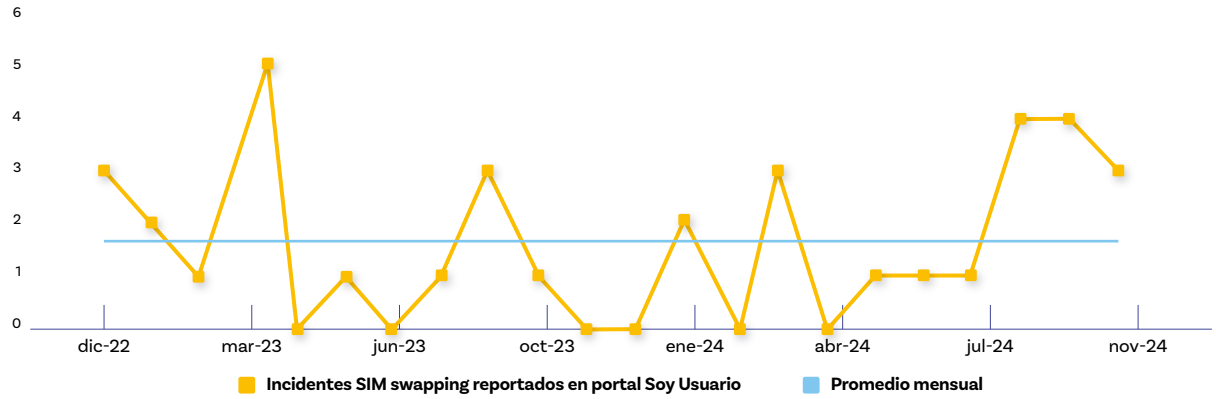


Fuente: Elaboración propia con base en las quejas recibidas a través del portal Soy Usuario
Nota: Para el caso de 2024 se está considerando la información disponible hasta octubre

[16] IFT (s.f.) Levanta tu queja" Soy Usuario". Disponible en: https://www.ift.org.mx/usuarios-y-audiencias/levanta-tu-queja-soy-usuario#:~:text=SOY%20USUARIO%20es%20la%20herramienta,se%20han%20vulnerado%20sus%20derechos.&text=la%20informaci%C3%B3n%20que%20necesitas%20para%20hacer%20valer%20tus%20derechos.

En la ***Gráfica 8*** se observa el comportamiento de los casos de SIM SWAPPING reportados a través de esta herramienta mes por mes. Podemos observar que de enero de 2023 a octubre de 2024 se han registrado un promedio de 1.64 casos por mes, siendo abril de 2023, el mes con el mayor número de casos.

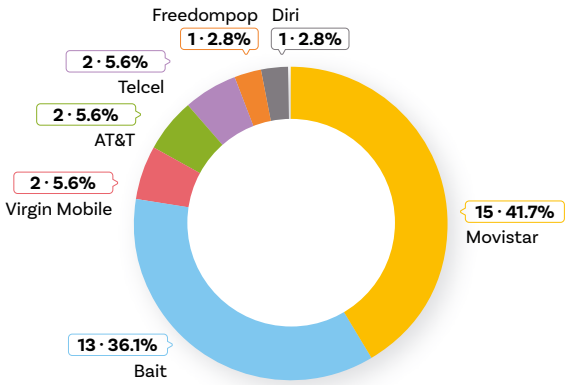
Gráfica 8.
Casos de SIM SWAPPING reportados a través del portal Soy Usuario de enero de 2023 a octubre de 2024.



Fuente: Elaboración propia con base en las quejas recibidas a través del portal Soy Usuario
Nota: Para el caso de 2024 se está considerando la información disponible hasta octubre

Asimismo, en la ***Gráfica 9*** podemos observar que, durante este periodo, 15 usuarios de Movistar presentaron inconformidades por haber sido víctimas de SIM SWAPPING, lo que representa el 41.7% del total de casos. En segundo lugar, se ubicó Bait con 13 casos, que representan el 36.1% del total, seguido de Virgin Mobile, AT&T y TELCEL, con 2 casos equivalentes al 5.6% para cada uno de ellos, finalmente FREEDOMPOP y Diri, con un caso, equivalente al 2.8% del total para cada uno.

Gráfica 9.
Casos de SIM SWAPPING reportados en el Portal Soy Usuario por proveedor.



Fuente: Elaboración propia con base en las quejas recibidas a través del portal Soy Usuario.

4.5. Asociación de Bancos de México (ABM)

La Asociación de Bancos de México (ABM) advierte sobre diversas formas de fraude telefónico, a través de la suplantación, destacando la importancia de adoptar medidas preventivas. De acuerdo con la ABM, las principales modalidades de fraudes son:

- **Vishing.** Es un fraude realizado mediante una llamada telefónica, generalmente con una voz automatizada y que simula ser de una institución bancaria, con la finalidad de conseguir los datos personales o bancarios de la víctima.

- **Smishing.** Es un fraude telefónico que se comete a través de un mensaje de texto (SMS) que afirma ser de una institución bancaria y por el cual se le pide información personal o financiera a la víctima.

- **Phishing.** A través de un correo electrónico que simula ser de una institución bancaria, se incluye un enlace malicioso que dirige a una página similar a la de la institución o empresa que simula ser. En esta página fraudulenta, la víctima introduce sus datos personales y el estafador logra obtenerlos.

- **Spoofing.** Con este fraude, el atacante "enmascara" o "disfraza" su número, para que aparezca el nombre de la institución bancaria en el identificador y así solicitar los datos personales de la víctima.

Asimismo, la ABM ha señalado que ha observado un notorio aumento en los casos de usurpación de identidad, específicamente a través de la suplantación de páginas digitales de instituciones financieras. Destacando que este tipo de fraude no es fácil de detectar, y las víctimas suelen percatarse de ello únicamente al recibir llamadas o notificaciones relacionadas con sus cuentas bancarias.

Por otro lado, se ha señalado que estos incidentes suelen iniciar con correos electrónicos que contienen enlaces que redirigen a páginas falsas, solicitando información personal como claves y contraseñas.

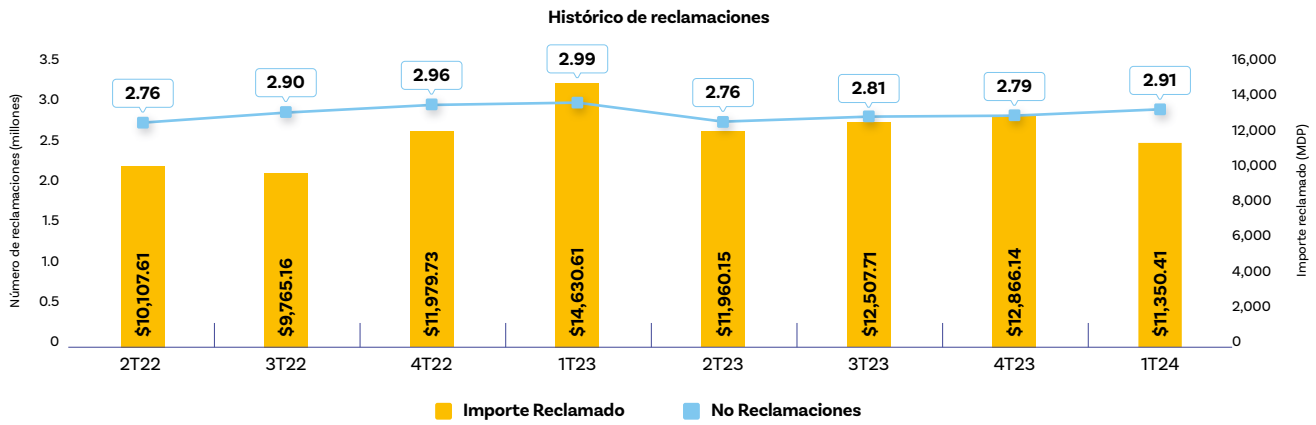
Durante el año 2020, la ABM compartió a este Instituto un listado de 104 posibles casos relacionados con la práctica de SIM SWAPPING, presentados por personas usuarias de servicios financieros y del servicio móvil de los concesionarios AT&T, Movistar y Telcel.

4.6. Comisión Nacional Bancaria y de Valores (CNBV)

La Comisión Nacional Bancaria y de Valores (CNBV) informó que las reclamaciones relacionadas con transferencias no reconocidas y suplantación de identidad pueden derivar en casos de SIM SWAPPING.

A continuación, se muestra un análisis realizado por la CNBV sobre el número de reclamaciones, así como del importe de lo reclamado, entre el segundo trimestre del año 2022 (2T22) y el primer trimestre del año 2024 (1T24).

Gráfica 10.
Histórico de Reclamaciones.

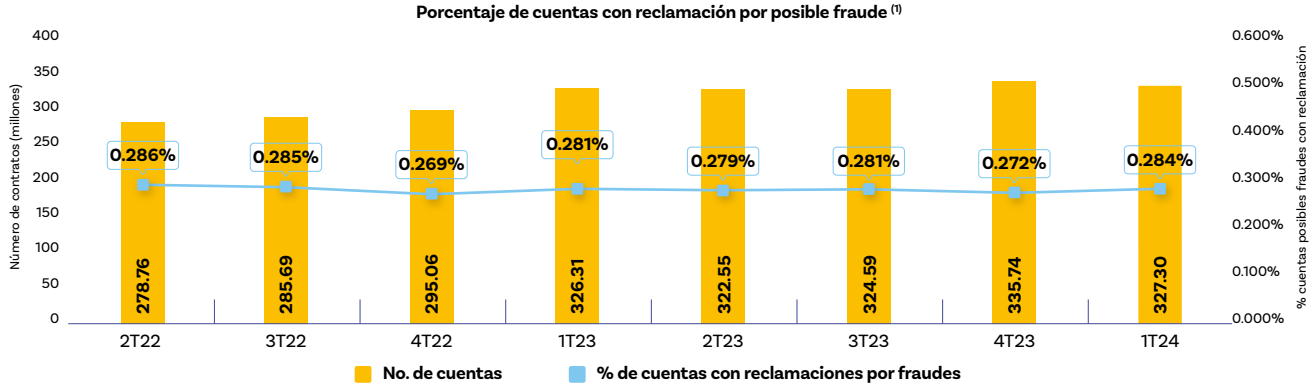


Fuente: Comisión Nacional Bancaria y de Valores.

El número de reclamaciones fluctúa entre 2.76% y 2.99% durante este período, y los montos reclamados presentan una variación significativa, alcanzando un pico de 14,630.61 MDP en el primer trimestre del año 2023 (1T23) y disminuyendo posteriormente a 11,350.41 MDP en el primer trimestre del año 2024 (1T24).

La CNBV señaló que para realizar un análisis de las reclamaciones que pudieran tener relación con algún tipo de fraude, consideró aquellas reclamaciones relacionadas con: cargos no reconocidos, inconformidad por alteración de pagarés, transferencias no reconocidas, retiros no reconocidos, cheques mal negociados y suplantación de identidad. Por otra parte, para realizar un análisis del número de cuentas con reclamación por posible fraude estableció un periodo del segundo trimestre del año 2022 hasta el primer trimestre del año 2024.

Gráfica 11.
Porcentaje de Cuentas con Reclamación por Posible Fraude.



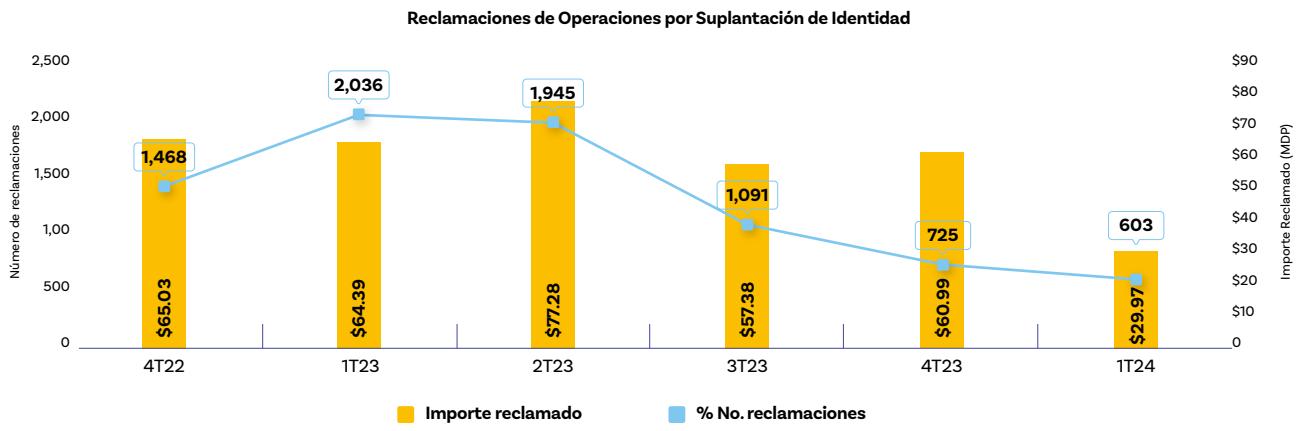
(1) Solo se incluye información de cuentas de depósitos a la vista, valores e instrumentos de inversión, tarjeta de crédito, tarjeta de débito, tarjeta prepagada y cuentas de nómina

Fuente: Comisión Nacional Bancaria y de Valores.

Como se puede observar en el gráfico, el número de cuentas con reclamaciones por posible fraude ha mantenido una tendencia al alza. El porcentaje de cuentas afectadas fluctúa entre el 0.269% y el 0.286%. Este porcentaje es relevante, ya que, a pesar de que para el primer trimestre de 2024 el porcentaje se ubicó en 0.284%, el número de contratos aumentó significativamente: pasó de 278.6 millones en el segundo trimestre de 2022 a 327.3 millones en el primer trimestre de 2024, lo que representa un aumento en el número de cuentas con reclamaciones por fraudes.

La CNBV informó que durante el primer trimestre del año 2024 se registraron 603 reclamaciones por suplantación de identidad y un total de $29.97 millones de pesos reclamados por las operaciones realizadas.

Gráfica 12.
Reclamación de Operaciones por Suplantación de Identidad.



Fuente: Comisión Nacional Bancaria y de Valores

Como se observa en la gráfica, el pico máximo de reclamaciones ocurrió durante el primer trimestre de 2023, mientras que el pico máximo de importe reclamado ocurrió durante el segundo trimestre de 2023 con 77.28 millones de pesos.

Las cifras compartidas por la CNBV sugieren que hay vulnerabilidades en la seguridad de las cuentas que están siendo explotadas y se refuerza la necesidad de implementar medidas preventivas más efectivas para proteger a las personas contra el SIM SWAPPING y otros tipos de fraudes.

Con lo anterior, se puede observar la presencia de casos de SIM SWAPPING en México, su *modus operandi* y la posible incidencia de acuerdo con lo informado por las citadas instituciones. Ante esta situación, es crucial fortalecer los protocolos de verificación de identidad, políticas y medidas de seguridad establecidos por los proveedores de servicios financieros y los proveedores de servicios de telecomunicaciones para enfrentar este tipo de prácticas indebidas de manera efectiva.

5. ACCIONES DE LOS REGULADORES DEL SECTOR DE LAS TELECOMUNICACIONES PARA PREVENIR EL SIM SWAPPING

En el presente apartado se muestra la información que fue brindada a este Instituto por algunos organismos reguladores del sector de las telecomunicaciones, en atención a diversas consultas que fueron formuladas sobre las estrategias emprendidas con el propósito de hacer frente al fenómeno del SIM SWAPPING.

A continuación, se presenta una tabla que detalla los países consultados, el registro y desglose de las respuestas por parte de las autoridades.

Tabla 1.

País	Regulador	Se obtuvo información del regulador
Alemania	Agencia Federal de Redes (BNetzA)	Sí
Brasil	Agencia Nacional de Telecomunicaciones (ANATEL)	Sí
Canadá	Comisión Canadiense de Radio, Televisión y Telecomunicaciones (CRTC)	Sí
Chile	Subsecretaría de Telecomunicaciones (SUBTEL)	Sí
Colombia	Comisión de Regulación de Comunicaciones (CRC)	Sí
España	Comisión Nacional de los Mercados y la Competencia (CNMC)	Sí
Estados Unidos de América	Comisión Federal de Comunicaciones (FCC)	Sí
Reino Unido	Oficina de Comunicaciones (OFCOM)	Sí

A continuación, se detallan las respuestas obtenidas y la información brindada:

5.1. Alemania

5.1.1. Bundesnetzagentur (BNetzA)

La Bundesnetzagentur (en español, Agencia Federal de Redes) es la principal autoridad en materia de infraestructuras y promueve la competencia en los mercados de energía, telecomunicaciones, correos y ferrocarriles para garantizar la eficiencia de las redes. Además, protege los intereses de las personas que utilizan estas redes[17].

De acuerdo con información proporcionada por la agencia, hasta la fecha, la BnetzA no cuenta con normas específicas que asignen al regulador responsabilidades para prevenir el SIM SWAPPING, ni tampoco se han llevado a cabo estadísticas al respecto. No obstante, en los últimos meses, la unidad encargada de combatir el uso indebido de números ha enfrentado un aumento significativo en los casos de SIM SWAPPING.

Dado que los actos pueden constituir presuntamente delitos, corresponde a las autoridades competentes investigar y sancionar dichos actos, por lo que la BnetzA no tiene la responsabilidad ni la autorización para recibir denuncias penales.

En caso de sospecha de un delito, la Bnetza aconseja informar a las autoridades policiales competentes, de acuerdo con el artículo 124 de la Ley Alemana de Telecomunicaciones (TKG). Además, recomienda a los consumidores afectados que denuncien estos casos ante las autoridades policiales.

Como única medida, el operador de redes móviles Vodafone informó recientemente a la Nbetza que ha establecido un tope temporal de 1,000 mensajes de texto al mes para sus clientes, con el fin de limitar los daños, en parte como consecuencia del aumento de los casos de SIM SWAPPING.

5.2. Brasil

5.2.1. Agência Nacional de Telecomunicações (ANATEL)

La Agência Nacional de Telecomunicações (en español, Agencia Nacional de Telecomunicaciones), mencionó que se analiza la práctica de SIM SWAPPING como un tipo de secuestro de línea.

Este fraude implica que un delincuente consigue activar un nuevo chip (tarjeta SIM) utilizando la línea telefónica de la víctima. Ante la sospecha de secuestro de línea, la ANATEL recomienda realizar acciones como:

- Reportar inmediatamente al proveedor de servicios a través de sus canales oficiales.
- Registrar un reporte policial ante la Policía Civil de la Unidad de la Federación correspondiente para proteger a la víctima y colaborar en la identificación de los delincuentes.

El órgano regulador junto con el sector de telecomunicaciones, han implementado medidas para prevenir el SIM SWAPPING, como son:

- **Autenticación en Portabilidad:** Se ha introducido un segundo factor de autenticación en el proceso de portabilidad, que requiere enviar un mensaje de texto al terminal que solicita la portabilidad para confirmar la solicitud. Si no se confirma, la solicitud se cancela.
- **Prevención de Cambio de SIM**: Incluye la validación del consumidor mediante técnicas de biometría facial o de voz.
- **Tecnología Open Gateway:** En el sector financiero, permite verificar si ha habido cambios recientes en la relación entre el número de teléfono del cliente y la tarjeta SIM durante una transacción financiera, lo que ayuda a decidir la aprobación de la transacción.

[17] Bundesnetzagentur (2024). About us. Disponible en: https://www.bundesnetzagentur.de/EN/General/Bundesnetzagentur/AboutUs/start.html

- **Resolución N° 738/2020:** Modifica el Reglamento de Servicios de Telecomunicaciones para incluir medidas contra el fraude y apoyar la seguridad pública. El Artículo 65-M de esta resolución establece que los proveedores deben adoptar medidas técnicas y administrativas necesarias para prevenir, detener y mitigar los efectos de fraudes relacionados con la prestación de servicios de telecomunicaciones. Este artículo también enfatiza que, al implementar acciones coordinadas para combatir el fraude, los costos y beneficios deben ser compartidos entre los proveedores, considerando el tamaño de la empresa.
- **Control de Números Fraudulentos:** Los operadores deben proporcionar información sobre números fraudulentos a las autoridades cuando se les solicite.

5.3. Canadá

5.3.1. Canadian Radio-television and Telecommunications Commission (CRTC)

La Canadian Radio-television and Telecommunications Commission (en español, Comisión Canadiense de Radio, Televisión y Telecomunicaciones) es un organismo administrativo encargado de regular y supervisar la radiodifusión y las telecomunicaciones en Canadá en beneficio del interés público, asegurando que los ciudadanos canadienses tengan acceso a un sistema de comunicaciones de alta calidad que fomente la innovación y mejore su calidad de vida[18].

De acuerdo con información proporcionada por la Comisión, hasta el momento, no existen mandatos regulatorios por parte de la CRTC que obliguen a los proveedores de servicios de telecomunicaciones (TSP, por sus siglas en inglés) a implementar medidas contra el intercambio de SIM.

Sin embargo, la CRTC tiene las siguientes funciones:

1. Recopila datos cuantitativos y cualitativos sobre el número de incidentes de intercambio de SIM superiores a un umbral y
2. Pide a cada uno de los proveedores de servicios inalámbricos que presenten estadísticas mensuales sobre el número de intercambios fraudulentos de SIM detectados.

En julio de 2021, la CRTC dijo públicamente que *"hubo una disminución del 95% en el número total de transferencias no autorizadas de números de teléfonos móviles e intercambios de SIM desde octubre de 2020 hasta mayo de 2021"*[19]. Sin embargo, en virtud de la Sección 38 de la Ley de Telecomunicaciones de Canadá[20], las estadísticas sobre SIM SWAPPING son de carácter confidencial y no pueden ser divulgadas.

Como medida para abordar el fraude de SIM SWAPPING, la CRTC ha solicitado a los TSP la implementación de soluciones efectivas. Estos proveedores han colaborado con socios en la industria de las telecomunicaciones de Canadá para establecer un protocolo común. Sin embargo, la información del protocolo es de carácter confidencial; toda vez que su divulgación podría ayudar a estafadores a evadir cualquier nueva medida de seguridad y permitirles desarrollar nuevas técnicas para perjudicar a los consumidores canadienses.

Asimismo, se informó que es responsabilidad de cada TSP identificar y reportar estos incidentes, y deben implementar protocolos y procedimientos para prevenir la recurrencia del intercambio de SIM, abordando las causas subyacentes.

[18] CRTC (2024). About us. Disponible en: https://crtc.gc.ca/eng/acrtc/org.htm

[19] CRTC (8 de julio de 2021). Telecom Commission Letter addressed to the Distribution List, expedient 8665-C12-202000280. Disponible en: https://crtc.gc.ca/eng/archive/2021/lt210708.htm

[20] Telecommunications Act [S.C. 1993, c. 38], Act current to 2024-05-14 and last amended on 2023-06-22. Consolidated Acts, Justice Laws Website.

5.4. Chile

5.4.1. Subsecretaría de Telecomunicaciones (SUBTEL)

La SUBTEL es un órgano dependiente del Ministerio de Transportes y Telecomunicaciones que se encarga de coordinar, promover, fomentar y desarrollar las telecomunicaciones en Chile, para transformar a este sector en motor para el desarrollo económico y social de la nación[21].

Con información proporcionada por SUBTEL y la revisión de otras fuentes de información, el 26 de julio de 2022, la SUBTEL y la Subsecretaría de Prevención del Delito (SPD) en conjunto con la Policía de Investigaciones (PDI), dieron a conocer las medidas[22] del Gobierno para contrarrestar las prácticas fraudulentas en telefonía, como el SIM SWAPPING, el phishing o las estafas por medio de llamadas.

El plan incluye tres ejes:

- **Acción:** Introducir una serie de normativas por parte de la SUBTEL para mejorar los protocolos de transacción entre las empresas y los usuarios, utilizando parámetros biométricos;
- **Fiscalización:** Constante fiscalización de los protocolos de las empresas de telecomunicaciones, evitando que la información personal de los usuarios esté en riesgo, y
- **Prevención:** Entregar a los usuarios una serie de recomendaciones para que puedan identificar los diferentes tipos de estafas a través de canales masivos de información.

Asimismo, la SUBTEL a través de la modificación al artículo 15° del decreto del supremo Nº 18 de 2014 que aprueba el reglamento de servicios de telecomunicaciones otorga la facultad a la SUBTEL para "*establecer estándares de seguridad, con protocolos o factores de autentificación mínimos que deberán cumplir los proveedores de servicios de telecomunicaciones con el objeto de verificar la identidad inequívoca de las partes, tales como preguntas de validación, biometría, certificados de firma electrónica avanzada, entre otros*"[23].

De esta forma, el pasado 6 de abril de 2024, se promulgaron los "Requisitos mínimos de verificación de identidad y estándares de seguridad aplicables por proveedores de servicios de telecomunicaciones en los casos indicados"[24], resolviéndose lo siguiente:

> *"Artículo 1°. La presente norma aplicará a los procesos llevados a cabo por proveedores de servicios de telecomunicaciones, con motivo de la celebración, modificación y término de los contratos, así como otros actos que puedan traducirse en obligaciones a interesados o suscriptores, tales como venta y entrega de equipos y activación de tarjetas SIM.*

[21] SUBTEL (2024). Que es SUBTEL. Disponible en: https://www.subtel.gob.cl/quienes-somos/

[22] SUBTEL (26 de julio de 2022). Gobierno presenta plan de acción para enfrentar estafas telefónicas ante aumento sostenido de delitos asociados. Sala de Prensa. Disponible en: https://www.subtel.gob.cl/gobierno-presenta-plan-de-accion-para-enfrentar-estafas-telefonicas-ante-aumento-sostenido-de-delitos-asociados/

[23] Artículo 15°(c), modificado por el Decreto 46 [Decreto 46, 15/junio/2023] que modifica el Decreto N.º 18, de 2014, que aprueba reglamento de servicios de telecomunicaciones que indica [Decreto 18, 13/febrero/2014] Ministerio de Transportes y Telecomunicaciones; Subsecretaría de Telecomunicaciones, 09/enero/2014, República de Chile.

[24] Resolución 566 exenta (06/abril/2024) [Ministerio de Transportes y Telecomunicaciones; Subsecretaria de Telecomunicaciones]. Por la cual se establece requisitos mínimos de verificación de identidad y estándares de seguridad aplicables por proveedores de servicios de telecomunicaciones en los casos indicados, República de Chile.

Artículo 2°. La celebración, modificación y término de los contratos de los servicios, así como la activación de tarjetas SIM y la venta de equipos, en la medida que el cobro de este último se efectúe en el documento de cobro emitido por su proveedor, deberá realizarse, contemplando al menos uno de los siguientes estándares de seguridad para efectos de la validación de identidad, sin importar el canal de atención utilizado (presencial, telefónico o virtual):

a) Solicitar la cédula de identidad del solicitante y verificar la identidad de éste mediante biometría de huella dactilar viva, capturándola y comparándola con la huella registrada por el Servicio de Registro Civil e Identificación.

b) Verificar la identidad del solicitante mediante biometría facial, validando la coincidencia entre la captura de la fotografía de la cédula de identidad y el rostro escaneado, efectuando prueba de detección de vida y descartando la suplantación hecha con, a lo menos: fotos, videos, cambio de imágenes, proyección de videos o máscaras.

El resultado de la verificación biométrica debe ingresar en forma automática en el sistema comercial del proveedor del servicio, sin intervención de personas, y sólo el resultado correcto de la verificación permitirá continuar con la solicitud.

Artículo 3°. Tratándose de la actuación a través de terceros que representen al interesado o suscriptor, se estará a la aplicación de las reglas generales al respecto, recayendo en la proveedora la responsabilidad de verificar, conforme a lo anterior, la identidad del representante y su capacidad de representar al interesado o suscriptor. La validación de identidad se realizará de acuerdo a los métodos señalados precedentemente.

Si la solicitud es efectuada por alguien quien, debido a un robo, hurto o extravío no cuenta con su cédula de identidad, se debe requerir el comprobante de bloqueo expedido por el Servicio de Registro Civil e Identificación y el comprobante de denuncia ante Carabineros de Chile, Policía de Investigaciones de Chile o Ministerio Público, en caso de hurto o robo de la cédula de identidad, y se aplicará al menos uno de los estándares de seguridad del artículo 2º de la presente resolución utilizando para tales efectos el pasaporte o algún otro documento oficial...

Artículo 4°. La entrega de equipos a domicilio a un solicitante o a un tercero autorizado por éste, se hará en la dirección indicada al momento de la venta. Se deberá verificar que los datos de la cédula de identidad de quien recibe, coincide con los del solicitante o del tercero autorizado, indicados en la venta, obteniendo, además, un registro fotográfico de la entrega.

Artículo 5°. La activación de la tarjeta SIM asociada al servicio se efectuará luego de cumplido alguno de los requisitos indicados en el artículo 2º, y se registrará en el sistema de la concesionaria, los datos de identificación de éste y otros que se requieran para la provisión del servicio.

Artículo 6°. La externalización o subcontratación de actividades a terceros por parte de los proveedores de servicios de telecomunicaciones, no liberará de responsabilidad en el cumplimiento de las obligaciones establecidas en la presente norma, respecto de sus suscriptores o usuarios ni respecto de esta Subsecretaría, así como tampoco aquellas que correspondan en el ámbito civil o penal, de ser el caso."

5.5. Colombia

5.5.1. Comisión de Regulación de Comunicaciones (CRC)

La CRC es el órgano responsable de fomentar y regular la competencia justa, así como de prevenir prácticas desleales. Asimismo, supervisa el acceso y uso de todas las redes, así como el ingreso a los mercados de los servicios de telecomunicaciones, televisión abierta y radiodifusión sonora[25].

En atención a las consultas formuladas, se informó que la CRC no tiene atribuciones para realizar labores de vigilancia, inspección y control, ni tiene normativas específicas para abordar el SIM SWAPPING o tomar acciones legales contra quienes la realizan. No obstante, lo anterior, en el artículo 2.1.10.7 de la Resolución 5111 de 2017[26] en la que se modifica el Capítulo 1 del Título II de la Resolución CRC 5050 de 2016, se establece que:

- Es responsabilidad de los operadores utilizar herramientas tecnológicas apropiadas para evitar fraudes dentro de sus redes, y realizar controles regulares para evaluar la eficacia de dichos mecanismos, y
- Cuando un usuario presente una PQR (petición/queja/reclamo) que pueda estar relacionada con un posible fraude, el operador está obligado a investigar las causas. Si determina que no existe fraude, debe explicar al usuario las razones de dicha conclusión. Sin embargo, si se demuestra que el usuario actuó diligentemente en el uso del servicio contratado, no se le cobrarán los consumos objeto de la reclamación.

Por su parte, en la resolución No. 7151 de 2023[27] se modificaron las disposiciones del régimen de Portabilidad Numérica Móvil definidas en el Capítulo 6 del Título II de la Resolución CRC 5050 de 2016, debido a que existían dificultades para validar la titularidad en el proceso de portación. Entre los cambios efectuados, a continuación, se mencionan los principales:

1. El proveedor debe solicitar un NIP como requisito indispensable para autenticar la condición de Usuario del número a ser portado, a través del envío de una SMS que diga "*Su Código NIP es xxxxx y es personal. Se usará para pasar su línea xxxxxxxxxx a (nombre comercial del PRST receptor). Si no solicitó este cambio, contacte a su proveedor de inmediato*".
2. En la solicitud de portación, el usuario debe proporcionar el NIP de confirmación para los usuarios de servicios móviles.
3. El proveedor debe llevar a cabo una verificación de la solicitud, la cual incluirá la revisión del NIP de confirmación y su coincidencia con el número no geográfico de las redes sujetas a portación.
4. La solicitud será rechazada si los datos del documento de identificación del solicitante, como la fecha de expedición y el número del documento, no coinciden con los del titular de la línea. Además, si el titular niega haber solicitado el proceso de portación, este deberá detenerse de inmediato, sin importar en qué etapa se encuentre.

[25] CRC (2024). Misión, visión, funciones y deberes. Disponible en: https://www.crcom.gov.co/es/transparencia-y-acceso-a-la-informacion-publica/informacion-de-la-entidad/mision-vision-funciones-y-deberes#cont

[26] Artículo 2.1.10.7. Prevención de Fraudes, por la cual se establece el Régimen de Protección de los Derechos de los Usuarios de Servicios de Comunicaciones, se modifica el Capítulo 1 del Título II de la Resolución CRC 5050 de 2016 y se dictan otras disposiciones. Diario Oficial No. 50.157 de 24 de febrero de 2017.

[27] Artículo 2.6.4.2. NIP de confirmación, Resolución No. 7151 DE 2023 "Por la cual se modifican disposiciones del régimen de Portabilidad Numérica Móvil definidas en el Capítulo 6 del Título II de la Resolución CRC 5050 de 2016 y se dictan otras disposiciones".

5.6. España

5.6.1. Comisión Nacional de los Mercados y la Competencia (CNMC)

La CNMC es el organismo encargado de fomentar y preservar el correcto funcionamiento de todos los mercados en beneficio de consumidores y de las empresas. Su objetivo es asegurar, preservar y fomentar el funcionamiento, la transparencia y la existencia de competencia efectiva en todos los mercados y sectores productivos, en beneficio de consumidores y usuarios.[28]

Actualmente, en atención a las consultas formuladas, la CNMC no posee competencias directas sobre este asunto y no ha adoptado ninguna decisión al respecto, por lo que carece de estadísticas relacionadas sobre el SIM SWAPPING. Aunque la CNMC está facultada para resolver conflictos entre operadores en casos de tráficos irregulares en las redes o uso indebido de la numeración, no ha intervenido en conflictos vinculados a prácticas de SIM SWAPPING de las que haya tenido conocimiento.

5.7. Estados Unidos de América

5.7.1. Federal Communications Commission (FCC)

La Federal Communications Commission (en español, Comisión Federal de Comunicaciones) es un órgano autónomo responsable de implementar y hacer cumplir las leyes y regulaciones de comunicaciones de los Estados Unidos de América y regula las comunicaciones interestatales e internacionales por radio, televisión, cable, satélite y cable[29].

De acuerdo con información proporcionada por la Comisión, en septiembre de 2021, la FCC adoptó un Aviso sobre el fraude de intercambio y transferencia de SIM[30], proponiendo modificar las reglas de la Información de Red Propiedad del Cliente (CPNI, por sus siglas en inglés)[31] y la Portabilidad de Número Local (LNP, por sus siglas en inglés) únicamente para los Proveedores de Servicio de Radio Móvil comercial (CMRS, por sus siglas en inglés). Con estas reglas se pretende crear un marco uniforme en toda la industria inalámbrica móvil para los tipos de políticas y procedimientos que los proveedores deben emplear para combatir el fraude de SIM SWAPPING. Además, se busca brindar flexibilidad a los CMRS para que establezcan medidas específicas de protección contra el fraude, permitiéndoles ofrecer las protecciones más avanzadas disponibles.

En términos generales, las nuevas reglas para los CMRS son las siguientes:

1. Utilizar métodos seguros para autenticar a los clientes antes de realizar cambios de SIM y puertos numéricos;
2. Implementar procesos para responder a intentos fallidos de autenticación, capacitación obligatoria para empleados sobre el manejo de intercambio de SIM, fraude de transferencia y el establecimiento de salvaguardas para prevenir que empleados accedan a la CPNI hasta que los clientes hayan sido autenticados;
3. Notificar a los clientes sobre cambios de SIM y solicitudes de transferencia, ofreciendo a los clientes la opción de bloquear sus cuentas para evitar el procesamiento de SIM, cambios y la portabilidad de números. Asimismo, informar a los clientes sobre los mecanismos de protección de cuentas disponibles con anticipación;

[28] CNMC (2024). Qué es la CNMC. Disponible en: https://www.cnmc.es/sobre-la-cnmc/que-es-la-cnmc

[29] FCC (2024). About the FCC. Disponible en: https://www.fcc.gov/about/overview

[30] FCC (Nov 16, 2023). In the Matter of Protecting Consumers from SIM Swap and Port-Out Fraud. Bureau Wireline Competition. Disponible en: https://www.fcc.gov/document/fcc-adopts-rules-protect-consumers-cell-phone-accounts-0

[31] Se refiere a los datos sobre el uso de los servicios de telecomunicaciones proporcionados por los clientes a los operadores. Abarca información como los números de teléfono llamados, la frecuencia, duración y horario de las llamadas, y los servicios adquiridos, como la llamada en espera.

4. Mantener un proceso claro para que los clientes informen el fraude, realizar investigaciones y remediar rápidamente el fraude, así como proporcionar rápidamente a los clientes documentación del fraude relacionado con sus cuentas, y
5. Llevar un registro de las solicitudes de cambio de SIM y las medidas de autenticación que utilizan.

Adicionalmente, es importante destacar que el artículo 222 de la Ley de Comunicaciones de 1934[32], obliga a los operadores de telecomunicaciones a proteger la privacidad y seguridad de la información sobre sus clientes a la que tienen acceso. La Sección 222(c) establece que un proveedor de servicios de telecomunicaciones solo puede usar, compartir o permitir el acceso a la información personal del cliente cuando lo exige la ley, con la aprobación del cliente y en la provisión del servicio de telecomunicaciones o en servicios necesarios para brindar dicho servicio.

Ante la evolución de la telefonía móvil y el aumento de los fraudes, la FCC ha actualizado sus normas para proteger la CPNI:

1. En 1998, promulgó por primera vez normas para aplicar las obligaciones legales expresadas en la Sección 222, imponiendo restricciones sobre el uso y divulgación de la CPNI, además de establecer salvaguardas para protegerla contra el uso o divulgación no autorizados de la misma[33].
2. En 2007, modificó sus normas para abordar el "pretexto"[34], restringiendo la divulgación de las llamadas e imponiendo requisitos de contraseña para acceder a la cuenta. Asimismo, se exigió a los operadores autenticar adecuadamente tanto a los clientes nuevos como a los existentes que buscan acceder a CPNI en línea. Además, el Congreso adoptó prohibiciones penales tanto para la obtención de CPNI de un operador de telecomunicaciones como para la venta, transferencia, compra o recepción de CPNI obtenida fraudulentamente[35].

5.8. Reino Unido

5.8.1 Office of Communications (OFCOM)

La Office of Communications (en español, Oficina de Comunicaciones) es el órgano encargado de regular los servicios de telecomunicaciones. Se encarga de que los ciudadanos del Reino Unido obtengan lo mejor de los servicios de banda ancha, teléfono residencial y móviles, además de estar atentos a la televisión y a la radio. Supervisa el servicio postal universal, cuida las ondas de radio y también ayuda a garantizar que las personas no sean estafadas y estén protegidas de malas prácticas[36].

De acuerdo a la información proporcionada por el regulador, la OFCOM aún no ha realizado un análisis significativo sobre SIM SWAPPING. Sin embargo, ha tomado acciones sobre el intercambio de tarjetas SIM para hacer frente a las llamadas y mensajes de texto fraudulentos a través de publicaciones sobre las verificaciones de identidad que los operadores de redes móviles (OMR) y virtuales (OMV) deben llevar a cabo para facilitar el cambio o la portabilidad de números.

[32] 47 U.S.C. § 222. Véase también Aplicación de la Ley de Telecomunicaciones de 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, et al., CC Docket Nos. 96-115.

[33] Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of CustomerProprietary Network Information and Other Customer Information; IP-Enabled Services, CC Docket No. 96-115, WC Docket No. 04-36, 22 FCC Rcd 6927, 6931, pag. 5 (2007).

[34] Es un esquema en el que un mal actor se hace pasar por un cliente autorizado para acceder a los detalles de las llamadas o a otros registros de comunicaciones privadas.

[35] Telephone records and privacy protection act of 2006, Pub. L. 109-476, 120 Stat. 3568 (2007) (codification an 18 USC § 1039).

[36] OFCOM (24 de junio de 2010). What is Ofcom? Disponible en: https://www.ofcom.org.uk/about-ofcom/what-we-do/what-is-ofcom/

De lo reportado por OFCOM se menciona que, un cliente debe ser debidamente verificado antes de recibir el código de autorización de portabilidad (PAC, por sus siglas en inglés), el cual es necesario para cambiar de proveedor de telefonía móvil manteniendo su número actual.

Aunque existe un requisito de completar el cambio en un minuto, los operadores de redes móviles y los operadores móviles virtuales pueden "detener el reloj" para realizar las verificaciones necesarias.

5.8.2. Carta del sector del fraude: telecomunicaciones

Frente a la creciente amenaza de fraudes a gran escala en Reino Unido, los proveedores de telecomunicaciones y el Gobierno Británico, a través del Ministerio del Interior, trabajan de manera coordinada con otras industrias y partes interesadas para reducir su impacto. Por lo anterior, se implementó la Carta Sectorial[37] en la que se incluyen las soluciones ejecutadas por los proveedores de telecomunicaciones para reducir el fraude y las estafas, en la cual se ajustarán a las obligaciones legales y reglamentarias de los proveedores, incluso en relación con la protección de datos. En particular, abordan el SIM SWAPPING en la acción 4:

> "***Acción 4. Uso de verificación en tiempo real para abordar el fraude en el intercambio de SIM y la portabilidad de números móviles.***
>
> ***Objetivo.*** *Permitir que se reduzca el fraude mediante un esfuerzo coordinado de la industria de las telecomunicaciones y la banca.*
>
> ***Acción.*** *La industria de las telecomunicaciones continuará respaldando a la industria bancaria al ofrecer una verificación en tiempo real constante para determinar si un teléfono móvil ha sufrido un cambio de tarjeta SIM o de operador utilizando el estándar de seguridad de cuenta Mobile Connect de GSMA, el cual es compatible con todos los proveedores.*
>
> *Los proveedores de servicios de telecomunicaciones colaborarán con UK Finance para asegurarse de que la industria bancaria esté completamente informada sobre los datos de SIM-Swap/MNP disponibles y para investigar otros datos/servicios que los proveedores puedan ofrecer para disminuir este tipo de fraude.*
>
> ***Resultado.*** *Reducir el riesgo de fraude de intercambio de SIM y MNP.*
>
> *Implementar 3 meses – 1 año."*

De las consultas formuladas a los reguladores del sector de telecomunicaciones, se ha evidenciado que el fenómeno del SIM SWAPPING se encuentra presente en distintos países y ha generado un impacto negativo y significativo en distintos sectores de la sociedad. Además, ha demostrado ser una amenaza creciente para la seguridad de los datos personales y financieros de los usuarios.

Por lo anterior, aunque no en todas las autoridades regulatorias el fenómeno de SIM SWAPPING es parte de su jurisdicción, se han implementado diversas acciones destinadas a erradicar o disminuir esta problemática, mismas que han consistido en la emisión de disposiciones normativas para definir los procedimientos para la sustitución de tarjetas SIM, mecanismos de autenticación y de información para las personas usuarias cuando se realice este tipo de solicitudes. Asimismo, se han establecido recomendaciones para que las personas puedan actuar cuando se haya efectuado este tipo de solicitudes sin su consentimiento y para que se mantenga un registro de las solicitudes de sustitución de tarjeras SIM, entre otras.

Finalmente, se ha advertido que las actividades de sensibilización e información a la población sobre esta problemática han sido fundamentales para prevenir su materialización.

[37] Gobierno de Reino Unido (2019). *Carta del sector del fraude: telecomunicaciones.* Actualizado el 21 de noviembre de 2022. Disponible en: https://www.gov.uk/government/publications/joint-fraud-taskforce-telecommunications-charter/fraud-sector-charter-telecommunications-accessible-version

6. CAMBIO DE TARJETA SIM EN MÉXICO

Actualmente, los concesionarios y autorizados para prestar el servicio móvil en México cuentan con diversos sistemas de atención a personas usuarias, físicos o electrónicos, a través de los cuales atienden las solicitudes de servicio, trámites, aclaraciones o quejas por parte de sus usuarios o suscriptores.

En algunas ocasiones, los concesionarios y autorizados atienden las quejas, solicitudes de servicio o trámites de las personas usuarias a través de algún sistema de atención específico, dependiendo de la naturaleza de estos y los requisitos para efectuarlos.

Asimismo, los concesionarios y autorizados habilitan la posibilidad de que las personas usuarias o suscriptores realicen algunas peticiones de servicio o trámites a través de sus puntos de distribución o aquellos que son operados por terceros.

En este sentido, resulta importante conocer los sistemas de atención por medio de los cuales las personas pueden solicitar una nueva tarjeta SIM asociada a un número telefónico, los requisitos y los mecanismos para validar la identidad de las personas solicitantes.

De un análisis a la información que los principales concesionarios y autorizados para prestar el servicio móvil compartieron con este Instituto se puede advertir lo siguiente:

6.1. Sistema de atención a través de los cuales se puede solicitar el cambio de una tarjeta SIM.

La mayoría de los concesionarios y autorizados señalan que la solicitud de la tarjeta SIM debe realizarse de manera presencial en los centros de atención y en algunos casos, se menciona que dicha solicitud también puede realizarse a través de los puntos de distribución; sin embargo, no se señala si las solicitudes se pueden realizar a través de los puntos de distribución propios u operados por terceros.

Asimismo, existen algunos casos en los que dichas solicitudes pueden ser formuladas a través de la página de internet del concesionario o autorizado, o vía WhatsApp.

6.2. Requisitos para solicitar el cambio de una tarjeta SIM.

Del análisis a la información con la que cuenta este Instituto, se puede advertir que los requisitos que se le solicitan a las personas usuarias varían dependiendo del concesionario o autorizado, así como del esquema de contratación, prepago o pospago.

A continuación, se mencionan los requisitos generales que se identificaron:

Prepago:

- Apersonarse en los Centros de Atención a Clientes, ingresar a página electrónica o solicitar vía electrónica el inicio de la solicitud.
- Presentar una identificación oficial.
- Atender preguntas de seguridad sobre la actividad de la línea.

Pospago:

- Apersonarse en los Centros de Atención a Clientes, ingresar a página electrónica o solicitar vía electrónica el inicio de la solicitud.
- Presentar una identificación oficial.
- Atender preguntas de seguridad sobre la actividad de la línea.
- Autenticación mediante Datos Biométricos.

6.3. Mecanismos de Verificación de Identidad del Solicitante.

Así como los requisitos para solicitar el cambio de una tarjeta SIM, los procedimientos utilizados para verificar la identidad de los solicitantes varían atendiendo al concesionario o autorizado, y el esquema de contratación.

A continuación, se mencionan los mecanismos generales identificados:

Prepago:

- Presentar una identificación oficial.
- Atender preguntas de seguridad sobre la actividad de la línea.

Pospago:

- Presentar una identificación oficial.
- Autenticación mediante Datos Biométricos o Preguntas de Seguridad.
- Notificación de solicitud de tarjeta SIM.

6.4. Notificación de solicitud de tarjeta SIM.

Del análisis a la información proporcionada por los concesionarios y autorizados, se ha detectado que solo algunos de estos envían notificaciones automáticas a la persona usuaria mediante SMS y/o correo electrónico sobre la solicitud y el proceso de reemplazo de la tarjeta SIM.

Las notificaciones permiten a las personas usuarias estar informadas de los pasos que deben seguir, el estado de su solicitud y de cualquier requerimiento adicional que pueda surgir durante el proceso de reemplazo, fortaleciendo así la confianza en el servicio y asegurando una mejor experiencia.

6.5. Medidas preventivas adoptadas por los concesionarios y autorizados para prestar el servicio móvil.

Las medidas preventivas adoptadas por los concesionarios y autorizados para garantizar la calidad y seguridad del servicio móvil incluyen:

Métodos de autenticación: Se requiere que las personas usuarias presenten identificación oficial y, en algunos casos, realicen autenticación biométrica durante el proceso de solicitud de reemplazo de SIM.

Preguntas de seguridad: Para las líneas no personalizadas, se aplican preguntas de seguridad relacionadas con el uso habitual de la línea para validar la identidad del usuario.

Monitoreo continuo: Se implementan procesos de monitoreo constante para identificar y gestionar actividades sospechosas o intentos de fraude.

Capacitación del personal: Los empleados reciben formación continua para manejar las solicitudes de los usuarios de manera efectiva y prevenir posibles fraudes.

Notificaciones a los usuarios: Se utilizan SMS y correos electrónicos para informar a los usuarios sobre el estado de sus solicitudes y cualquier cambio relevante en su cuenta.

Desactivación de líneas con reporte de robo o extravío: En caso de reportes de SIM robadas o perdidas, se procede a la desactivación inmediata de la línea afectada hasta que se verifique la identidad del usuario.

Plazos de espera: Se establece un periodo de gracia para el cambio de SIM, durante el cual se evita la asignación inmediata de un número a un nuevo dispositivo, permitiendo la verificación adecuada.

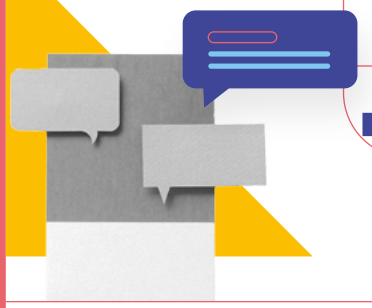
Facultad del usuario: Los titulares de líneas tienen la opción de notificar y corregir errores relacionados con la suplantación de identidad, asegurando su derecho a la protección de sus datos.

Como se puede advertir, actualmente los concesionarios o autorizados permiten a las personas usuarias solicitar un cambio o sustitución de tarjeta SIM en sus propios sistemas de atención presenciales donde han establecido mecanismos para la verificación de la identidad de los solicitantes. Sin embargo, también se pueden realizar dichas solicitudes en puntos de distribución propios u operados por terceros y, en algunos casos, los autorizados permiten que se realicen por páginas de internet o vía plataformas digitales de mensajería.

Lo anterior resulta relevante, si consideramos que los concesionarios o autorizados se encuentran obligados a contar en sus sistemas de atención con personal capacitado para la debida atención de las personas usuarias. Respecto a los mecanismos de autenticación, algunos concesionarios han informado que implementaron la autenticación por medio de los datos biométricos, a fin de prevenir un acceso indebido a los datos personales de las personas usuarias.

Sin embargo, cuando no se cuenta con datos personales de la persona usuaria, algunos concesionarios y autorizados realizan la autenticación de la misma por medio de preguntas de seguridad que ayudan a confirmar la identidad del solicitante. Por otra parte, los concesionarios y autorizados informaron que notifican a los usuarios mediante correo electrónico y SMS cuando se realiza una solicitud de cambio o sustitución de tarjeta SIM. Esta medida es especialmente relevante en los casos en los que la solicitud no proviene del titular de la línea, ya que permite a este tomar medidas inmediatas para evitar suplantaciones de identidad y cambios no autorizados. La información que reciben los usuarios es esencial para actuar ante situaciones no consentidas. En este sentido, los concesionarios y autorizados mencionan que utilizan notificaciones para mantener a las personas usuarias informadas sobre el estado de sus solicitudes y prevenir posibles fraudes.

Como se observa, se ha adoptado un enfoque particular para prevenir el SIM SWAPPING, compartiendo algunas estrategias como la verificación de identidad y autenticación biométrica para el cambio o reposición de tarjetas SIM. Las notificaciones proactivas y el uso de preguntas de seguridad para las personas usuarias en prepago son prácticas comunes que ayudan a detectar y prevenir fraudes. Sin embargo, es importante reconocer las limitaciones de las preguntas de seguridad, ya que pueden ser menos eficaces por la posibilidad de que otras personas conozcan la información solicitada, lo que puede comprometer la efectividad de este método.



7. CONCLUSIONES

El avance tecnológico y el incremento en el uso de las tecnologías de la información y comunicación conlleva el desafío de que las personas estén mejor informadas y preparadas para enfrentar los riesgos de ser víctimas de algún delito cibernético.

En este sentido, el fraude es un delito en aumento, que se ha ido trasladando a la esfera de los delitos cibernéticos, donde por las dificultades de la verificación a través de medios digitales, permite que se cometan distintas modalidades de fraude relacionados con la suplantación de identidad. Una de estas modalidades de suplantación de identidad es el SIM SWAPPING, el cual a su vez abre la posibilidad a la comisión de una gran variedad de delitos en perjuicio de las personas usuarias, de su privacidad y de su patrimonio.

Respecto a la información sobre los procesos que cada concesionario o autorizado reportó, se ha observado la implementación de diversos mecanismos para prevenir el SIM SWAPPING, utilizando estrategias orientadas a mejorar la seguridad de las personas usuarias y mitigar riesgos de manera efectiva durante el proceso de cambio o reposición de tarjetas SIM.

Dentro de las estrategias mencionadas se encuentran:

- **Verificación de Identidad:** Realizada a través de la presentación de una identificación oficial por parte de las personas usuarias al momento de solicitar el cambio o reposición de su tarjeta SIM.
- **Notificaciones Proactivas:** Enviadas a los métodos de contacto registrados de la persona usuaria, como correo electrónico o mensajes SMS a otros números registrados. Estas notificaciones alertan a las personas usuarias sobre intentos de cambio de SIM, permitiéndoles tomar medidas antes de que cualquier cambio se efectúe.

Por otro lado, se identificó que las preguntas de seguridad pueden ser menos efectivas para mitigar el SIM SWAPPING. Su efectividad puede comprometerse por la posibilidad de que otras personas conozcan la información solicitada por el asesor de la operadora o se obtenga mediante métodos de ingeniería social, redes sociales, u otras fuentes públicas.

Para mejorar la efectividad de las preguntas de seguridad, se ha recomendado:

- **Utilizar preguntas menos obvias** que no estén relacionadas con información pública fácilmente accesible.
- **Actualizar las preguntas y respuestas regularmente** para reducir la probabilidad de que sean conocidas por otras personas.
- **Complementarlas con otros métodos de autenticación**, como la verificación en dos pasos (2FA) que utilice aplicaciones de autenticación.
- **Mejorar continuamente los procesos**, adaptando las medidas de seguridad según evoluciona la amenaza del SIM SWAPPING.

Adicionalmente, es crucial alfabetizar a las personas usuarias sobre los posibles riesgos y proporcionarles información clara sobre las medidas que deben tomar para protegerse contra fraudes y robos de identidad.

Como se señala, el SIM SWAPPING, se realiza a través de varias mecánicas de ingeniería social y tecnologías de la información, por lo tanto, se combinan diversos actos que evidencian que nuestra legislación queda rebasada.

Por ello, es necesario implementar buenas prácticas en capacitación, ciberseguridad y alfabetización digital dirigida a proveedores de servicios de telefonía móvil y a su personal, así como difundirlas a las personas usuarias, a través de instituciones gubernamentales y los mismos proveedores de telefonía móvil.

El SIM SWAPPING es un problema relativamente nuevo que, derivado de las consultas hechas a algunos reguladores del sector de las telecomunicaciones a nivel internacional, se puede observar que aún no cuentan con una normativa específica sobre el cambio de tarjetas SIM, a pesar de su incremento. Algunos reguladores consideran el SIM SWAPPING como un delito, lo cual limita su capacidad para sancionar esta actividad. Por ello, se han apoyado en distintas instituciones gubernamentales para recibir asesoramiento sobre las medidas a tomar para prevenir este tipo de fraude.

Finalmente, se considera importante observar las acciones ejecutadas por aquellos reguladores que sí cuentan con una normativa específica para el cambio de tarjetas SIM, en donde se han implementado medidas estrictas e impuesto obligaciones a los prestadores de servicios móviles para la implementación de mecanismos efectivos para garantizar la seguridad en los procedimientos de cambios de tarjeta SIM.

De esta manera, consideramos relevante tomar como ejemplo las buenas prácticas para implementar acciones regulatorias destinadas a erradicar o, en su defecto, mitigar esta problemática del SIM SWAPPING en nuestro país, así como establecer métodos y mecanismos que permitan dar seguimiento a la incidencia de este tipo de prácticas.

GLOSARIO Y ACRÓNIMOS

- **ABM.** Asociación de Bancos de México
- **BfDI.** Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
- **CDETECH.** Consejo de Datos y Tecnologías Emergentes
- **CGPU.** Coordinación General de Política del Usuario
- **CMRS.** Commercial Mobile Radio Service
- **CNMC.** Comisión Nacional de los Mercados y la Competencia
- **CONDUSEF.** Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros
- **CPNI.** Customer Proprietary Network Information
- **CRC.** Comisión de Regulación de Comunicaciones
- **CRTC.** Canadian Radio-television and Telecommunications Commission
- **ENVIPE.** Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública
- **FCC.** Federal Communications Comission
- **GN.** Guardia Nacional
- **IA.** Inteligencia Artificial
- **INAI.** Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
- **INEGI.** Instituto Nacional de Estadística y Geografía
- **LFPDPPP.** Ley Federal de Protección de Datos Personales en Posesión de los Particulares
- **LNP.** Local Number Portability
- **PDI.** Policía de Investigaciones
- **PORI.** Posible Robo de Identidad
- **SESNSP.** Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública
- **SPD.** Subsecretaría de Prevención del Delito
- **SSC.** Secretaría de Seguridad Ciudadana de la Ciudad de México
- **SUBTEL.** Subsecretaría de Telecomunicaciones
- **TUO.** Texto Único Ordenado
- **TSP.** Telecommunications Service Providers

REFERENCIAS

Alday, Barco, Carbonell et. al. (2019). *Diccionario de Protección de Datos Personales. Conceptos fundamentales.* Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), Primera edición, México, pág. 240, ISBN: 978-607-98648-3-5. Disponible en: https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/DICCIONARIO_PDP_digital.pdf

Artículo 2.1.10.7. Prevención de Fraudes, por la cual se establece el Régimen de Protección de los Derechos de los Usuarios de Servicios de Comunicaciones, se modifica el Capítulo 1 del Título II de la Resolución CRC 5050 de 2016 y se dictan otras disposiciones. Diario Oficial No. 50.157 de 24 de febrero de 2017.

Artículo 2.6.4.2. NIP de confirmación, Resolución No. 7151 DE 2023 "Por la cual se modifican disposiciones del régimen de Portabilidad Numérica Móvil definidas en el Capítulo 6 del Título II de la Resolución CRC 5050 de 2016 y se dictan otras disposiciones".

ATIS (marzo de 2024). *Enhancing Telecom Security through Self-Sovereign Identity: A Solution to SIM Swap Fraud.* Resources, White Papers, pp. 4 y 5. Disponible en: https://atis.org/resources/enhancing-telecom-security-through-self-sovereign-identity-a-solution-to-sim-swap-fraud/

Bundesnetzagentur (2024). *About us.* Disponible en: https://www.bundesnetzagentur.de/EN/General/Bundesnetzagentur/AboutUs/start.html

CNMC (2024). *Qué es la CNMC.* Disponible en: https://www.cnmc.es/sobre-la-cnmc/que-es-la-cnmc

CONDUSEF (2021) Anuario Estadístico 2020. Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. Consultado en: https://www.condusef.gob.mx/documentos/estadistica/estad2021/anuario_2020.pdf

CONDUSEF (2022) Anuario Estadístico 2021. Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. Consultado en: https://www.condusef.gob.mx/documentos/estadistica/estad2021/anuario_2021.pdf

CONDUSEF (2023) Anuario Estadístico 2022. Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. Consultado en: https://www.condusef.gob.mx/documentos/estadistica/estad2022/ANUARIO_2022.pdf

CONDUSEF (marzo de 2023). *Los fraudes cibernéticos se actualizan*, Revista Proteja su Dinero, p. 20-22. Consultado en: https://revista.condusef.gob.mx/wp-content/uploads/2023/03/fraude_276.pdf

CONDUSEF (s.f). *Modalidad de fraude también conocido como SIM SWAPPING.* Disponible en: https://www.condusef.gob.mx/?p=contenido&idc=1594&idcat=3

CONDUSEF (2019). *Fraudes cibernéticos y Tradicionales.* Consultado en: https://www.condusef.gob.mx/documentos/comercio/FraudesCiber-3erTrim2019.pdf

CONDUSEF (2017). *¿Sabes qué es el Robo de Identidad?*, Gobierno de México. Consultado en: https://www.gob.mx/condusef/articulos/recomendaciones-para-prevenir-el-robo-de-identidad

CONDUSEF (s.f). *CONDUSEF lanza portal de fraudes financieros*, Gobierno de México. Consultado en: https://www.condusef.gob.mx/?p=contenido&idc=360&idcat=1

CONDUSEF (s.f). *Mantente alerta ante el Robo de Identidad*, Gobierno de México. Consultado en: https://www.condusef.gob.mx/?p=contenido&idc=1713&idcat=1#:~:text=La%20Comisi%C3%B3n%20Nacional%20para%20la,su%20autorizaci%C3%B3n%2C%20usualmente%20para%20cometer

CONDUSEF (s.f). *Tipos de fraude*, Gobierno de México. Consultado en: https://www.condusef.gob.mx/?p=tipos-de-fraude

CRC (2024). *Misión, visión, funciones y deberes.* Disponible en: https://www.crcom.gov.co/es/transparencia-y-acceso-a-la-informacion-publica/informacion-de-la-entidad/mision-vision-funciones-y-deberes#cont

CRTC (8 de julio de 2021). *Telecom Commission Letter addressed to the Distribution List*, expedient 8665-C12-202000280. Disponible en: https://crtc.gc.ca/eng/archive/2021/lt210708.htm

CRTC (2024). *About us.* Disponible en: https://crtc.gc.ca/eng/acrtc/org.htm

Decreto 46 [Decreto 46, 15/junio/2023] que modifica el Decreto N.º 18, de 2014, que aprueba reglamento de servicios de telecomunicaciones que indica [Decreto 18, 13/febrero/2014] Ministerio de Transportes y Telecomunicaciones; Subsecretaría de Telecomunicaciones, 09/enero/2014, República de Chile.

FCC (Nov 16, 2023). *In the Matter of Protecting Consumers from SIM Swap and Port-Out Fraud, Bureau* Wireline Competition. Disponible en: https://www.fcc.gov/document/fcc-adopts-rules-protect-consumers-cell-phone-accounts-0

FCC (2024). *About the FCC.* Disponible en: https://www.fcc.gov/about/overview

Fernández Yúbal (6 de octubre de 2021). *Verificación en 2 pasos o 2FA: qué es, para qué sirve y qué métodos existen.* Xataca. Disponible en: https://www.xataka.com/basics/verificacion-dos-pasos-2fa-que-sirve-que-metodos-existen

Gobierno de Reino Unido (2019). *Carta del sector del fraude: telecomunicaciones.* Actualizado el 21 de noviembre de 2022. Disponible en: https://www.gov.uk/government/publications/joint-fraud-taskforce-telecommunications-charter/fraud-sector-charter-telecommunications-accessible-version

IFT (s.f.) *Levanta tu queja" Soy Usuario".* Disponible en: https://www.ift.org.mx/usuarios-y-audiencias/levanta-tu-queja-soy-usuario#:~:text=SOY%20USUARIO%20es%20la%20herramienta,se%20han%20vulnerado%20sus%20derechos.&text=la%20informaci%C3%B3n%20que%20necesitas%20para%20hacer%20valer%20tus%20derechos.

Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of CustomerProprietary Network Information and Other Customer Information; IP-Enabled Services, CC Docket No. 96-115, WC Docket No. 04-36, 22 FCC Rcd 6927, 6931, pag. 5 (2007).

INEGI (2024). *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares.* Disponible en: https://www.inegi.org.mx/programas/endutih/2023/

INTERPOL (s.f.) *La ciberdelincuencia traspasa fronteras y evoluciona a gran velocidad.* Disponible en: https://www.interpol.int/es/Delitos/Ciberdelincuencia

Kaspersky (s.f.) ¿Qué es la ingeniería social? Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

OFCOM (24 de junio de 2010). *What is Ofcom?* Disponible en: https://www.ofcom.org.uk/about-ofcom/what-we-do/what-is-ofcom/

Redacción CDMX (27 de enero de 2023). *En 2022 la Condusef contabilizó 16 mil casos de robo de identidad*, El Universal Puebla, Economía y Negocio. Consultado en: https://www.eluniversalpuebla.com.mx/economia-y-negocios/en-2022-la-condusef-contabilizo-16-mil-casos-de-robo-de-identidad/

Resolución 566 exenta (06/abril/2024) [Ministerio de Transportes y Telecomunicaciones; Subsecretaria de Telecomunicaciones]. Por la cual se establece requisitos mínimos de verificación de identidad y estándares de seguridad aplicables por proveedores de servicios de telecomunicaciones en los casos indicados, República de Chile.

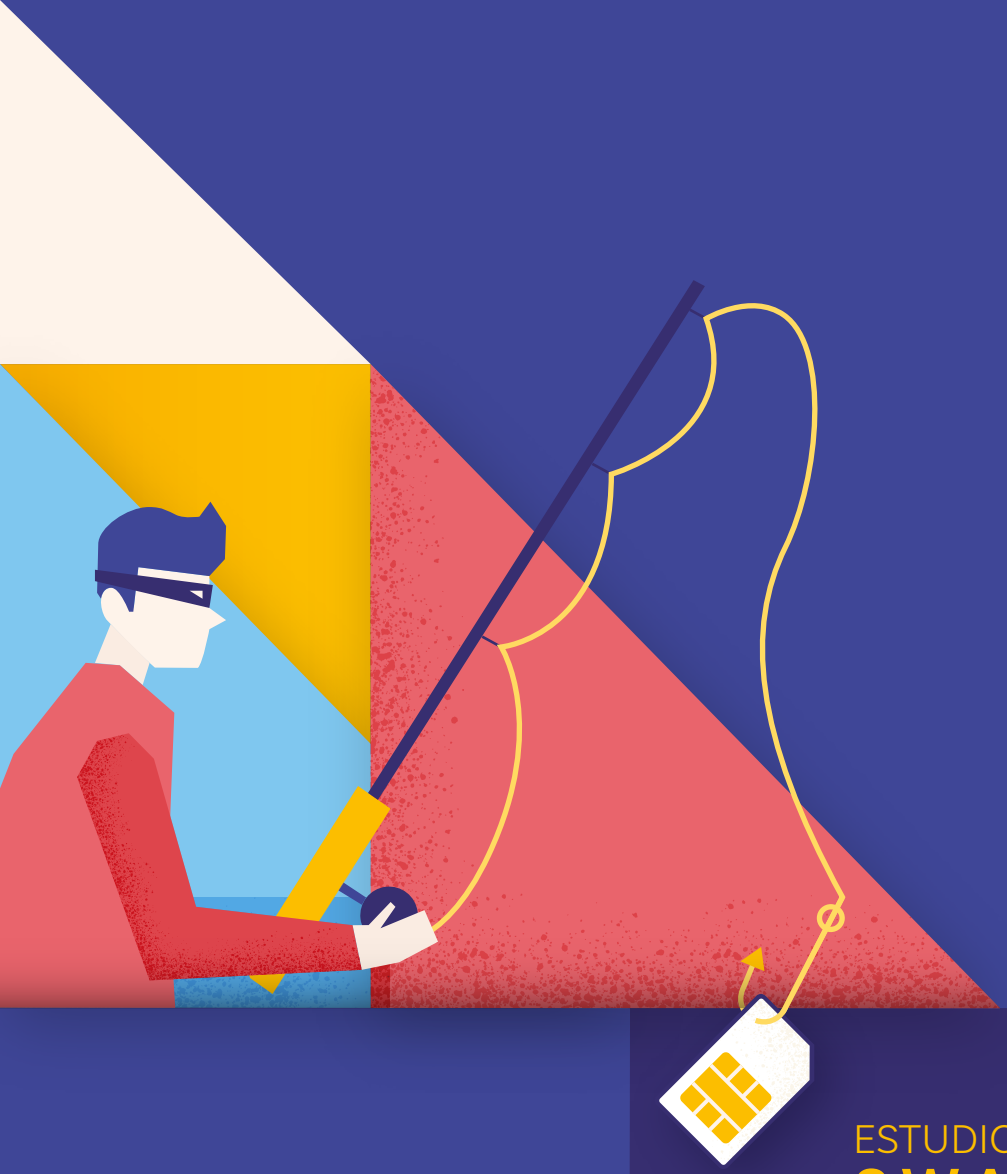
SSC (29 de octubre de 2020). *Policía Cibernética de la SSC alerta a la ciudadanía sobre nueva modalidad de fraude denominada "SIM SWAPPING" O "Duplicación de Sim".* Gobierno de la Ciudad de México. Disponible en: https://www.ssc.cdmx.gob.mx/comunicacion/nota/2191-policia-cibernetica-de-la-ssc-alerta-la-ciudadania-sobre-nueva-modalidad-de-fraude-denominada-sim-swapping-o-duplicacion-de-sim

SUBTEL (2024). *Que es SUBTEL*. Disponible en: https://www.subtel.gob.cl/quienes-somos/

SUBTEL (26 de julio de 2022). *Gobierno presenta plan de acción para enfrentar estafas telefónicas ante aumento sostenido de delitos asociados*, Sala de Prensa. Disponible en: https://www.subtel.gob.cl/gobierno-presenta-plan-de-accion-para-enfrentar-estafas-telefonicas-ante-aumento-sostenido-de-delitos-asociados/

Telecommunications Act [S.C. 1993, c. 38], Act current to 2024-05-14 and last amended on 2023-06-22. Consolidated Acts, Justice Laws Website.

Telephone records and privacy protection act of 2006, Pub. L. 109-476, 120 Stat. 3568 (2007) (codification an 18 USC § 1039).



ESTUDIO DEL SIM SWAPPING EN MÉXICO

ift INSTITUTO FEDERAL DE TELECOMUNICACIONES

http://www.ift.org.mx

Insurgentes Sur #1143, Col. Nochebuena,
Demarcación Territorial Benito Juárez,
C.P. 03720, CDMX
Tel: 55 5015 4000 / 800 2000 120