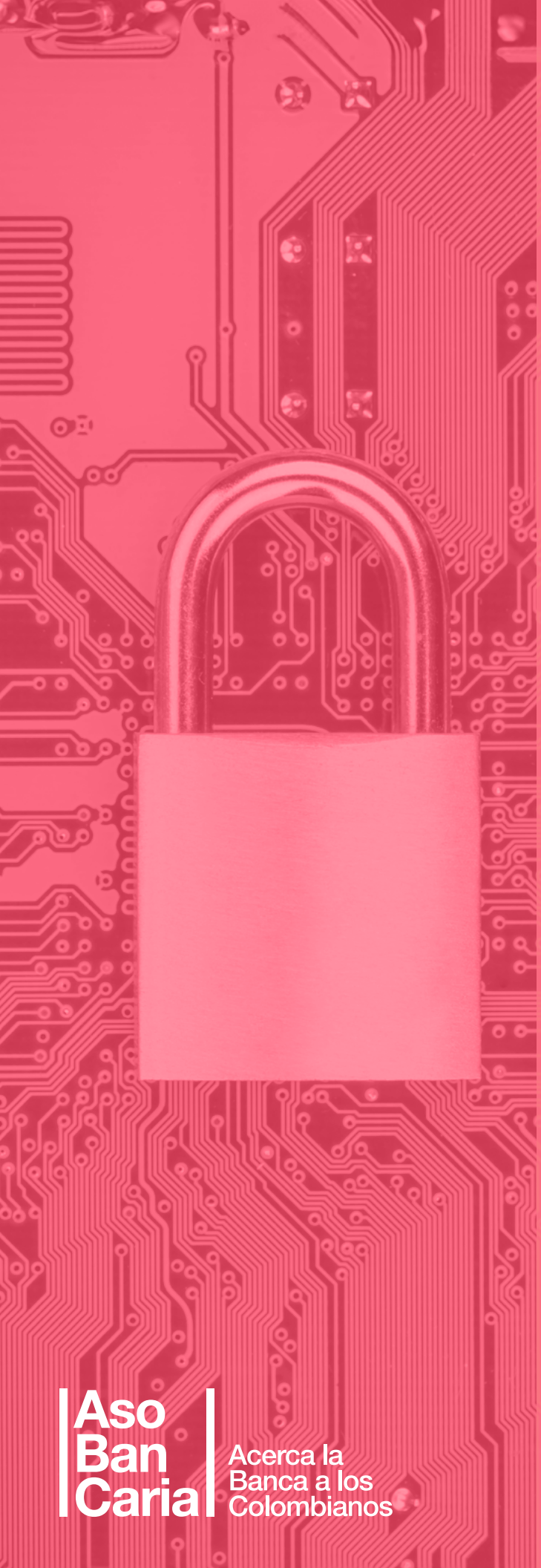


Tomo 2 - 2023

Documento de Política pública para reducir el delito de Hackeo

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**

- Mesa técnica de delitos bancarios

Índice:

1. Resumen Ejecutivo ..... 3.
2. Introducción ..... 4.
3. Contexto ..... 4.
4. Estructura de problemas ..... 5.
5. Análisis y posibles soluciones ..... 6.
6. Alternativas ..... 9.
7. Stakeholders o actores de interés ..... 10.
8. Estructura de trabajo ..... 11.
9. Pasos a seguir ..... 13.
10. Bibliografía ..... 13.

Resumen Ejecutivo

Nombre de la iniciativa:

Iniciativa direccionada a reducir los delitos informáticos por el hackeo en dispositivos digitales.

Metodología:

Se conformó una mesa técnica de delitos bancarios, priorizando el delito de *hackeo*. En esta mesa técnica se definieron las problemáticas y las posibles soluciones para reducir el delito priorizado.

Organización de la iniciativa:

ASOBANCARIA.

Objetivo[1]:

Minimizar el *hackeo* a clientes afectados por *malware* y otros accesos intrusivos en un 10% en 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 realizar un análisis cualitativo de las problemáticas de las entidades financieras y bancarias en relación con el delito de *hackeo* con acceso intrusivo por terceros en los canales digitales, este documento se realizó a través de una metodología[2] de construcción conjunta. El *hackeo* se define como las diferentes técnicas que utilizan los criminales para atacar informáticamente los dispositivos y recolectar información con el fin de acceder a los canales digitales y realizar operaciones fraudulentas.

Con este ataque informático, los delincuentes vulneran la seguridad del dispositivo e ingresan a los canales digitales de las entidades financieras, realizando transferencias no consentidas por los usuarios. La modalidad más usada en el *hackeo* es la implantación de *malware*[3], estos son enviados principalmente por correos, sitios web y mensajes de textos, y existe otras técnicas de *hacking.* Como la monitorización, D.O.S[4], entre otros. (Silva, L., Rentería E. Duque, J., 2011)

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 establecer acciones para reducir el impacto del hackeo en Colombia, con el fin de asegurar que los clientes del sistema financiero no sean objeto de fraude digital a través del acceso intrusivo de los canales digitales. Según el observatorio del delito, entre julio de 2021 a julio de 2023 se reportaron 117.074 denuncias de delitos informáticos, y en especial, la modalidad de acceso abusivo a un sistema informático se realizaron 22.773 denuncias, con lo que se convierte en la tercera modalidad más recurrente con un 19,45% en este periodo[5]. Sin embargo, se observa una reducción de 19,56% entre los periodos de enero a julio de 2022 y 2023, pasando de 7.791 denuncias de acceso abusivo a un sistema informático a 6.265 respectivamente para el año 2023. (Cifras del observatorio del delito - Policía Nacional de Colombia, 2023).

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 un término general para cualquier tipo de software con intenciones maliciosas. La mayoría de las amenazas online son algún tipo de *malware*.

4 Es una aplicación de software diseñada para ejecutarse en los smartphones (teléfonos inteligentes), tabletas y otros dispositivos móviles.

5 Las primeras 2 modalidades según el código penal son con un 41,82% el hurto por medios informáticos y semejantes y un 19,72% la violación de datos personales en el mismo periodo.

Estructura de problemas

Para definir los problemas 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. Las principales conclusiones fueron:

Problema principal

El principal problema encontrado es la falta de incentivos de los usuarios en descargar y mantener un sistema de antivirus en los dispositivos digitales que detecte preventivamente tipos de ataques maliciosos usados para acceder a los canales digitales de las entidades financieras.

Problemas secundarios

En la mesa técnica de delitos bancarios se encontraron los cinco problemas secundarios relacionados con el delito de *hackeo*, estos son:

- No hay un procedimiento claro que permita bloquear rápidamente las direcciones IP y dominios de donde proceden los *malware* maliciosos.
- Los sistemas de identificación que no implementan biometría son vulnerables por las bandas criminales para robar el dinero de la víctima y su identidad.
- Falta de comunicación entre las autoridades judiciales y el sistema financiero para intercambiar información que permita detectar dominios e IP´s de donde provienen los *malware*.
- Falta de programas de gobierno que busque implementar el uso de sistemas de antivirus gratuitos que detecten intentos de intrusión informática para los dispositivos digitales, app´s y portales web.
- Falta de campañas de sensibilización sobre el manejo de la información, su divulgación y conocimiento de los signos de alerta de un *hackeo*.

Efectos de problemas

La mesa técnica determina que los efectos de los problemas secundarios son:

- Una cantidad elevada de clientes afectados por la demora en el bloqueo de las direcciones IP´s y dominios donde proceden los *malware* maliciosos.
- No hay una articulación para compartir información que dinamice las investigaciones y acerque a las autoridades judiciales con la banca para reducir el delito.
- Los dispositivos digitales que no tienen en su sistema un programa de antivirus, tienen deficiencias de seguridad informática, esto los hace vulnerables y fáciles de hackear.
- Los usuarios no tienen un conocimiento claro sobre las estrategias de fraude digital y técnicas de hackeo que utilizan los delincuentes para vulnerar los dispositivos, robar la información y acceder a los portales bancarios.

Análisis y posibles soluciones

Analizamos los problemas propuestos en tres ejes:

1. Falta de procedimientos para bloquear rápidamente las direcciones IP´s y dominios que contienen *malware*.
2. Falta de incentivos de los usuarios para tener un sistema antivirus en su dispositivo.
3. Campañas de educación financiera masiva.

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

1. Falta de procedimientos para bloquear rápidamente las direcciones IP´s y dominios que contienen *malware*.

Existen diferentes razones que no permite el bloqueo de las direcciones IP´s y dominios que contienen *malware* en los tiempos requeridos. No existe un procedimiento claro para bloquear las direcciones IP´s. Actualmente las Telcos tienen la capacidad de bloquear las direcciones IP´s, sin embargo, no existe un procedimiento con tiempos de respuesta ni documentos específicos que estandarice las solicitudes respectivas. Adicionalmente, el bloqueo de dominios en Colombia solo se realiza a través de una orden judicial. La congestión judicial en Colombia genera que los tiempos de respuesta sean lentos y los dominios no sean bloqueados rápidamente aumentando la cantidad de usuarios afectados por ataques de delitos informáticos. Frente a esta problemática la mesa de delitos bancarios propone:

1. Impulsar desde la Superintendencia Financiera de Colombia la creación de un Proyecto de Ley que faculte a dicha superintendencia u otra institución en poder bloquear dominios utilizados para suplantar y robar información financiera. **(Impacto: 5 | Esfuerzo: 4)**

2. Impulsar desde la Comisión de Regulación de Comunicaciones la creación de una resolución que establezca el procedimiento para bloquear direcciones IP´s. La comisión debe determinar qué tipo de informes, documentos, tiempo e información deben cumplir las Telcos al solicitar el bloqueo de una dirección IP usada para enviar software malicioso. **(Impacto: 4 | Esfuerzo: 4)**

3. Crear un portal de verificación previa de enlaces por parte del Ministerio de Tecnologías de la información y comunicación, donde los usuarios puedan verificar preventivamente el origen y seguridad de los sitios web, y de esta forma, garantice conexión segura en la internet. **(Impacto: 4 | Esfuerzo: 3)**[6]

Solución:

La mesa técnica después de sopesar los pro y contras definió que se debe crear soluciones que ayuden al sector financiero a bloquear rápidamente los dominios fraudulentos, reduciendo los tiempos tiempos en los que estos se mantienen activos. De igual manera,

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

es necesario buscar los puntos de origen del programa maligno, para ello, se debe crear un procedimiento para bloquear direcciones IP´s que permita cerrar desde el origen los múltiples *malwares* que se estén enviando desde una dirección IP específica.

Por último, las soluciones presentadas anteriormente son defensivas ante los enlaces utilizados para realizar múltiples delitos de hackeo, phishing, entre otros; por ello, la mesa técnica piensa que se debe diseñar una solución preventiva donde el cliente tenga la posibilidad de verificar el origen del sitio web, con ello, identificar si es una URL con riesgo a ser víctima de fraude digital.

2 . Falta de incentivos de los usuarios para tener un sistema antivirus en su dispositivo.

Existe una falta de incentivos para tener un sistema de antivirus actualizado en los dispositivos digitales. En el mercado hay restricciones de acceso a estos sistemas, una de ellas son los precios elevados de tener un software que sea capaz de detectar *malwares* utilizados para acceder a los canales digitales de las entidades financieras. Los usuarios toman la decisión de no comprar software o comprar una licencia "*crackeada*", que carece de sistemas de actualizaciones ante eventuales amenazas e indicadores de compromiso deficientes. En segundo lugar, no existen protocolos de seguridad que deben mantener los dispositivos digitales en Colombia. Frente a estas problemáticas la mesa de delitos bancarios propone:

1. Impulsar desde el Ministerio de Tecnologías de la Información y las Comunicaciones la creación de un programa que tenga como objetivo crear y distribuir un software de antivirus actualizado con licencia gratuita al público, que logre detectar cuando el dispositivo esta en riesgo de infección informática. Es importante para lograr el uso masivo de este programa, una campaña de comunicaciones que resalte los beneficios de tener este software para la protección digital de las personas que lo utilicen. **(Impacto: 5 | Esfuerzo: 3)**

2. Crear una comisión con las entidades de gobierno, autoridades, miembros de la sociedad civil y otros actores encargados de presentar recomendaciones y buenas prácticas sobre los protocolos de seguridad que deben tener los dispositivos digitales en Colombia **(Impacto: 4 | Esfuerzo:2)**

Solución:

La mesa técnica después de sopesar los pro y contras definió que es necesario eliminar las barreras de acceso de las personas para tener un software de antivirus actualizado y confiable que sea gratuito[7]. Así mismo, se recomienda crear una comisión o equipo asesor que pueda compartir a la sociedad su conocimiento sobre el avance en seguridad digital que debe tener el país, por lo cual, es esencial crear este equipo que se articule al sector privado y público para orientar las estrategias de seguridad digital en el país, esto contrarresta las malas prácticas o vulnerabilidades informáticas que pueden tener las empresas y entidades de gobierno.

7 En la revisión de literatura, encontramos que no hay ningún país del mundo ha puesto en disposición un programa de antivirus de manera gratuita y libre para el uso de la sociedad.

3 . Campañas de educación financiera masiva

De acuerdo con la mesa técnica, se determinan que existen en las campañas de educación financiera en materia de fraude digital sobre hackeo. Esta afirmación se apoya en el informe *"The 2018 Norton Cyber Security Insights Report – Global results"* donde través de una evaluación realizada a más de 16 mil usuarios en 16 países concluyó que el 30% de los participantes no sabía que su dispositivo móvil podía ser hackeado. Adicionalmente, dentro de las 3 principales causas del hackeo, se encuentra: El débil conocimiento técnico de modalidades utilizadas en el hackeo, malas prácticas de seguridad cibernética y brecha de conocimiento generacional en seguridad digital. Es por ello, que se debe crear iniciativas direccionadas a mejorar la educación ante el fraude digital en hackeo, donde se tenga la oportunidad de enseñar las principales estrategias y alertas para tener en cuenta ante posibles eventos de infección informática, y con ello, crear una cultura de seguridad digital en Colombia.

Frente a esta problemática la mesa de delitos bancarios propone:

1. Crear un programa de educación financiera radial a través de las emisoras de la Policía Nacional con la participación de testimonios de clientes afectados y la participación de las entidades bancarias, autoridades, entre otros actores. **(Impacto: 5 | Esfuerzo: 3)**

2. Crear un programa televisivo desde el Ministerio de Tecnologías de la Información y Comunicaciones y RTVC[8] guiado a explicar y capacitar a la población colombiana en estrategias para prevenir el hackeo. **(Impacto: 5 | Esfuerzo: 4)**

Solución:

La mesa técnica después de sopesar los pro y contras definió que se debe crear un programa de educación financiera radial y televisiva a través de las emisoras de la Policía Nacional y RCTV. Este debe ser un programa masivo con mínimo 10 horas de contenido auditivo y 2 horas de contenido televisivo por cada delito informático, donde se debe explicar las alertas tempranas que deben tener las personas ante posibles casos de fraude digital, que puede incluir testimonios de víctimas, autoridades y entidades financieras.

Este programa busca crear personas prevenidas y consientes de sus practicas ante el fraude digital, esta afirmación se refleja en las recomendaciones del documento *"Estudio de mecanismos comportamentales frente al fraude digital"*, donde manifiesta la importancia de convertir a los usuarios es personas prevenidas y consientes de sus acciones ante posibles casos de fraude digital, reconociendo acciones que puedan repercutir en ser victimas de los ciberdelincuentes.

8 RADIO TELEVISIÓN NACIONAL DE COLOMBIA RTVC S.A.S (Sistema de Medios Públicos)

Alternativas

En este punto, se establecen las diferentes alternativas frente al objetivo principal que consiste en minimizar el hackeo a clientes afectados por malwares y otros accesos intrusivos en un 10% en el 2024. Para ello, se hace la relación entre el impacto y el esfuerzo (I-E) lo que arroja la alternativa principal, la alternativa secundaria y las alternativas de apoyo.

A continuación, se presentan los resultados promedio por los asistentes a la mesa técnica, estos son:

1. **Alternativa principal:** Impulsar desde el Ministerio de Tecnologías de la Información y las Comunicaciones un programa para poner a disposición del público un software de antivirus actualizado con licencia gratuita y crear una comisión público-privada que oriente la estrategia la estrategia de seguridad digital en el país. **Ratio: 4.**

2. **Alternativa Secundaria:** Crear un programa de educación financiera radial donde se creen una serie de contenidos que generen conciencia a las personas sobre los factores de riesgo o alertas que deben tener ante el fraude digital. **Ratio[9]:3.**

3. **Alternativa de Apoyo:** Crear un Proyecto de Ley que faculte a la Superintendencia Financiera de Colombia u otra institución de gobierno a bloquear dominios utilizados para el fraude digital, y que a través de una resolución se cree un procedimiento que permita bloquear las direcciones IP´s de manera más rápida por las Telcos. Así mismo, crear un portal de verificación previa de enlaces, donde los usuarios puedan verificar preventivamente el origen y seguridad de las URL´s. **Ratio: 2.**

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

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[10] y así determinar los actores principales y secundarios que permitan asignar actividades principales para el plan de acción y la reducción del delito priorizado.

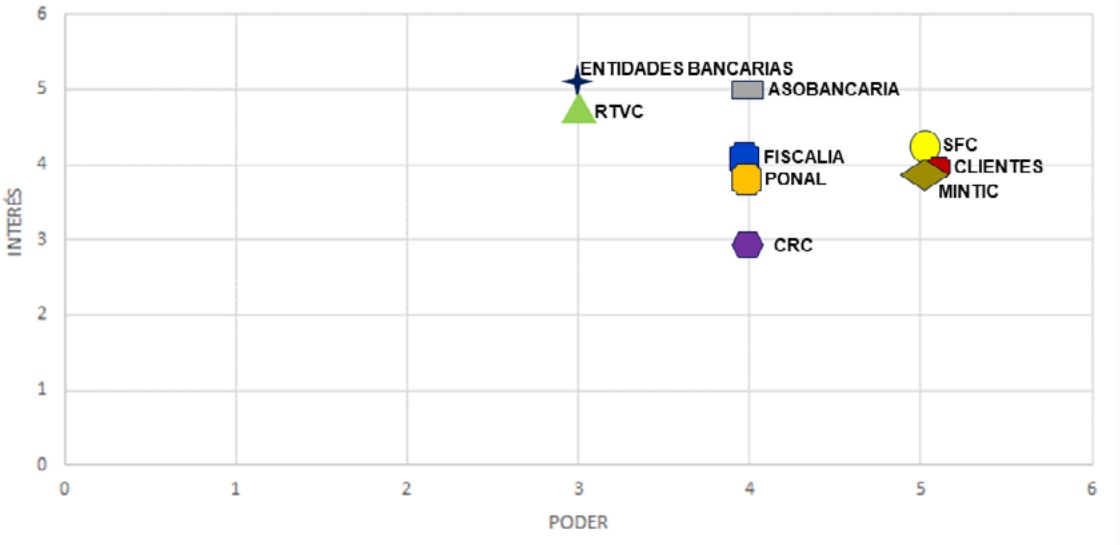
Tabla 1: Actores bajo Power Interest

Actores de ejecución para alternativas	Interés	Poder	Ratio	Tipo de actor
Superintendencia Financiera de Ciolombia	4	5	4,5	Principal
Clientes	4	5	4,5	Principal
Ministerio TIC	4	5	4,5	Principal
Asobancaria	5	4	4,5	Principal
Fiscalía	4	4	4	Secundario
Policia Nacional	4	4	4	Secundario
Entidades Financiera y Bancarias	5	3	4	Secundario
RTVC	5	3	4	Secundario
Comisión de Regulación de Comunicaciones	3	4	3,5	Secundario
Promedios	4,22	4,11	4,1666667	

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[11]



Fuente: Elaboración Mesa técnica.

10 Es una metodología de distancia al promedio, que me permite evaluar la relevancia de una acción o idea respecto al universo.

11 Relación del poder y el interés que señalan la importancia de cada actor para lograr el objetivo, pero no se asume responsabilidades específicas para el plan de acción o plan de trabajo.

Estructura de trabajo

Tabla 2: Estructura de trabajo

Nivel	Alternativa	Alcance/Objetivo	Actividades	Responsable	Tiempo de Realización
PRINCIPAL	Impulsar desde el Ministerio de Tecnologías de la Información y las Comunicaciones un programa para poner a disposición del público un software de antivirus actualizado con licencia gratuita y crear una comisión público-privada que oriente la estrategia de seguridad digital en el país.	Tener un software de antivirus actualizado a disposición del público con licencia gratuita	Crear un proceso licitatorio que permita determinar los requerimientos técnicos, condiciones y características informáticas del desarrollo del software de antivirus, que permita ponerlo a disposición de la sociedad de manera gratuita.	MinTIC	Mediano plazo
			Acompañar el proceso de implementación y creación del software de antivirus, soporte, plan de actualizaciones y lanzamiento del programa de antivirus	MinTIC	Mediano plazo
			Realizar un seguimiento del uso del programa e impacto del software de antivirus gratuito a la sociedad.	MinTIC	Largo plazo
			Crear un plan de comunicaciones centrado en las ventajas de tener un antivirus para la protección de los datos y dispositivos digitales de las personas, usabilidad y otros aspectos.	MinTIC	Corto plazo
		Tener una comisión público-privada que oriente la estrategia de seguridad digital en el país.	Presidir la secretaria técnica de la comisión especial para generar las recomendaciones y documentos que se centren en reducir el delito de hackeo y otros delitos informáticos.	Asobancaria / MinTIC	Corto plazo
			Crear el memorando de entendimiento de los participantes de las mesas técnicas, donde se defina el tiempo, facultad, reuniones y otras características.	Asobancaria / MinTIC	Mediano plazo
			Construir un documento técnico que defina recomendaciones y buenas prácticas de seguridad digital que debe tener los ciudadanos, sector privados y sector público, este documento establece requerimientos mínimos en seguridad de los dispositivos digitales y protocolos de respuesta ante una infección informática a través de un malware.	Asobancaria / MinTIC / Policía / Fiscalía / CRC / SFC	Mediano plazo
SECUNDARIA	Crear un programa de educación financiera radial donde se creen una serie de contenidos que generen conciencia a las personas sobre los factores de riesgo o alertas que deben tener ante el fraude digital.	Lograr un alcance de hasta 1 millón de audioescuchas recurrentes en el programa radial.	Construir conjuntamente la estrategia de la campaña masiva de educación financiera.	Asobancaria / Fiscalía / Policía	Corto plazo
			Realizar una mesa técnica de los departamentos de educación financiera donde se discuta las directrices y la estrategia de las campaña masiva de educación financiera.	Asobancaria / Fiscalía / Policía	Corto plazo
			Crear el contenido del programa de educación financiera masivo, teniendo en cuenta las modalidades, experiencias y aspectos de sensibilización.	Asobancaria / Fiscalía / Policía / MinTIC	Mediano plazo
			Realizar el programa en una duración de 3 meses con un tiempo promedio al aire de 15 horas en radio y 2 horas en Señal Colombia.	Policía / MinTIC	Mediano plazo
		Lograr conformar un programa contra los delitos informáticos que sea recurrente para la sociedad.	Crear campaña de comunicaciones invitando a participar y escuchar las sesiones en radio y televisión a las personas.	Asobancaria / Fiscalía / Policía / MinTIC / Entidades bancarias	Mediano plazo
			Incentivar a los clientes a difundir a través del voz a voz las características del Hackeo y aspectos a tener en cuenta aprendidos en la campaña de educación financiera.	Asobancaria / MinTIC / Entidades bancarias	Corto plazo
			Realizar una medición del impacto del programa con usuarios que recibieron la capacitación y evaluar la posibilidad de hacer más etapas con otros delitos informáticos.	Asobancaria / Fiscalía / Policía / MinTIC	Largo plazo

Nivel	Alternativa	Alcance/Objetivo	Actividades	Responsable	Tiempo de Realización
APOYO	Crear un Proyecto de Ley que faculte a la Superintendencia Financiera de Colombia u otra institución de gobierno a bloquear dominios utilizados para el fraude digital, y que a través de una resolución se cree un procedimiento que permita bloquear las direcciones IP´s de manera más rápida por las Telcos. Así mismo, crear un portal de verificación previa de enlaces, donde los usuarios puedan verificar preventivamente el origen y seguridad de las URL´s.	Crear un proyecto de ley y documentos de políticas publicas para crear un procedimiento para bloquear dominios.	Crear un plan de acción para definir las actividades necesarias para realizar los procedimientos, resoluciones y otras acciones que tiene como objetivo reducir el delito de hackeo en Colombia.	Superintendencia Financiera de Colombia / Policía/Fiscalía	Corto plazo
			Crear el borrador de proyecto de ley que permita a la Superintendencia Financiera de Colombia tener la facultad de bloquear las URL´s utilizadas para implantar programas maliciosos a los dispositivos digitales.	Superintendencia Financiera de Colombia / Policía/Fiscalía	Corto plazo
		Entregar una resolución que establezca un procedimiento que permita bloquear las direcciones IP´s de manera más rápida por parte de las Telcos.	Actualizar el procedimiento de la denuncia de bloqueo de URL´s con el fin de facilitar los prerrequisitos y material probatorio para bloque de enlaces utilizados para implantar malware u otros delitos informáticos.	Fiscalía / Policía	Mediano plazo
			Expedir una resolución que permita definir las características y disposiciones que debe tener las solicitudes de bloqueo de las direcciones IP´s utilizadas para enviar enlaces maliciosos utilizados para hackeo u otros delitos informáticos.	Comisión de Regulación de Comunicaciones / Telcos	Largo plazo
		Crear un portal de verificación previa de enlaces, donde los usuarios puedan verificar preventivamente el origen y seguridad de las URL´s.	Definir el procedimiento de solicitud de bloqueo de las Telcos, conjuntamente con los tiempos de respuesta, documentos técnicos y pruebas de uso indebido de la IP´s para enviar software maliciosos.	Comisión de Regulación de Comunicaciones / Telcos	Largo plazo
			Definir el funcionamiento del portal web sobre cuales serán los canales de denuncia, manejo de la información, procedimientos de bloqueo, gobernanza, operador del portal, entre otros.	MinTIC	Corto plazo
			Realizar un campaña de comunicaciones para informar a los clientes como usar el portal y como pueden denunciar preventivamente una URL maliciosa en la web.	MinTIC / Entidades bancarias	Mediano plazo
			Construir el portal web para denuncias de URL´s maliciosas, con manuales de uso y otras disposiciones.	MinTIC / Fiscalía / Policía	Corto 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

- 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.
- Silva, L., Rentería E. Duque, J., 2011. Análisis comparativo de las principales técnicas de hacking empresarial. Universidad del Pereira. Pereira, Colombia.
- Instituto Nacional de Ciberseguridad – INCIBE, 2016. Tecnologías biométricas aplicadas a la ciberseguridad. Madrid, España.
- Norton, 2018. Cyber Security Insights Report. Recuperado de: https://www.nortonlifelock.com/us/en/newsroom/press-kits/2018-norton-lifelock-cyber-safety-insights-report/
- Cárdenas, J. C., Sensata Research UX., 2022. Estudio de mecanismos comportamentales frente al fraude digital. Recuperado de: https://www.asobancaria.com/wp-content/uploads/2023/02/Estudio_de_mecanismos_comportamentales_frente_al_fraude_digital.pdf

Aso
Ban
Caria

Acerca la
Banca a los
Colombianos