Tomo 1 - 2022

Documento de Política pública para reducir el delito de suplantación de Sim Card

Bogotá, Colombia.

Aso Ban Caria
Acerca la Banca a los Colombianos

Autores:

Jonathan Malagón	Presidente – **Asobancaria**
Alejandro Vera Sandoval	Vicepresidente Técnico – **Asobancaria**
Jaime Andrés Rincón Arteaga	Director de la Dirección de Gestión Operativa y Seguridad – **Asobancaria**
Elkin Sebastian Espinosa Garcia	Profesional Senior de la Dirección de Gestión Operativa y Seguridad – **Asobancaria**
Juan David Urquijo Vanegas	Profesional Junior de la Dirección de Gestión Operativa y Seguridad – **Asobancaria**

-Mesa técnica de delitos bancarios
-Suplantación de Identidad ante Operadores Móviles

Índice:

Resumen Ejecutivo

Nombre de la iniciativa:

Estrategia de acciones y actividades para reducir el delito informático de suplantación de identidad ante operadores móviles.

Metodología:

Se conformó una mesa técnica de delitos bancarios, priorizando el delito informático de suplantación de identidad ante operadores móviles. En esta mesa técnica se realizaron sesiones en donde se definen las problemáticas y las posibles soluciones para reducir el delito priorizado.

Organización de la iniciativa:

ASOBANCARIA.

Objetivo[1]:

Minimizar la suplantación de personas por medio de la reposición de *Sim Card* en un 15% para el 2024

1 El cumplimiento del objetivo está relacionado con realizar las tareas de la estructura de trabajo en el punto 8 del documento.

Introducción

Este documento está centrado en hacer un análisis cualitativo de las problemáticas de las entidades financieras y bancarias en relación con el delito priorizado de la suplantación de identidad ante operadores móviles "Sim Swap" a través de una metodología[2] de construcción conjunta. El *Sim Swap* consiste en el uso de ingeniería social por parte de los delincuentes para robar información, y con ello, suplantar a su víctima ante su operador de telefonía móvil con el fin de obtener la reposición de la *Sim Card* del afectado.

Con esta acción los delincuentes pueden acceder a las claves de confirmación, las cuales son enviadas por mensajes de texto, por las entidades financieras, y así ingresar a los diferentes canales digitales bancarios para finalmente realizar transacciones fraudulentas. Esta afirmación se apoya la infografía *"SIM SWAPPING*[3] *ESTAFA REALIZADA CAMBIANDO LA SIM"*[4], documento realizado por el centro de capacidades de la ciberseguridad del C4, donde se discuten los diferentes *modus operandi* que pueden utilizar los delincuentes para robar información (Policía Nacional de Colombia-C4, 2021).

Este documento es una guía de acciones y actividades que muestra los diagnósticos, problemáticas y posibles soluciones, además de una serie de compromisos y propuestas para minimizar el delito priorizado.

Contexto

Este documento busca fortalecer las acciones para reducir el impacto negativo de la suplantación de personas con el fin de obtener la *Sim Card* y así acceder a los canales digitales de los bancos y cometer defraudaciones. Desde Octubre de 2020 a Octubre de 2022 se han reportado 124 mil denuncias por delitos informáticos, de las cuales 47 mil son por hurto por medios informáticos, esto representa el 37,9% del total de modalidades. El Sim Swap se encuentra dentro de las principales modalidades utilizadas por los delincuentes para materializar este hurto. (Cifras del observatorio del delito - Policía Nacional de Colombia, 2022).

2 Metodología en diferentes sesiones con los actores que manifiestan los problemas, retos, soluciones, alternativas sobre el delito priorizado; esto permite identificar cuáles son las recomendaciones de actividades bajo un plan de acción o plan de trabajo por cada uno de los grupos de interés para lograr la reducción del delito en el corto y mediano plazo.

3 Es el nombre de referencia internacional a la modalidad de fraude por clonación de tarjeta *Sim Card*.

4 https://caivirtual.policia.gov.co/sites/default/files/sim_swappin_0.pdf

Estructura de problemas

En un ejercicio de construcción conjunta, se crearon mesas de trabajo con reuniones periódicas con la Policía Nacional, Fiscalía, bancos e instituciones financieras que permiten concluir las diferentes problemáticas ante el delito. Los principales problemas encontrados son:

Problema principal

El principal problema encontrado es la falta de colaboración de diferentes actores en los procedimientos para disminuir los casos de suplantación por *Sim Swap*. Este problema se caracteriza por la desarticulación de los planes de las entidades de gobierno, Telcos[5] y entidades financieras y bancarias que deben tener estrategias para reducir la suplantación por clonación de *Sim Card.*

Problemas secundarios

En la mesa técnica de delitos bancarios se encontraran cinco problemas secundarios relacionados con el delito de Sim Swapping, estos son:

- Dificultades para establecer las denuncias a través de portales virtuales.
- Falta de programas de educación financiera para que los clientes validen con quién comparten la información.
- El desconocimiento de los asesores comerciales de los bancos sobre los protocolos y pasos para reportar a la Fiscalía cuando ocurren estos casos.
- Falta de regulación para la implementación de programas que garanticen la seguridad en la reposición de la *Sim Card.*
- Falta de colaboración entre los bancos y las Telcos para implementar procedimientos articulados.

Adicionalmente, se encontró frente a los problemas secundarios las siguientes consideraciones:

- Los clientes no saben cómo presentar la evidencia digital para instaurar su denuncia y así obtener una respuesta efectiva por parte de los entes de investigación.
- Los clientes no identifican cuáles *modus operandi* utilizan los delincuentes para robar información y suplantarlos ante las Telcos.
- Se evidencia una inadecuada presentación de las denuncias por casos de suplantación por parte de los clientes ante los entes de investigación.
- No existen lineamientos claros sobre las obligaciones de las Telcos en materia de los programas mínimos de identificación y verificación que garanticen la seguridad de los productos de los clientes.
- Las acciones de las entidades de gobierno, Telcos[6] y entidades financieras y bancarias no tienen unos lineamientos o plan estratégico claro para reducir la suplantación a través de reposición fraudulenta de *Sim Cards*.

5 Empresa de telecomunicaciones dedicada a brindar servicios de operación móvil

Problemáticas y posibles soluciones

Las problemáticas relacionadas se centran en 5 ejes:

1. Mecanismo de denuncia.
2. Educación financiera.
3. Falta de capacitación de funcionarios.
4. Regulación de programas de identificación.
5. Verificación y desarticulación de los actores.

A continuación, se presentará un resumen de cada una de las problemáticas:

1. Mecanismo de denuncia

Existen múltiples retos relacionados con los mecanismos de denuncia. Por ejemplo, existen problemas con la cadena de custodia, que en ocasiones no se cumple, lo que genera que se pierda la evidencia. Así mismo, los ciudadanos se quejan porque no saben el estado de sus denuncias y si estas fueron realmente atendidas. Por último, existe una percepción de ineficiencia, dado que la mayoría de los casos no son resueltos por la autoridad. Estas situaciones han llevado a que la ciudadanía no instaure la denuncia o desistan del proceso. Frente a esta problemática la mesa de delitos bancarios propone:

1. Crear una plataforma de alertas para los denunciantes donde la Fiscalía reporte el avance de las denuncias y los tiempos de respuesta en cada etapa. **(Impacto: 4,5 | Esfuerzo: 4)**[6]

2. Publicar y publicitar los procesos y procedimientos que se tienen para instaurar las denuncias en los delitos de suplantación. **(Impacto: 3,5 | Esfuerzo: 4)**

3. Generar un manual de cadena de custodia frente a evidencia digital. **(Impacto: 3.5| Esfuerzo 3.8)**

Solución:

La mesa técnica después de sopesar los pro y contras definió que la primera opción tiene más impacto y menos esfuerzo. Por lo cual, se propone crear una plataforma de alertas para los denunciantes, con el fin de implicar al denunciante en los procesos de denuncia, y hacer seguimiento del estado de la evidencia y el proceso; Así mismo, se recomienda publicar y publicitar los procesos y procedimientos para instaurar denuncias de tal forma que sea más de más fácil acceso y conocido por la ciudadanía. Frente al problema de cadena de custodia de la evidencia digital, se plantea generar un manual de buenas prácticas por parte de la fiscalía general de la nación, frente al manejo de esta evidencia.

6 Metodología de evaluación donde la mesa técnica hace una relación entre el impacto y el esfuerzo de implementar actividades por cada proposición.

2 . Educación financiera

Parte de la incidencia del delito, se debe a la falta de conocimiento de los distintos actores frente a la modalidad. Es necesario crear soluciones direccionadas a mejorar la educación financiera de los clientes, frente a posibles casos de suplantación para reposición de *Sim Card.* Un ejemplo de ello se rescata de la cartilla del Ministerio del Interior y Seguridad Pública Chileno *"Ciberconsejos de seguridad para evitar los peligros del Sim Swapping"*, en la cual se resaltan las modalidades y los planes de acción en caso de tener señales de alerta contra el *Sim Swapping.* Frente a esta problemática la mesa de delitos bancarios propone:

1. Campañas masivas de sensibilización donde se realicen ejercicios de gamificación[7] centrados en explicar las modalidades y *modus operandi* del *Sim Swapping* a través de la recreación de escenarios y signos de alerta ante una posible clonación de la Sim Card. **(Impacto: 4 | Esfuerzo: 3,25)**

2. Realizar un modelo de cooperación entre entidades de gobierno, Telcos y entidades financieras y bancarias bajo una estrategia de comunicaciones conjunta a través de medios masivos y nuevos medios con tendencias virales, enfocándose en mensajes con lenguaje cotidiano, cifras, ejemplos y pasos de acción ante una posible situación de riesgo. **(Impacto: 4,4 | Esfuerzo: 3)**

3. Unificar las directrices estratégicas por parte del departamento de educación financiera y de seguridad de entidades de gobierno, Telcos y entidades financieras y bancarias. **(Impacto: 4 | Esfuerzo: 4,5)**

Solución:

La mesa técnica, tras considerar los pro y contras, determinó que la primera opción tiene más impacto y menos esfuerzo. Por lo cual, se propone realizar campañas masivas con ejercicios de gamificación que tengan como finalidad recrear escenarios donde se explique en ambientes simulados cómo son los signos de alerta, maneras y modalidades de los delincuentes para robar información. También, se recomienda unificar las directrices estratégicas por parte del departamento de educación financiera de las entidades financieras y bancarias para hacer campañas con el mismo enfoque. La técnica de gamificación permite generar una mayor conciencia a la ciudadanía a través de un enfoque didáctico y de fácil entendimiento. Los esfuerzos de concientización deben ser coordinados entre los diferentes actores, de tal forma que se sumen las diferentes iniciativas.

7 Es una técnica de educación y aprendizaje a través de técnica de juegos que tiene como objetivo conocer las habilidades de los participantes ante un posible escenario o actividad planteada.

3 . Falta de capacitación en seguridad digital para funcionarios de Telcos y bancos

La mesa técnica encontró que actualmente no existen programas de capacitación de ciberseguridad a funcionarios de bancos y Telcos que se enfoquen en explicar los diferentes *modus operandi*, modalidades, rutas de denuncia, manejo de evidencia digital, entre otros. Frente a esta problemática la mesa de delitos bancarios propone:

1. Realizar campañas de capacitación para los funcionarios de bancos y las Telcos, para concientizar a los asesores en detectar la suplantación de una persona a través de la reexpedición de la *Sim Card*, estas capacitaciones estarán centradas en identificar comportamientos de alerta por parte de un usuario interesado en reponer una *Sim Card*. **(Impacto: 3 | Esfuerzo:3**

2. Implementar una plataforma en línea de información compartida, donde todos los operadores de telecomunicaciones y bancos tengan a su disposición los registros y reposiciones de clientes[8]. **(Impacto: 4 | Esfuerzo: 4,5)**

Solución:

La mesa técnica, después de sopesar los pro y contras determinó que la segunda opción tiene mayor impacto con menos esfuerzo. Por lo cual, se propone que a futuro se implemente una plataforma en línea de información compartida entre operadores y bancos, que permita a las entidades financieras contar con información sobre las renovaciones de Sim Card de los Clientes, de tal forma que puedan incluir esta información en sus motores de fraude. También, se deben desarrollar campañas al interior de las entidades para sensibilizar a los funcionarios de bancos y Telcos sobre esta modalidad. En particular se propone sensibilizar a los funcionarios encargados de realizar los trámites de modificación de Sim Card o sustitución de contratos.

8 Los clientes que repongan una *Sim Card* sean notificados en tiempo real a las entidades bancarias y financieras que permita tener en supervisión y alerta las cuentas relacionadas con ese número móvil restringiendo operaciones bancarias y transacciones por un determino tiempo.

4 . Regulación de programas de identificación y verificación

De acuerdo con lo discutido por la mesa de trabajo, existen oportunidades de mejora en los programas de identificación y verificación de clientes de los operadores móviles. Según la mesa de trabajo, es necesario aplicar controles más robustos de seguridad en el momento de autenticación en los diferentes canales transaccionales. Esto podría lograrse a través de programas como BIO-SWAP[8], este programa se explica en el artículo *"Open Research Problems in Network Security[9]"* y consiste en una plataforma biométrica web donde los clientes se registran previamente y el cambio de *Sim Card* tiene verificación a través de diferentes medios móviles. El sistema no es centralizado, sino adoptado por cada empresa de operadores móviles. (Camenisch, J.; Dubovitskaya, M., 2010). El programa permite además ser una solución para el Sim Swap ya que como se menciona en el documento *"Awareness of Sim Swap Attack"*; ayuda a atacar la modalidad incluso cuando existe portabilidad numérica entre operadores. (Awale, S.; Gupta, P., 2019).

De esta forma, es imperativo involucrar a las compañías de telefonía móvil en las soluciones para los casos de *Sim Swap*. Los operadores deben robustecer sus controles de verificación e identificación de los clientes de tal forma que se minimice la suplantación de identidad en la expedición de *Sim Cards*. Frente a esta problemática la mesa de delitos bancarios propone:

1. Implementar sistemas de autentificación frente a los diferentes procesos que se realizan ante los operadores móviles, por ello, se requiere establecer necesariamente una regulación a través de la Comisión de Regulación de Comunicaciones (CRC). Esta regulación debe especificar los requisitos mínimos, de verificación que deben implementar los operadores móviles en una reexpedición de Sim Card o procesos que implique cambio de titular de la cuenta. **(Impacto: 4,2 | Esfuerzo: 3,5).**

2. Desarrollar un programa en toda la industria de las Telcos, donde se implemente la autenticación biométrica a través de terceros en alianza con los Operadores. **(Impacto: 4,5 | Esfuerzo: 4).**

Solución:

La mesa técnica después de determinar los pro y contras, llegó a la conclusión de que la primera opción tiene más impacto y menos esfuerzo. Por lo cual, se estableció necesario solicitar una regulación a través de la Comisión de Regulación de Comunicaciones para que los operadores de telefonía móvil celular implementen sistemas de verificación y autentificación más robustos en la reexpedición de *Sim Card* o procesos que implique el cambio de titular de la cuenta.

9 Es un sistema de registro previo con datos biométricos, donde la operación e implementación depende de un proveedor y la empresa de comunicaciones en diferentes países de Europa. *"Open Research Problems in Network Security*

5 . Articulación de los actores.

Actualmente, existen acciones individuales para disminuir el delito priorizado y no existe un marco de acciones conjuntas por parte de las entidades de gobierno, Telcos, bancos e instituciones financieras que sincronicen las acciones para atacar el delito. Para solucionar esta situación se presenten las siguientes propuestas:

1. Conformar un equipo multidisciplinar y multiorganizacional centrado en llevar a cabo recomendaciones en materia de mejoras en los mecanismos de denuncia, estrategias institucionales para reducir el delito, campañas de sensibilización segmentadas, entre otros aspectos. **(Impacto: 4,5 | Esfuerzo: 3)**

2. Crear un canal o medio para intercambiar experiencias de las entidades de gobierno, Telcos, bancos e instituciones financieras. **(Impacto: 4 | Esfuerzo: 3,5)**

Solución:

La mesa técnica, luego de analizar los pro y contras, determinó que la segunda opción tiene mayor impacto con un menor esfuerzo. Por lo cual, se propone conformar un equipo multidisciplinar y multiorganizacional centrado en llevar a cabo recomendaciones en materia de mejoras en los mecanismos de denuncia, estrategias institucionales para reducir el delito, campañas de sensibilización segmentadas entre clientes, entre otros aspectos; adicionalmente, se recomienda en este grupo se comparta experiencias entre las diferentes organizaciones participes.

Alternativas

En este punto, se establecen las diferentes alternativas frente al objetivo principal que consiste en minimizar la suplantación de personas por medio de la reposición de *Sim Card* en un 15% para el 2024. Para ello, se hace la relación entre el impacto y el esfuerzo (I-E) que arroja la alternativa principal, la alternativa secundaria y las alternativas de apoyo.

1. **Alternativa principal:** Conformar un equipo multidisciplinar y multiorganizacional centrado en llevar a cabo recomendaciones en materia de mejoras en los mecanismos de denuncia, estrategias institucionales para reducir el delito, campañas de sensibilización segmentadas, entre otros aspectos; adicionalmente, se recomienda en este grupo se comparta experiencias entre las diferentes organizaciones participes. **Ratio[10]:1,5**

2. **Alternativa Secundario:** Realizar campañas masivas con ejercicios de gamificación que tengan como finalidad recrear escenarios donde se explique en ambientes simulados como son los signos de alerta, maneras y modalidades de los delincuentes para robar información. También, se recomienda unificar las directrices estratégicas por parte del departamento de educación financiera de las entidades financieras y bancarias para hacer campañas con el mismo enfoque. **Ratio:0,75**

3. **Alternativa de Apoyo:** Impulsar una regulación a través de la Comisión de Regulación de Comunicaciones para robustecer los sistemas de verificación y autentificación que deben existir en un proceso de reexpedición de Sim Card o procesos que impliquen cambio de titular. **Ratio:0,7**

4. **Alternativa de Apoyo:** Implementar una plataforma en línea de información compartida entre operadores y bancos, que permita a las entidades financieras contar con información sobre las renovaciones de *Sim Card* de los Clientes, de tal forma que puedan incluir esta información en sus motores de fraude[11]. También, desarrollar campañas al interior de las entidades para sensibilizar a los funcionarios de bancos y Telcos sobre esta modalidad. **Ratio:0,5**

5. **Alternativa de Apoyo:** Crear una plataforma de alertas para los denunciantes, con el fin de que se pueda realizar un seguimiento al estado de la denuncia por parte de la ciudadanía. se recomienda publicar y publicitar los procesos y procedimientos para instaurar denuncias de tal forma que sea más de más fácil acceso y conocido por la ciudadanía. Frente al problema de cadena de custodia de la evidencia digital, se plantea generar un manual de buenas prácticas por parte de la fiscalía general de la nación, frente al manejo de esta evidencia. **Ratio:0,5**

10 Relación cuantificada entre el interés y el esfuerzo refleja el ratio o proporción de la solución.

11 Los clientes que repongan una Sim Card sean notificados en tiempo real a las entidades bancarias y financieras que permita tener en supervisión y alerta las cuentas relacionadas con ese número móvil restringiendo operaciones bancarias y transacciones por un determino tiempo

Stakeholders o actores de interés

Una vez definidos los *stakeholders* o grupo de interés que se relacionan con la alternativa principal, alternativa secundaria y alternativas de apoyo. Se realiza una relación entre el interés y el poder de cada actor, permitiendo crear una ratio promedio para asignar el papel clave de cada uno respecto a las actividades bajo una metodología de distancia[12] y así determinar los actores principales y secundarios que permitan asignar actividades principales para el plan de acción y la reducción del delito priorizado.

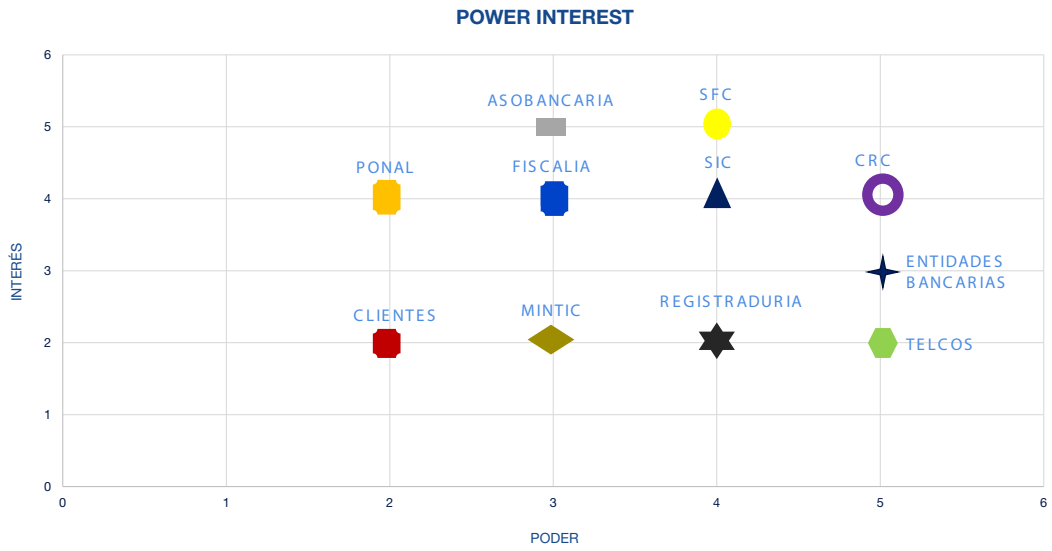
Tabla 1: Actores bajo Power Interest

Actores de ejecución para alternativas	Interés	Poder	Ratio	Tipo de actor
Superintendencia de Industria y Comercio	3	4	3,5	Principal
Superintendencia Financiera de Colombia	5	4	4,5	Principal
Telcos - ISP	2	5	3,5	Principal
Fiscalía	4	3	3,5	Principal
Asobancaria	5	3	4	Principal
Bancos y entidades financieras	5	4	4,5	Principal
Comisión de regulación de comunicaciones (CRC)	4	5	4,5	Principal
Policia Nacional	4	2	3	Secundario
Clientes	2	2	2	Secundario
Ministerio TIC	2	3	2,5	Secundario
Registraduría	2	4	3	Secundario
Promedios	3,45	3,55	3,5	

Fuente: Elaboración Mesa técnica.

*Las calificaciones de interés y poder son realizadas por la mesa técnica a través de promedios de votación por una encuesta realizada en la sesión de trabajo respectiva.

Gráfica 1: Actores bajo Power Interest



Fuente: Elaboración Mesa técnica.

12 Es una metodología de distancia al promedio, que permite evaluar la relevancia de un actor para cumplir un objetivo y su incidencia respecto al resultado. Los actores de interés son elegidos por la mesa técnica respecto a las alternativas y los análisis de problemáticas y alternativas.

Estructura de trabajo

Tabla 2: Estructura de trabajo

Nivel	Alternativa	Alcance/Objetivo	Actividades	Responsable	Tiempo de Realización
PRINCIPAL	Conformar un equipo multidisciplinar y multiorganizacional centrado en llevar a cabo recomendaciones en materia de mejoras en los mecanismos de denuncia, estrategias institucionales para reducir el delito, campañas de sensibilización segmentadas, entre otros aspectos; adicionalmente, se recomienda en este grupo se comparta experiencias entre las diferentes organizaciones participes.	Plan unificado y marco de acción en el corto y mediano plazo contra el Sim Swap con estrategias claras en las acciones de todos los actores involucrados.	Presidir la mesa técnica con los actores relevantes para sacar un documento de política publica y la creación de un marco de acción por cada uno de los actores comprometidos con la reducción del delito.	Superintendencia Financiera / Superintendencia de Industria y Comercio	Corto plazo
			Elaborar una cartilla de masiva difusión sobre las diferentes modalidades que utilizan los ciberdelincuentes para robar información necesaria para la reexpedición de la Sim Card.	Policía Nacional/ Asobancaria/Telcos	Corto Plazo
			Establecer en el corto y mediano plazo las diferentes resoluciones necesarias para dar cumplimiento al marco regulatorio en el corto y mediano plazo.	Comisión de Regulación de Comunicaciones	Corto plazo
			Presentar un plan estratégico TIC para mejorar en el corto y mediano plazo las estrategias para reducir el Sim Swap.	Telcos	Mediano plazo
			Documentar los clientes que han sido victimas y aspectos a tener en cuenta la mesa en el momento de formular las estrategias.	Bancos y entidades financieras	Corto plazo
			Incentivar a los clientes a denunciar cuando sufren en caso de suplantación y tomar acciones de cambiar claves y bloquear todas las bancas móviles.	Clientes / Bancos y entidades financieras	Corto plazo
			Crear un procedimiento para compartir experiencias entre las entidades bancarias y financieras con las organizaciones participes de este equipo.	Asobancaria	Mediano plazo
			Realizar una capacitación a los fiscales en el manejo de la evidencia digital, identificación de patrones criminales, entre otros.	Fiscalía	Corto plazo
SECUNDARIO	Realizar campañas masivas con ejercicios de gamificación que tengan como finalidad recrear escenarios donde se explique en ambientes simulados como son los signos de alerta, maneras y modalidades de los delincuentes para robar información. También, se recomienda unificar las directrices estratégicas por parte del departamento de educación financiera de las entidades financieras y bancarias para hacer campañas con el mismo enfoque	Campaña de gamificación por parte de por lo menos 5 bancos en Colombia con 10.000 clientes que aprendan los modus operandi y estrategias de los delincuentes al realizar Sim Swap.	Diseñar una estrategia conjunta para los bancos que consistan en realizar una campaña de gamificación que involucren a los actores.	Asobancaria	Mediano plazo
			Acompañar a los Bancos en el diseño de las campañas de gamificación, recreando situaciones reales acorde al delito del Sim Swap.	Superintendencia Financiera / Superintendencia de Industria y Comercio	Corto plazo
			Realizar una mesa técnica de los departamentos de educación financiera donde se discuta las directrices de las campañas con el fin de unificar el enfoque de todas las entidades.	Asobancaria / Bancos y entidades financieras	Corto plazo
			Realizar la campaña masiva con los clientes y la presentación de escenarios para los clientes.	Bancos y entidades financieras	Mediano plazo
			Participar activamente en las campañas de gamificación y difundir a través del voz a voz las características del Sim Swap y aspectos a tener en cuenta.	Clientes	Corto plazo

Nivel	Alternativa	Alcance/Objetivo	Actividades	Responsable	Tiempo de Realización
APOYO	Impulsar una regulación a través de la Comisión de Regulación de Comunicaciones para robustecer los sistemas de verificación y autentificación que deben existir en un proceso de reexpedición de Sim Card o procesos que impliquen cambio de titular.	Regulación con los sistemas de verificación y autentificación que debe tener una Telco en el proceso de reexpedición de su Sim Card y cambios de titular.	Crear un marco de apoyo sobre programas que se centren en impulsar tecnología de biometría y otro tipo de TIC´S centrados en reducir el fraude y la suplantación en Colombia.	Ministerio TIC	Corto plazo
			Definir las resoluciones necesarias para regularizar los sistemas de verificación con diversos filtros y factores que prevea la suplantación de clientes.	Comisión de Regulación de Comunicaciones	Mediano plazo
			Implementar los sistemas de biometría para la reexpedición de Sim Card, también vincular el funcionamiento y activación de la Sim Card al código IMEI de cada celular.	Telcos	Mediano plazo
			Revisar técnicamente alternativas mas seguras para la entrega de mensajes SMS.	Bancos y entidades financieras	Corto plazo
			Implementar en una App que migre la entrega de mensajes de textos tradicional a mensajes push.	Bancos y entidades financieras	Corto plazo
			Apoyar en la implementación de los sistemas de autentificación como la Biometría en Colombia por parte de los bancos y las Telcos.	Registraduría Nacional	Mediano plazo
APOYO	Implementar una plataforma en línea de información compartida entre operadores y bancos, que permita a las entidades financieras contar con información sobre las renovaciones de Sim Card de los Clientes, de tal forma que puedan incluir esta información en sus motores de fraude. También, desarrollar campañas al interior de las entidades para sensibilizar a los funcionarios de bancos y Telcos sobre esta modalidad.	Plataforma donde las Telcos y los bancos pueden tener acceso en tiempo real de quien expide una Sim Card para poder tener un alerta previa sobre el riesgo de fraude por suplantación	Definir los parámetros de la plataforma sobre que información compartirán con los bancos y los manuales de uso del mismo.	Comisión de Regulación de Comunicaciones	Mediano plazo
			Definir la parte operativa de la plataforma y accesos por parte de los miembros de los bancos. Es importante definir el esquema de alertas de las personas que reexpiden las Sim Cards y realizan operaciones deshabitúales por el consumidor.	Bancos y entidades financieras	Mediano plazo
			Fortalecer los equipos comerciales y asesores en línea en las diferentes estrategias de suplantación.	Bancos y entidades financieras	Corto plazo
			Construir y ofrecer la plataforma que permita compartir la información entre Telcos y Bancos.	Asobancaria / Telcos	Largo plazo
APOYO	Crear una plataforma de alertas para los denunciantes, con el fin de que se pueda realizar un seguimiento al estado de la denuncia por parte de la ciudadanía. se recomienda publicar y publicitar los procesos y procedimientos para instaurar denuncias de tal forma que sea más de más fácil acceso y conocido por la ciudadanía. Frente al problema de cadena de custodia de la evidencia digital, se plantea generar un manual de buenas prácticas por parte de la fiscalía general de la nación, frente al manejo de esta evidencia.	Plataforma donde los usuarios tenga acceso a ver el estado de su proceso, sindicados, evidencia y avance en tiempos como una acción de información abierta.	Construcción de plataforma que muestre la ruta o guía en tiempo real del proceso, que acerque la investigación a la victima y evolución del proceso.	Fiscalía	Largo plazo
			Publicar en las páginas de cada una de las entidades financieras, la ruta de denuncia para los clientes que sufran de una suplantación.	Bancos y entidades financieras	Corto plazo
			Generar un manual de buenas prácticas por parte de la fiscalía general de la nación frente al manejo de esta evidencia.	Fiscalía	Mediano plazo
			Realizar seguimiento oportuno de cada caso de denuncias instaurado por el denunciante con notificaciones de novedades.	Clientes	Corto plazo
			Permitir a los bancos a instaurar desde las áreas de servicio al cliente, procesos de denuncias de los clientes y poder hacer asesoría y seguimiento a cada caso de suplantación presentado.	Bancos y entidades financieras	Mediano plazo

Pasos a Seguir

- Hacer una reunión con los tomadores de decisión de todos los actores involucrados en este documento y crear equipos de trabajo para realizar todas las actividades programadas en este documento.
- Crear una batería de seguimiento e indicador de cumplimiento de cada actividad para poder evaluar la ejecución del plan de trabajo.

Bibliografía

- Centro Cibernético Policial, 2020. SIM SWAPPING ESTAFA REALIZADA CAMBIANDO LA SIM. Bogotá, Colombia.
- Observatorio del delito de la Policía Nacional, 2022. Cifras de delitos informáticos entre el 1 de enero de 2020 a 31 de agosto de 2022. Bogotá, Colombia.
- Snehal Manohar Awale, Dr. Praveen Gupta, 2019. “Awareness of Sim Swap Attack” Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-Issue-4, June 2019, pp.995-997, URL: *https://www.ijtsrd.com/papers/ijtsrd23982.pdf*
- Open Research Problems in Network Security: IFIP WG 11.4 International Workshop, iNetSec 2010, Sofia, Bulgaria, March 5-6, 2010, Revised Selected Papers Tapa blanda – 23 Febrero 2011.
- Ministerio del Interior y Seguridad Pública Chileno, 2022. Ciberconsejos de seguridad para evitar los peligros del Sim Swapping. Santiago de Chile, Chile.

Aso
Ban
Caria

Acerca la
Banca a los
Colombianos