

REPORTE ANUAL

Suplantación de identidad al Banco de Venezuela

2
0
2
4

Investigación realizada por el equipo SOTER

Índice

1. Sobre el Informe	2
1.1. Descargo de Responsabilidad	2
1.2. Nuestro objetivo	2
2. Panorama nacional	4
2.1. Un recuento del estado digital en Venezuela	4
2.2. ¿Qué tan popular es el Banco de Venezuela?	5
2.3. Venezuela en el puesto 65 en el mapeo global de ciberdelincuencia	6
2.4. Avances para incrementar la ciberdefensa	6
3. Dominios fraudulentos BDV registrados durante el 2024	7
4. Análisis de suplantación a través de Instagram	9
4.1. Más de 360 publicaciones de cuentas fraudulentas	9
5. Análisis de suplantación a través de Facebook	11
5.1. Páginas y cuentas fraudulentas	11
5.2. Segmentación y georreferenciación de gastos en publicidad	12
5.3. Más de 500 anuncios de estafas activos en Facebook e Instagram	14
6. Referencias bibliográficas	16
7. ¿Quiénes somos?	17

1. Sobre el Informe

1.1. Descargo de Responsabilidad

El presente informe se ha desarrollado respetando en todo momento la privacidad de los usuarios y la integridad de las plataformas analizadas, que son en su totalidad de dominio público, amparadas en lo establecido en los artículos 48, 57 y 58 de la Constitución de la República Bolivariana de Venezuela, así como en la Ley Orgánica de Telecomunicaciones vigente, en los artículos 2, literales 1, 6 y 8. Las responsabilidades están sujetas a la Ley Especial Contra Delitos Informáticos.

1.2. Nuestro objetivo

El informe ha sido elaborado exclusivamente con datos provenientes de fuentes abiertas, utilizando el método de investigación OSINT (Open Source Intelligence). No contiene información confidencial ni clasificada, y está redactado con un lenguaje accesible para el público en general.

El objetivo del presente informe es reflejar la preocupación por el crecimiento exponencial de los ciberataques contra la población venezolana mediante la suplantación de identidad del Banco de Venezuela, siendo la entidad bancaria actualmente la más grande del país. E igualmente, concienciar y educar a la sociedad sobre los riesgos y la magnitud de esta grave ciberamenaza que, desde nuestra perspectiva como investigadores, consideramos una APT persistente y un flagelo que daña a toda la ciudadanía.

En la primera fase, se procedió a la recolección de información mediante el uso de herramientas de código abierto (Open Source) en distintas redes sociales y, aprovechando técnicas avanzadas con motores de búsqueda, se indexaron grandes cantidades de enlaces fraudulentos con palabras clave como **bdvcreditos**, **bdvenlinea**, **bdvdigital**, **bdvfinanciamiento** y otras similares con

el rango de fecha del objetivo.

Una vez obtenidos los datos, se segmentó en categorías como tipos y métodos de ataques, técnicas empleadas y principal público objetivo de los cibercriminales. Todo esto sirvió de base para elaborar el análisis integral y las estadísticas, logrando obtener una visión más amplia sobre la suplantación de identidad durante el período de 2024, año en el que se identificó, además de lo anteriormente señalado, los estados más atacados y la inversión de los ciberdelincuentes en algunas de las redes sociales.

Es importante señalar que los resultados presentados a continuación no deben considerarse definitivos ni concluyentes. Este informe constituye únicamente una primera etapa en el proceso de diagnóstico, y los datos obtenidos hasta el momento son parte de un camino más amplio que deberá completarse con etapas adicionales de estudio y verificación. Cualquier conclusión o interpretación prematura de estos resultados sería errónea y podría llevar a una visión distorsionada de la situación.

Palabras clave: **Ciberseguridad, Ciberdelincuencia, Ciberamenazas, Banco de Venezuela (BDV), Suplantación de identidad, Phishing, Redes sociales, Dominios fraudulentos, Vishing, Smishing, Ciberdefensa, Consejo Nacional de Ciberseguridad, Ciberespacio, Ciberataques, Ciberguerra, Georreferenciación, Anuncios fraudulentos, Monitoreo de amenazas cibernéticas, Inteligencia de amenazas cibernéticas, APT (Amenaza Persistente Avanzada).**

2. Panorama nacional

2.1. Un recuento del estado digital en Venezuela

Según los últimos informes de la plataforma Datareportal.com, que procesa grandes cantidades de datos y elabora estudios sobre el estado digital de los países, Venezuela ha experimentado un incremento de actividad en el ciberespacio en comparación con años anteriores. Por ejemplo, desde 2019, Venezuela registra un crecimiento continuo del 10 % interanual y, según cifras publicadas por Meta, Facebook tenía más de 14 millones de usuarios activos a nivel nacional a principios de 2024. [1] Esta mejora de la interconectividad no solo indica un mayor acceso a la información en el país, sino también una tendencia a recibir mayor cantidad de ciberataques.

A continuación se presenta una gráfica que muestra la evolución de la dinámica digital en Venezuela desde 2018 hasta 2024. Los datos incluyen la población total, la media de conexiones de telefonía móvil, el número de usuarios de Internet y la cifra de usuarios activos en redes sociales hasta la fecha.

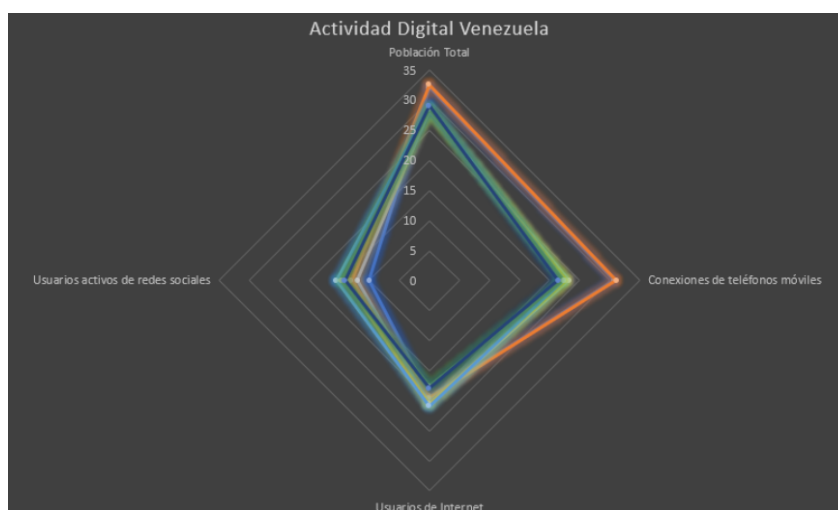


Figura 1: A partir de 2020, la actividad digital a través de teléfonos móviles ha permanecido relativamente estable, con un rango de entre 20 y 23 millones de usuarios activos, lo que convierte al teléfono móvil en el principal medio de acceso a internet en el país. En contraste, la cantidad de usuarios activos en redes sociales ha variado, alcanzando entre 10 y 15 millones de usuarios en el mismo período.

Teniendo en cuenta lo señalado, es Facebook la principal plataforma de interacción a nivel nacional y la fuente principal de ataque para los ciberdelincuentes. De igual forma, aunque el uso del dispositivo móvil sea el predominante, no todos los adultos lo utilizan para acceder a las redes sociales. Esto podría deberse al alto coste de las tarifas de telefonía móvil de las empresas de telecomunicaciones y que en las zonas rurales existe poco acceso a internet.

Por lo tanto, el vishing, el smishing y la suplantación de identidad en las plataformas más solicitadas (por necesidad), como Banco de Venezuela y Patria, son algunas de las opciones más favorables que tienen los cibercriminales para atacar a la población venezolana, sobre todo a sectores sociales populares con poca educación acerca del modus operandi de las ciberamenazas.

2.2. ¿Qué tan popular es el Banco de Venezuela?

La empresa de ciberseguridad gridinsoft.com señala que la institución bancaria actualmente está entre los 10.000 sitios más populares a nivel mundial. Así mismo, dataportal en sus informes periódicos indica que una de las páginas más solicitadas en Google por la población venezolana es Banco de Venezuela.

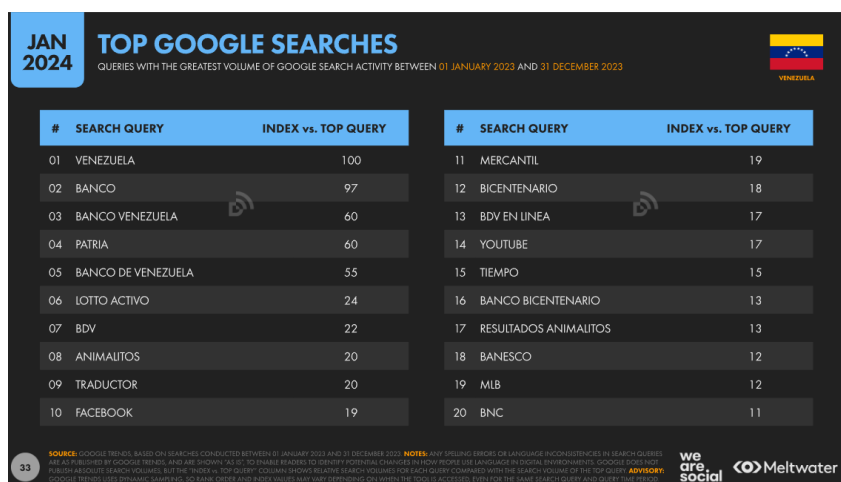


Figura 2: informe digital 2024, Dataportal.com

2.3. Venezuela en el puesto 65 en el mapeo global de ciberdelincuencia

Para el año 2023, según datos ofrecidos por una empresa de ciberseguridad, la nación caribeña se encontraba en el puesto 80 a nivel mundial en cuanto a ciberataques [2]. Esta posición refleja la necesidad de continuar los esfuerzos frente a las ciberamenazas existentes y futuras, para proteger las instituciones gubernamentales y a la población en general.

En abril de 2024, un grupo de investigadores del Departamento de Sociología de la Universidad de Oxford y de la UNSW Canberra Cyber publicó un informe tras 3 años de estudio: **Mapeo de la geografía global de la ciberdelincuencia con el Índice Mundial de Ciberdelincuencia**. Esta investigación, resultado de un profundo análisis, situó a Venezuela en el puesto 65[3].

2.4. Avances para incrementar la ciberdefensa

Luego de las elecciones presidenciales del 28-j, la ministra para Ciencia y Tecnología, Gabriela Jiménez, informó que 126 plataformas tecnológicas del Estado habían sufrido ciberataques.[4] Ante este gran desafío, el Gobierno de la República Bolivariana de Venezuela ha iniciado esfuerzos para incrementar la ciberdefensa en el país; una de las acciones más valiosas ha sido la creación del **Consejo Nacional de Ciberseguridad**, organismo que asesorará al presidente y al Consejo de Defensa del país en la elaboración de la política nacional de ciberseguridad, sus planes y programas de seguridad informática, vigilancia tecnológica, supervisión y control de incidentes telemáticos.[5], así como la inauguración de la **Universidad Nacional de las Ciencias Dr. Humberto Fernández-Morán**, donde estará la carrera de Ingeniería en Ciberseguridad ¹

¹<https://mincyt.gob.ve/inaugurada-universidad-nacional-de-las-ciencias-dr-humberto-fernandez-moran/>

3. Dominios fraudulentos BDV registrados durante el 2024

Aunque el Banco de Venezuela ha mantenido el mensaje en sus plataformas de redes sociales en el que insta a sus usuarios a que no ingresen en enlaces y URL sospechosos e ilegítimos, la forma más común en que los cibercriminales intentan estafar, robar cuentas y dinero, es a través de tácticas de **Ingeniería Social** a través del método phishing con palabras clave como **bdv.sitio.com**, **bdvlatam** o **bdv-onlinea.site**. Estas funcionan como camuflaje o *efecto camaleón* para que la operación sea más efectiva. Además, el contenido siempre va acompañada de imágenes del BDV (Banco de Venezuela) y un corto mensaje llamativo con oferta de créditos y financiamientos².

Cuando el usuario accede al enlace, se redirige automáticamente a una página de inicio similar a la del sitio legítimo, donde se le indica que, para recibir todos los beneficios, debe introducir su nombre de usuario y su contraseña. Una vez que el usuario ha realizado este paso, el cibercriminal obtiene las credenciales de la víctima y vacía su cuenta.

²Los registros presentados no corresponden a la totalidad de los enlaces fraudulentos, ya que existen dominios que no contienen palabras clave relacionadas con el sitio legítimo, como, por ejemplo, fabrmqno.ru.com.



Figura 3: Usuarios en la red social X (antes Twitter) denuncian páginas fraudulentas del BDV 2024

Para lograr conocer los dominios registrados durante el 2024 que han estado suplantando a la página oficial del Banco de Venezuela (bancodevenezuela.com), se filtraron palabras clave ya mencionadas en la página abtdomain.com [6], la cual publica los que se van creando diariamente a nivel global. Los resultados obtenidos indicaron que octubre fue el mes con más registros (13) y, hasta el día 20 de diciembre, hay un total de 60.



Figura 4: Dominios con palabra clave bdv registrados hasta diciembre 2024

Seguidamente, se realizó una verificación en línea a través de la página Whols.com [7] para conocer el estado actual de cada dominio. La gran mayoría están protegidos por Cloudflare o son subdominios y sin datos mayores.

soluciones-bdv.shop venezuela-bdv.com bdv-solicitudes.life
bdv-aplicacion.life bdv-banvanezco.website solicitud-bdv.digital

Figura 5: Algunos dominios fraudulentos encontrados

En contraste, se realizó una filtración por palabra clave haciendo uso de «Banesco» y «Bancaribe», siendo estas dos entidades bancarias reconocidas a nivel nacional. En este análisis, solo se encontraron tres dominios de ambas empresas durante todo el 2024: banesco-online.com, beneficios-banesco.com y banesco.site; bancaribe.com, bancaribe.org y bancaribe.site.

4. Análisis de suplantación a través de Instagram

4.1. Más de 360 publicaciones de cuentas fraudulentas

Las dos grandes redes sociales que los cibercriminales instrumentalizan para atacar a la población venezolana son, principalmente, Facebook e Instagram. Las técnicas incluyen:

- 1. Comprar cuentas falsas antiguas con numerosos seguidores. Los perfiles antiguos son trabajados en su mayoría mediante tácticas de márketing como “sígueme y te sigo” y temas sociales llamativos.**
- 2. Registrar cuentas nuevas y comprar falsos (bots) seguidores, comentarios, «me gusta».**
- 3. Robar cuentas de perfiles legítimos y usarlas de proxys en sus operaciones.**
- 4. Diseñar perfiles con imágenes a través de inteligencia artificial para captar la atención del público objetivo.**

La búsqueda de cuentas asociadas al BVD (Banco de Venezuela) en Instagram se llevó a cabo mediante distintos motores de búsqueda con el rango de fecha objetivo. Los resultados arrojaron 171 perfiles fraudulentos y más de 360 publicaciones de estafas activas.

Cliente BDV CREDITO, ¡AUMENTA TU LIMITE!	https://www.instagram.com/bd.vnetwork/p/DB1UBMCpLPN/
Tu club de Beneficios (@bdv.ajshshshdJehwh)	https://www.instagram.com/bdv.ajshshshdJehwh/
Gomez bolaños gutierrez Te ofrecemos esta oportunidad .	https://www.instagram.com/bdv.beneficio/reel/DDJeT6mxKo8/
bdv (@bdv.com.ven) • Instagram photos and videos	https://www.instagram.com/bdv.com.ven/
¡Somos BDV tu banco de confianza! (@bdv.creditos_)	https://www.instagram.com/bdv.creditos_/
BDV Personal (@bdv.creditos2024)	https://www.instagram.com/bdv.creditos2024/
BDV Art, Design & Living (@bdv.design)	https://www.instagram.com/bdv.design/
BDV En linea (@bdv.digital.enlinea)	https://www.instagram.com/bdv.digital.enlinea/
BDV Personas (@bdv.en.linea)	https://www.instagram.com/bdv.en.linea/reels/
Somos BDV 📄 ¡Solicita tu Crédito Ya! 📄 💰 Monto ...	https://www.instagram.com/bdv.prestamos2024/p/DDE8OXoJ2NR/
AUTORIZADO BDV ve (@bdv.servicios)	https://www.instagram.com/bdv.servicios/
bdv.venezuela.com (@bdv.venezuela.con)	https://www.instagram.com/bdv.venezuela.con/
Instagram photo by bdv venezuela • Nov 1, 2024 at 2:27 AM	https://www.instagram.com/bdv.venezuela.online.comar/p/DB0t3ycxZqq/
bdv.venezuelaa ¡operativo! Obtene tu nuevo biopago, no	https://www.instagram.com/bdv.venezuelaa/p/DC5DZFixA_P/
¡Créditos para empresas y empresarios!	https://www.instagram.com/bdv__creditos/p/DCuN513uVRU/
Accede a tu crédito con el Banco de Venezuela y haz ...	https://www.instagram.com/bdv__creditos_online/p/DDFgoREJvou/
BDV (@bdv_2025) • Instagram photos and videos	https://www.instagram.com/bdv_2025/
Instagram photo by Beneficios de BDV.en linea	https://www.instagram.com/bdv_241074/p/DCDD1v6ScZV/
BANCA MOVIL BDV (@bdv_banca.movil) • صور ومقاطع ...	https://www.instagram.com/bdv_banca.movil/?api=postMessage&hl=ar
BDV Crecimiento financiero Solicita ahora ! Qué esperas ...	https://www.instagram.com/bdv_crecimiento/p/DCKoMSmbvU7/
Bdv Para Ti! QUIERES UNA MOTO Y TIENES POCO ...	https://www.instagram.com/bdv_crediaactualfindemes/p/DACmLh5xnvW/
Instagram video by Bdv • Nov 29, 2024 at 5:13 PM	https://www.instagram.com/bdv_creditoenlinea_/reel/DC-gaEDt0Xv/
Solicita fácil y rápido tu tarjeta de crédito con nosotros	https://www.instagram.com/bdv_creditos2024/p/DC41QxepZW/
@bdv_empresa_ Para clientes de BDV ...	https://www.instagram.com/bdv_empresa_/p/DC0LKATum8G/
BDV en Linea (@bdv_financiero)	https://www.instagram.com/bdv_financiero/
BDV Home Online (@bdv_home_online)	https://www.instagram.com/bdv_home_online/
Banco de Venezuela BDV en linea Empresa!!	https://www.instagram.com/bdv_linea_empresas/
bdv_mercantil_empresa_ Si querés remodelar tu hogar ...	https://www.instagram.com/bdv_mercantil_empresa_/p/DDN3lwTuu-H/
bdv_oficial #EXCLUSIVO PARA CLIENTES BDV BANCO ...	https://www.instagram.com/bdv_oficial/p/C90iG_avcEV/
BDV (@bdv_oficial_2025) • Instagram photos and videos	https://www.instagram.com/bdv_oficial_2025/
Bdv Promociones Solo clientes Banco Venezuela	https://www.instagram.com/bdv_oficial2025/p/DBynbsxp7sj/
Accede a tu crédito con el Banco de Venezuela y haz ...	https://www.instagram.com/bdv_online_creditos/p/DC5nMOHxibR/

Figura 6: Algunas de las cuentas fraudulentas encontradas

Así mismo, el análisis reveló que los ciberdelincuentes intentan obtener resultados ofreciendo promociones exclusivas como incrementar el crédito bancario, acceder a financiamientos o solicitar tarjetas de crédito.

5. Análisis de suplantación a través de Facebook

Algunos usuarios han denunciado públicamente que 5 de 6 anuncios en alusión al Banco de Venezuela que se encuentran en la red social corresponden a páginas fraudulentas y a estafas. En la búsqueda de perfiles y páginas ilegítimas en esta red social, los resultados son incluso más preocupantes que en Instagram, a pesar de que el número de cuentas es inferior.

5.1. Páginas y cuentas fraudulentas

Los resultados arrojaron 155 cuentas activas con subdominios phishing, sobre todo aquellos que están alojados en replit.dev. Al sumar esta cantidad con los 60 dominios registrados, para diciembre 2024, podrían haber más de 215 páginas y perfiles en Facebook intentando robar a usuarios del Banco de Venezuela.

Uno de los patrones que se ha identificado entre los ciberdelincuentes es que puede tener varias cuentas de redes sociales. Además, puede interconectarlas para que lo publicado en Instagram se vea también en Facebook, lo que le permite ampliar significativamente la presencia digital.



Figura 7: Realizando una comparación con los datos indexados entre las cuentas y páginas de ambas plataformas, Facebook tiene un 52 % frente a un 48 % de Instagram.

5.2. Segmentación y georreferenciación de gastos en publicidad

La empresa Meta tiene una sección donde publica datos sobre los anuncios publicados ³. Parte del trabajo fue obtener la información del 2024 mediante la palabra clave **bdv**. Sumando lo invertido por cada cibercriminal, el monto total asciende a 18.800.708 bf. La información solo corresponde a anuncios ya finalizados, ya que los activos aún no están reflejados.

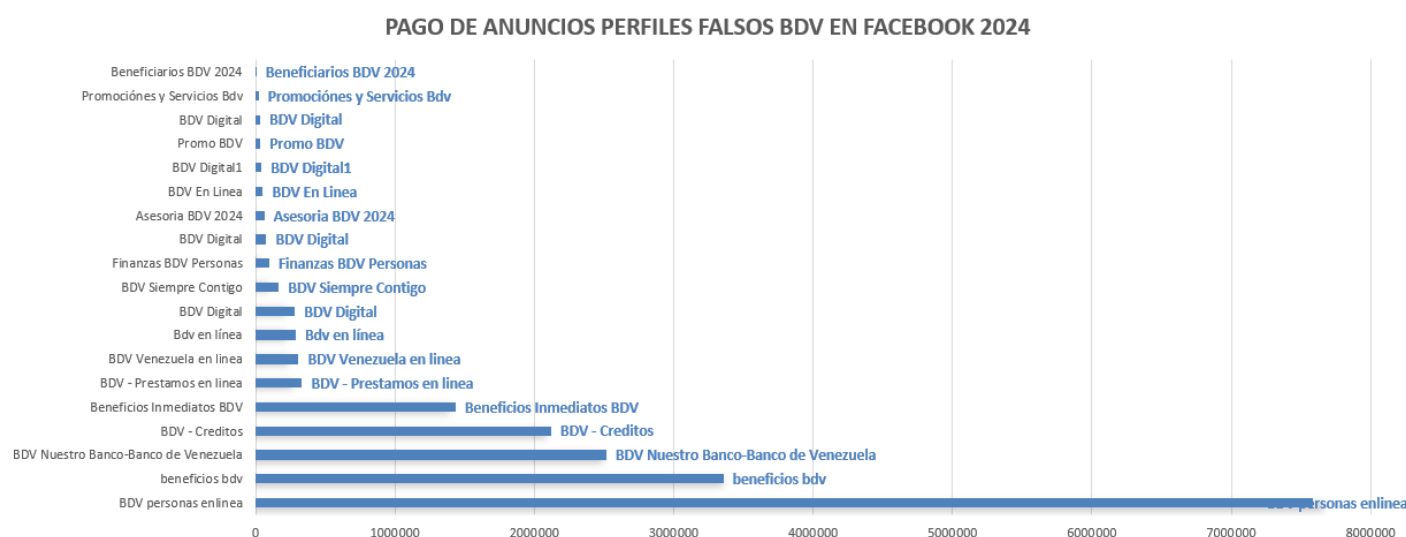


Figura 8: Para la construcción de esta gráfica se usaron los datos públicos ofrecidos por Meta. La información incluye pago de anuncios de Facebook e Instagram.

Luego de conocer cada página y perfil, se procedió a analizar uno por uno los anuncios. Meta ofrece la oportunidad de ver regiones geográficas, género y rango de edad de los usuarios a los que estaban dirigidos los anuncios ⁴ fueron los objetivos. Con la información obtenida y procesada, el porcentaje de estados más atacados se dividió de la siguiente manera:

- **Zulia:** 18 %
- **Caracas:** 11 %
- **Carabobo:** 8 %
- **Bolívar:** 7 %
- **Lara:** 6 %
- **Anzoátegui:** 5 %
- **Aragua:** 5 %
- **Miranda:** 4 %
- **Sucre:** 4 %
- **Táchira:** 4 %
- **Portuguesa:** 4 %
- **Falcón:** 3 %
- **Guárico:** 3 %
- **Mérida:** 3 %
- **Barinas:** 3 %
- **Monagas:** 3 %
- **Yaracuy:** 2 %
- **Apure:** 2 %
- **Trujillo:** 2 %
- **Nueva Esparta:** 1 %
- **Cojedes:** 1 %

³<https://www.facebook.com/ads/library/report/?source=nav-header>

⁴La sección solo refleja datos de Mujer y Hombre, sin incluir otras categorías de género

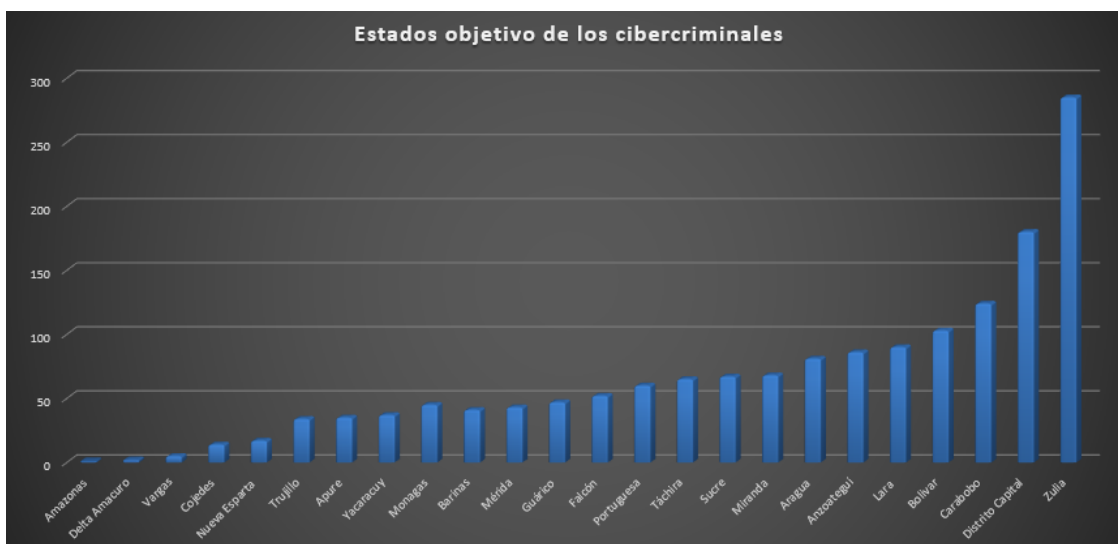


Figura 9: estados más atacados por los cibercriminales 2024

Las edades en Meta están divididos en 18-24, 25-34, 35-44, 45-54, 55-64, 65+ . Los resultados reflejaron que las mujeres son las más atacadas y que las adultas de 40 años en adelante son el principal objetivo.

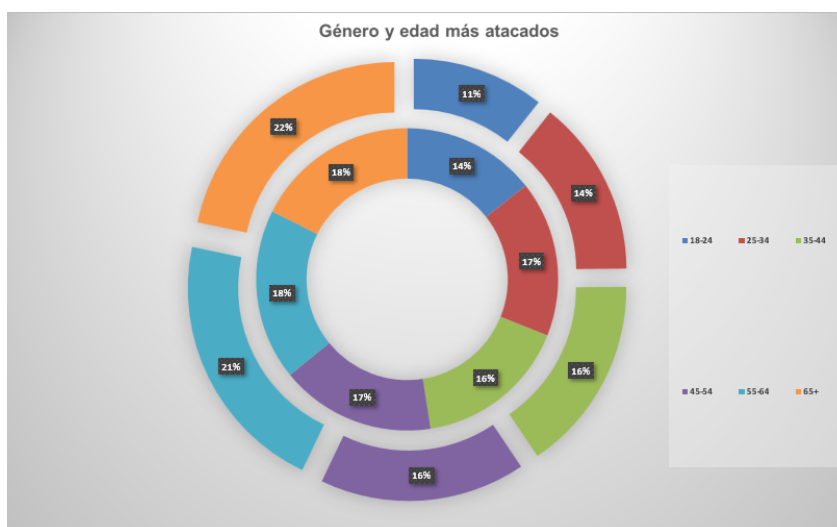


Figura 10: El anillo externo corresponde al porcentaje de edad y género femenino. Como se observa, las adultas a partir de 65 años tienen el valor más alto con un 22 %, seguidamente el rango de edad entre 55-64 un 21 %.

5.3. Más de 500 anuncios de estafas activos en Facebook e Instagram

En la sección de **biblioteca de anuncios**, la empresa publica los anuncios activos e inactivos semanalmente. Haciendo la búsqueda con la palabra clave **bdv**, se observaron más de 500 resultados en 2024. Solo en el mes de diciembre, hasta el día 27, existen cerca de 200 anuncios activos intentando estafar a los clientes del Banco de Venezuela.

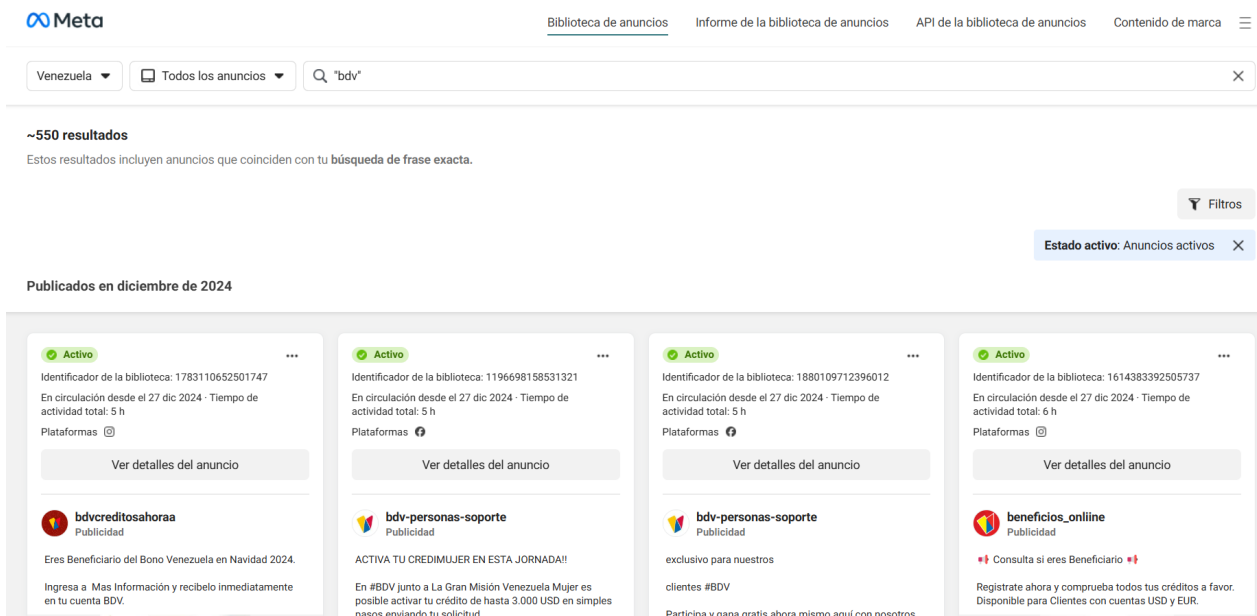


Figura 11: Captura de pantalla de la sección de anuncios de Meta. En la parte superior izquierda se pueden observar los resultados obtenidos a través de los filtros solicitados con la palabra bdv.

Meta, al permitir la manipulación de las URLs y el pago de publicidad sin alguna autenticación, facilita que los atacantes engañen al objetivo. En la sección de «**Información de la página**», se pueden observar algunos de los países con más administradores. Los principales incluyen a Venezuela, Colombia, México y Ecuador.

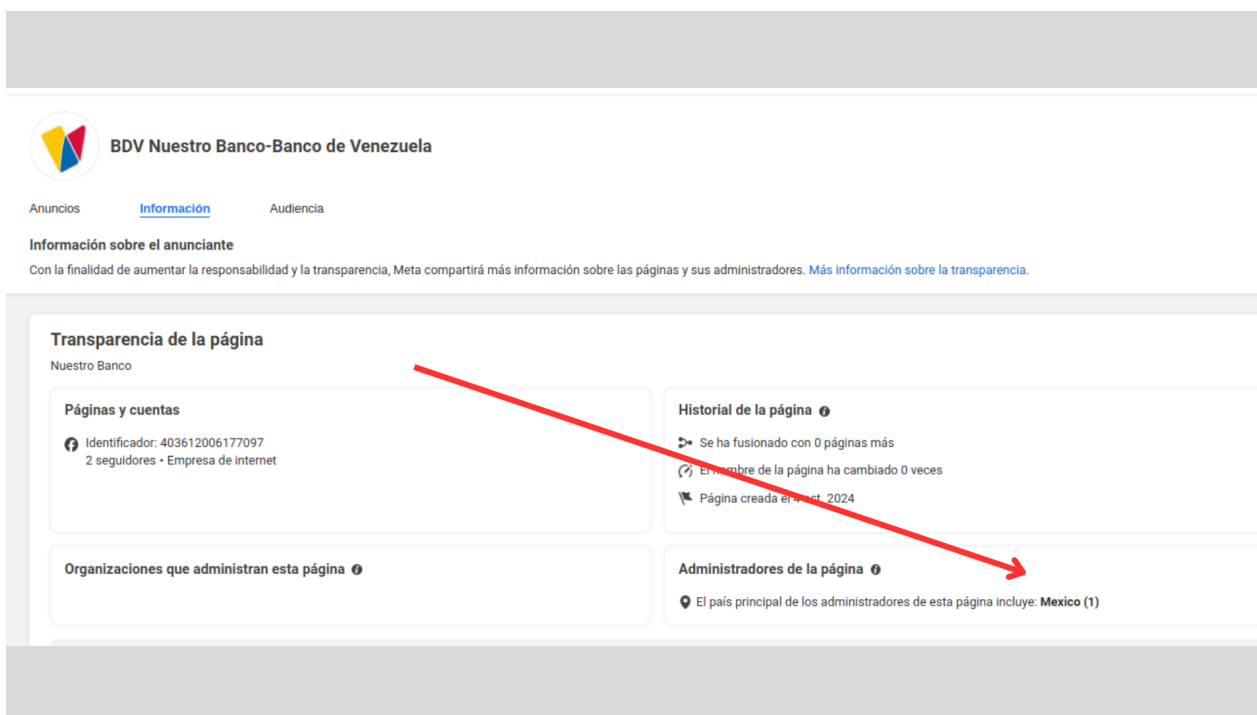


Figura 12: captura de pantalla biblioteca de anuncios Meta

Otro factor importante es la moneda de pago que aparece reflejada en la información de los anuncios. En la gran mayoría de los casos, se trata de moneda mexicana o colombiana. Estos elementos concuerdan con la reciente detención⁵ realizada por el Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC) en el estado Zulia, tras varias denuncias de usuarios del Banco de Venezuela que habían sido estafados con falsos anuncios de créditos y financiamientos. Al detenido se le incautaron varias tarjetas SIM de origen internacional y tarjetas de crédito colombianas, lo que podría indicar que los cibercriminales aprovechan la facilidad de registro y de método de pagos para intentar pasar desapercibidos.

⁵Detenido por estafar con anuncios falsos del Banco de Venezuela en redes socialeselcooperante. (2024, 9 diciembre). elcooperante.com. <https://elcooperante.com/detenido-por-estafar-con-anuncios-falsos-del-banco-de-venezuela-en-redes-sociales/>

6. Referencias bibliográficas

Referencias

- [1] Kemp, S. (2024, 23 de febrero). *Digital 2024: Venezuela — DataReportal – Global Digital Insights*. DataReportal – Global Digital Insights. <https://datareportal.com/reports/digital-2024-venezuela>.
- [2] González, T. (2023, 3 marzo). *Venezuela se encuentra en el puesto 80 de los países que más sufren ciberataques*. El Diario. <https://eldiario.com/2023/03/03/venezuela-entre-paises-con-mas-ciberataques/>.
- [3] Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., Varese, F. (2024). *Mapping the global geography of cybercrime with the World Cybercrime Index*. PLoS ONE, 19(4), e0297312. <https://doi.org/10.1371/journal.pone.0297312>.
- [4] Universal, D. E. (2024, 20 agosto). *Más de 120 plataformas tecnológicas de Venezuela sufrieron ciberataques*. El Universal.. <https://www.eluniversal.com/politica/189033/mas-de-120-plataformas-tecnologicas-de-venezuela-sufrieron-ciberataques>
- [5] Perez, D. (2024, 20 de agosto). *Gaceta oficial: Creado Consejo Nacional de Ciberseguridad*. <http://mippi.gob.ve/index.php/2024/08/20/gaceta-oficial-creado-consejo-nacional-de-ciberseguridad/>
- [6] (2024b, diciembre 20). *ABTDomain - All about domain*. ABTdomain. Recuperado de <https://abtdomain.com/>
- [7] *Whois.com - Domain Names. Identity for Everyone*. (s.f.) <https://www.whois.com/>.

7. ¿Quiénes somos?

SOTER es un grupo de jóvenes profesionales entusiastas interesados en la seguridad digital y la ciberseguridad. Nos especializamos en ciberdefensa y OSINT. Algunos de nuestros servicios incluyen:

- Apoyo en planificación
- Estudio y análisis de mercado
- Estudio y análisis de competencia
- Evaluación de estrategias de mercado.
- Análisis de producto y recomendaciones estratégicas
- Diseño e implementación de normas ISO27001
- Estudio integral de ciberseguridad para empresas
- Recolección y análisis de Datos
- Análisis de tendencias en RRSS y operaciones psicológicas
- Monitoreo de amenazas
- Estudio y análisis de campañas negras
- Investigación en redes sociales y fuentes públicas
- Identificación de noticias falsas
- Informes estratégicos
- Implementación y auditoría, pentesting, etc

Nuestro canal Telegram

<https://t.me/CiberseguridadEnVenezuela>

