ESPECIALIZACIÓN EN CIBERSEGURIDAD

GRADO DE SENSIBILIZACIÓN EMPRESARIAL DE LAS VULNERABILIDADES EXPUESTAS A TRAVÉS DE FUENTES ABIERTAS (OSINT) EN LOS PAISES DE SUR AMERICA

JHON CESAR ARANGO SERNA

Universidad® Católica de Manizales
VIGILADA MINEDUCACIÓN
Obra de Iglesia de la Congregación
Hermanas de la Caridad Dominicas de La Presentación de la Santísima Virgen

GRADO DE SENSIBILIZACIÓN EMPRESARIAL DE LAS VULNERABILIDADES EXPUESTAS A TRAVÉS DE FUENTES ABIERTAS (OSINT) EN LOS PAISES DE SUR AMERICA

Modalidad de grado: Monografía

Asesor: Hector Roberto Gordon Quinche

Jhon Cesar Arango Serna

UNIVERSIDAD CATÓLICA DE MANIZALES
FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESPECIALIZACION EN CIBERSEGURIDAD
MANIZALES, CALDAS
2023

NOTA DE ACEPTACIÓN: 5.0 – TRABAJO MERITORIO

DEDICATORIA

A DIOS, por permitirme escoger estar aquí

a mi MADRE por su amor incondicional.

a mi HIJO quien es mi orgullo, esta tesis es tuya.

a mi compañera de viaje, por tenerme paciencia, sin ti esto no sería posible.

AGRADECIMIENTOS

A la Universidad Católica de Manizales, por esta excelente oportunidad, a las personas que hicieron que esta tesis fuera una realidad; Hector, David, Carolina y Andrés gracias por ser parte de esta tesis, los llevo en mi corazón.

Tabla de contenido

Lista de Figuras

RESUMEN

A medida que avanza la tecnología, las técnicas de OSINT que es la búsqueda de información a través de fuentes abiertas han tomado bastante importancia. En lo relacionado con la seguridad de la información digital para los profesionales de la ciberseguridad ha cobrado mucho valor como técnicas en su quehacer diario, pero para la ciberdelincuencia se ha convertido en la navaja suiza necesaria para el descubrimiento de vulnerabilidades empresariales con posibilidad de explotación, sin el uso de técnicas avanzadas que se espera en este tipo de actividad.

El presente trabajo muestra el grado de vulnerabilidades que las fuentes abiertas exponen mes a mes a través de su plataforma más importante, con el fin de medir el grado de sensibilización que posee las empresas para combatir los riesgos cibernéticos.

Sin duda este trabajo servirá de apoyo a los profesionales de la ciberseguridad como una guía de sensibilización de las vulnerabilidades a las que puede estar las empresas expuestas y que son fácil accesos a través de internet

ABSTRACT

As technology advances, OSINT techniques, which is the search for information through open sources, have become quite important. In relation to the security of digital information, for cybersecurity professionals it has gained a lot of value as techniques in their daily work, but for cybercrime it has become the necessary Swiss army knife for the discovery of business vulnerabilities with the possibility of exploitation. without the use of advanced techniques that is expected in this type of activity.

This paper shows the degree of vulnerabilities that open sources expose month by month through their most important platform, in order to measure the degree of awareness that companies have to combat cyber risks.

Undoubtedly, this work will serve as a support for cybersecurity professionals as a guide to raise awareness of the vulnerabilities to which companies may be exposed and that are easily accessible through the Internet.

INTRODUCCIÓN

La dependencia cada día de la red de datos ha hecho que las tanto las personas como las empresas compartan sus contenidos digitales en internet, tal es el caso de los portales Web, portales transaccionales, redes sociales, bases de datos comerciales y no comerciales, Etc.

Esto a su vez trae consigo el nacimiento de lo que llamamos fuentes abiertas, que se define como todo portal o software que permite encontrar cierta información que puede estar publicada en internet y que no tiene ninguna restricción para su consulta. Sin embargo. Esta información puede tener datos sensibles que pueden ser usados por ciberdelincuentes para su uso propio en contra de un objetivo determinado.

Es ahí donde la búsqueda de información en fuentes abiertas, conocido también con el nombre de OSINT (Wikipedia, Wikipedia, 2022) (Open Source Intelligent) se ha convertido poco a poco, no solo para el profesional de ciberseguridad, sino también para el ciberdelincuente en una técnica que permite de una forma ágil descubrir información sensible de un objetivo específico.

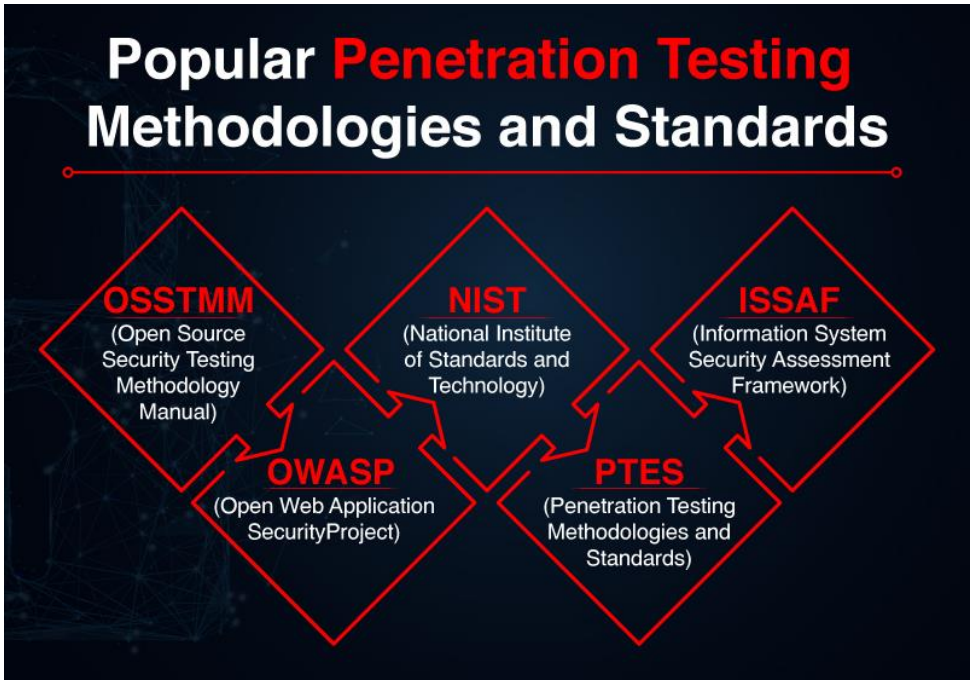
Uno podría pensar que a medida que avanza la tecnología podemos contar con sistemas más y más robustos y seguros, sin embargo, la forma de percibir la tecnología cae con las fuentes abiertas ya que a través de ellas las empresas sin saberlo están compartiendo a nivel mundial sus activos de información digital que pueden o no estar debidamente aseguradas para ser expuestas a la red de internet.

SITUACIÓN PROBLEMÁTICA

La búsqueda de vulnerabilidades a través de fuentes abiertas, ha expuesto a muchas empresas ante los ciberdelincuentes, trayendo consigo problemas que no solo tienen que ver con la Integridad, Confidencialidad y Disponibilidad de la información, sino que también recae en su productividad que implica grandes pérdidas tangibles e intangibles de su activo más valioso, La Información.

Los ciberdelincuentes actuales ya usan las fuentes abiertas como técnicas que hacen parte de las fases del Pentesting (Wikipedia, 2011), que sin duda en su mayor parte los lleva de la etapa del reconocimiento a la explotación evitándose a si el arduo camino del escaneo y enumeración. Ver **Figura 1**.

Figura 1. Metodologías y Estándares de Pentesting



PROBLEMA DE LA INVESTIGACIÓN

¿Las empresas son conscientes de la información expuesta de sus activos de información digital a través de fuentes abiertas.? (esto me lleva a una encuesta)

¿Las empresas son sensibles a las vulnerabilidades expuestas de sus activos de información digital a través de fuentes abiertas y hacen los correctivos necesarios?

OBJETIVOS

Objetivo General

Realizar un estudio de las vulnerabilidades expuestas en el último año 2022 a nivel empresarial de la información expuesta a través de fuentes abiertas.

Objetivos Específicos

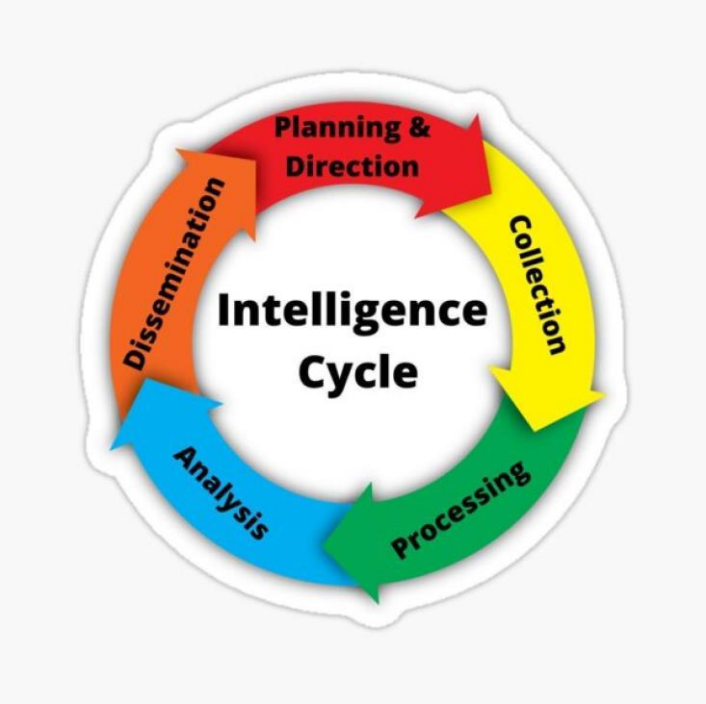
- Conocer el grado de sensibilización empresarial de las vulnerabilidades expuestas a través de la fuente abiertas como Shodan
- Categorizar las vulnerabilidades expuestas mes a mes, discriminadas por productos, puertos, sistemas operativos, países de sur América y por ciudades.
- Presentar estadísticas en base a esta investigación para que sirvan como fuente de información a las empresas y gremios de ellas se exponen.
- Exponer la realidad de nuevas técnicas usadas por ciberdelincuentes para el fácil acceso a activos de información a través de fuentes abiertas.

ANTECEDENTES

Podemos concluir que la era digital ha traído consigo grandes beneficios a nivel mundial, pero ha llevado también a una era de (des) información donde tanto las personas como las empresas sufren sus consecuencias, el termino Osint no es nuevo, ha cobrado mucha importancia en los últimos tiempos “Su origen se asocia al ámbito militar y se remonta a los años de la Segunda Guerra Mundial, en los que el FBIS (Foreing Broadcast Information Services) creado en 1941 por los Estados Unidos utilizaba las fuentes abiertas” (Seisdedos & Aguilera , 2020).

Antes de definir el termino de OSINT, primeros debemos hablar de lo que es inteligencia y para ellos nos basaremos en el gráfico de los 4 ciclos de la inteligencia propuesta por la OTAN. [1] (**Ver Figura 2**)

Figura 2 – Ciclo de la Inteligencia



[1] La Organización del Tratado del Atlántico Norte (**OTAN**)

La **inteligencia** es un concepto difícil de definir. Una definición sencilla la describe como la capacidad de generar información nueva combinando la que recibimos del exterior con aquella- de la que disponemos en nuestra memoria. Se trata de una capacidad general que implica varios factores: el pensamiento abstracto dirigido hacia la resolución de problemas o en la capacidad de adquirir conocimientos. La inteligencia implica en adquirir una seria de datos, para luego ser procesados y analizados con el fin de generar datos de utilidad para el analista.

La inteligencia puede ser aplicada en varios entornos, por ejemplo, en fuentes humanas los que se conoce con el nombre de HUMINT, en señales de radio lo que conlleva al SIGINT, en redes sociales lo que se llama SOCINT y por último la que representa la base de esta investigación, la que implica las fuentes abiertas que efectivamente se consideran de una fuente publica como Radio, Televisión, Internet conocido como OSINT.

No podemos caer en el error de confundir una fuente publica con una fuente gratuita ya que la fuente abierta permite acceder a la información de una manera legal, aunque de ello dependa de una suscripción mediante un pago.

JUSTIFICACIÓN

La presente investigación se justifica porque constituye una nueva metodología en que los profesionales de la ciberseguridad se podrán basar para descubrir los riegos tecnológicos tangibles a los que una organización puede estar expuesta a través de fuentes abiertas, por otro lado; los resultados de este estudio permitirán sensibilizar a las empresas en la importancia de asegurar sus activos de información digital antes de ser expuestos a la red de Internet.

CONTEXTO GEOGRAFICO

A pesar de que las técnicas de Osint son mundiales y podremos extraer información de cualquier parte del mundo, nos centraremos exclusivamente a los países de Sur América. Ver **Figura 3** - Mapa Político - Sur América

MARCO CONCEPTUAL

Vulnerabilidad Informática

Se define como la deficiencia que existe en un sistema de Software o de Hardware y que puede ser aprovechado por una persona mal intencionada (Intruso) que puede comprometer la Confidencialidad, Integridad y Disponibilidad de la información digital bien sea de una organización o una persona.

Osint

El termino OSINT hace referencia al conjunto de técnicas y herramientas para recopilar información de fuentes abiertas como lo puede ser radio, televisión, internet y prensa; para luego ser analizadas y correlaciones convirtiéndolas así en un nuevo conocimiento útil.

OSINT puede ser usada en muchos ámbitos: Financieros, Sociales, Policial, Militar, Político, Etc. Si nos centramos en el ámbito Tecnológico y concretamente en la Ciberseguridad, Osint puede ser usado para descubrir los activos de información de una organización o para descubrir información de una persona debido al exceso de la misma que esta pública.

Existe una variedad de fuentes abiertas que se consiguen en la red de datos de Internet, que tienen su propia especialidad como son los propios buscadores, las redes sociales y buscadores de dispositivos que están en línea. Ver **Figura 4**.

Figura 4 - Fuentes Abiertas

Api

El término API es una abreviatura de Application Programming Interfaces, que se traduce como una interfaz de programación de aplicaciones. Se trata de un código o token que es entregado por algunas fuentes públicas, que permite utilizar sus herramientas de una forma avanzada.

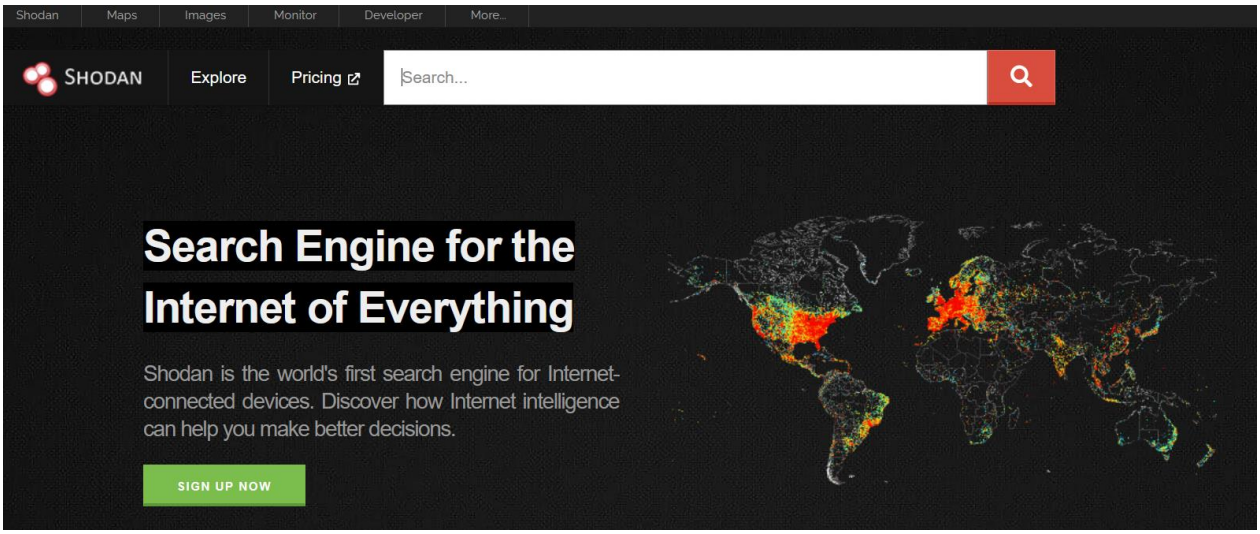
Shodan

En Shodan puedes encontrar información sobre los dispositivos conectados en Internet a través de una dirección IP pública. Por lo tanto, verás datos como el sistema operativo, la versión, el tipo de dispositivo y más sobre un que un puerto o servicio.

Incluso puedes ver capturas de pantalla y transmisiones de cámaras de seguridad en vivo. Esto ocurre debido a que muchos sistemas informáticos no configuran su ciberseguridad de forma correcta. Por ello, se puede acceder a algunos puertos confidenciales sin necesidad de usar un nombre de usuario y contraseña.

Gracias a buscadores como Shodan, un profesional de la ciberseguridad o un ciberdelincuente podrá obtener información muy relevante sin necesidad de realizar un escaneo activo hacia si objetivo. La mayoría de esta información han sido guardados y publicados por este motor de búsqueda. Shodan es uno de los buscadores para encontrar dispositivos escaneados más confiables y suele utilizarse bastante en el mundo del hacking ético y la seguridad informática. Ver **Figura 5**.

Figura 5 - Shodan



Shodan es una fuente abierta que permite la búsqueda de los dispositivos en línea como routers, equipos, cámaras web, etc. Fue lanzado en el año 2009 con el fin de buscar dispositivos integrados a Internet. A través de su API, permite el uso avanzado de la herramienta, lo que conlleva a convertirse en una herramienta muy poderosa y a su vez muy peligrosa.

En mayo de 2013 CNN Money[2] público un artículo donde mencionaba los peligroso de dicha herramienta al exponer sistemas de control de tráfico, a su vez en el mismo año la empresa Forbes[3] saca un artículo donde explica que Shodan se utilizó para encontrar fallos en cámaras web y por mencionar otra referencia, la CSO Online[4] público un artículo donde referencia las ventajas y desventajas de la herramienta, haciendo énfasis a las exposición de vulnerabilidades de dispositivos del Internet de las Cosas.

[2] https://money.cnn.com/gallery/technology/security/2013/05/01/shodan-most-dangerous-internet-searches/index.html

[3] https://www.forbes.com/sites/kashmirhill/2013/09/04/camera-company-that-let-hackers-spy-on-naked-customers-ordered-by-ftc-to-get-its-security-act-together/?sh=51d0f1a738ef

[4] https://www.csoonline.com/article/2867407/shodan-exposes-iot-vulnerabilities.html

Al utilizar Shodan, puedes especificar tu búsqueda. Por medio del uso de filtros, que te ayuda a localizar dispositivos determinados, algunos de estos filtros te permiten clasificar sus resultados por:

- Ciudad.
- País.
- Coordenada.
- Hostname.
- Organización
- Dirección IP.
- Sistema operativo.
- Puerto.
- Etc.

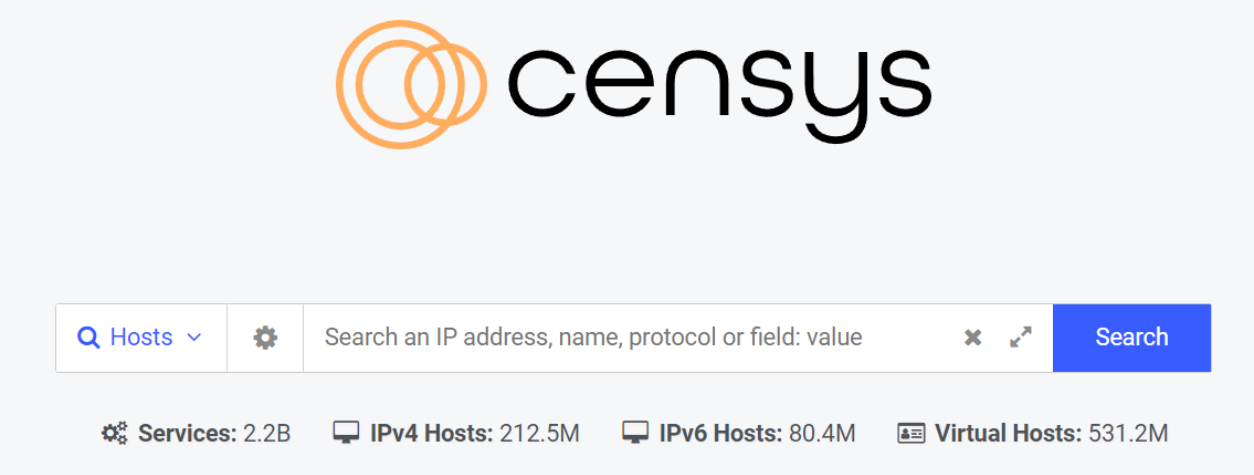
Sin duda que Shodan, es catalogado por muchos como el buscador más peligroso que existe en la red de internet.

Censys

Censys es un servicio de motor de búsqueda y procesamiento de datos a través el cual un usuario puede realizar consultas sobre equipos, programas y redes que componen la Internet. Para ello, el sistema colecciona información sobre todos ellos valiéndose de dos programas específicos: ZMAP y ZGrab, que se encargan de explorar el espacio de direcciones IPv4.

Este buscador, cuya alimentación de datos se realiza con la cooperación de Google, ya ha permitido a distintas compañías de seguridad y a ciberdelincuentes descubrir que un importante número de routers, módems, cámaras IP, teléfonos VoIP, etc., se hallan expuestos en internet por la falta de seguridad en sus configuraciones. Ver **Figura 6**

Figura 6 – Censys



Criminal Ip

Es un motor de búsqueda OSINT de seguridad prometedor con un revolucionario sistema de búsqueda basado en IP y tecnología de seguimiento. Este sistema utiliza inteligencia de amenazas cibernéticas basada en IP para proporcionar funciones de BÚSQUEDA e INTELIGENCIA para que los usuarios encuentren toda la información de Internet sobre activos de TI, como direcciones IP y enlaces maliciosos, sitios de phishing, certificados, sistemas de control industrial, IoT, servidores, CCTV, etc.

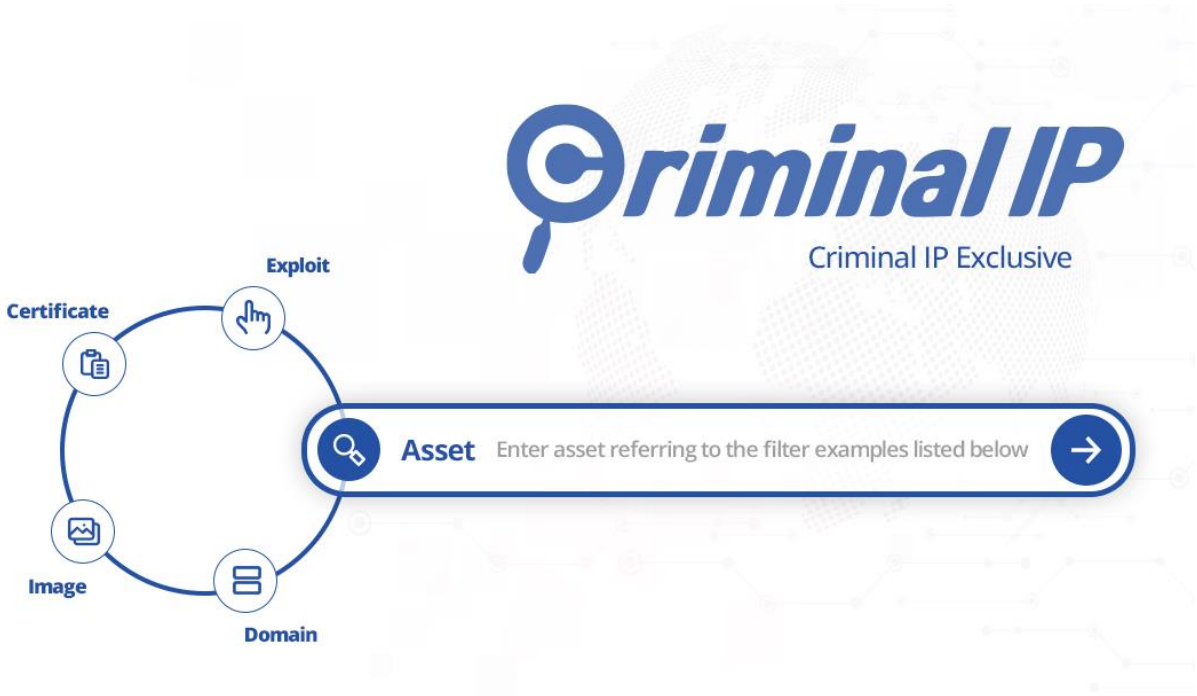
Criminal IP proporciona resultados de búsqueda a partir de palabras claves ingresadas y las compara con la información almacenada en sus registros. Permite reducir los resultados a través del uso de filtros y los usuarios también pueden encontrar puertos abiertos y vulnerabilidades, geolocalización de IP, así como registros de abuso para realizar un seguimiento de las direcciones IP maliciosas. Criminal IP actualmente ofrece 4 modos de búsqueda diferentes:

- Búsqueda de activos
- Búsqueda de dominio
- Búsqueda de imágenes

- Búsqueda de exploits

Criminal IP permite la opresión en un servicio Beta gratuito, lo que significa que todos pueden acceder a esta útil tecnología de forma gratuita. Ver **Figura 7**

Figura 7 - Criminal IP



Zoomeye

El primer motor de búsqueda del ciberespacio de China, algo preocupante ya que es la competencia directa de los motores de búsquedas americanos como Shodan, Censys y Criminal IP. ZoomEye mapea el ciberespacio local las 24 horas del día, los 7 días de la semana a través de una gran cantidad de nodos de mapeo y encuestas globales basadas en IPv6, IPv4 y bases de datos de nombres de dominio del sitio. Ver **Figura 8**

Figura 8 - ZoomEye

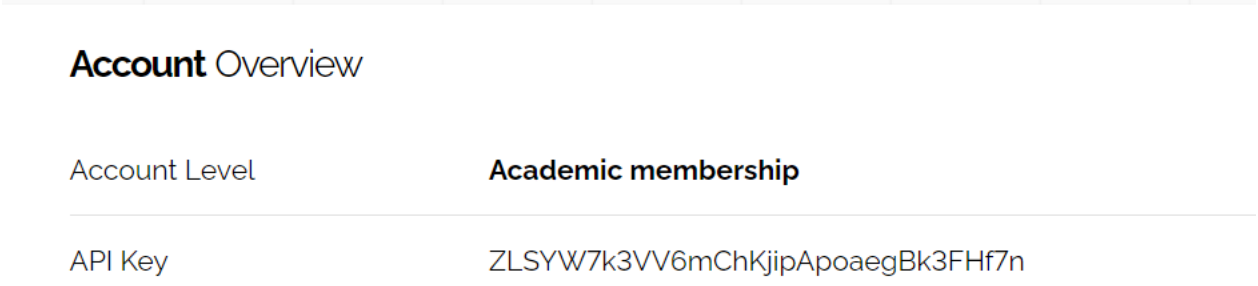
Puede utilizar este buscador para descubrir activos de destino de forma precisa y rápida. Para ello, cuentan con múltiples tipos de equipos como una router, CDN, Big Data, grabadoras de voz, CMS, frameworks web, plataformas de software y mucho más.

También puede buscar por temas especiales y verificar la evaluación del impacto de la vulnerabilidad. Estos temas incluyen bases de datos, industrias, Servicios, firewalls, enrutadores, almacenamiento en red, cámaras, impresoras, WAF, almacenamiento en red, etc., y verifique los informes para tener una idea detallada.

El Poder De Las Api's Keys

Una de las características especiales que tienen los buscadores antes explicados, es el uso de su API, pues ellas permiten automatizar a través de código muchas de las consultas para extraer información útil para el investigador. . Ver **Figura 9**

Figura 9 - Ejemplo API de Shodan



Las API's sin duda hacen que estos buscadores se vuelvan peligrosos porque con la consulta adecuada, un ciberdelincuente puede conocer en segundos las vulnerabilidades registradas en una zona específica y gracias a estos resultados, poder automatizar la ejecución de un ciber ataque de forma masiva, tema que desarrollaremos en el presente proyecto.

MARCO LEGAL

¿Qué tan legal es la actividad que realiza los buscadores como Shodan, Zoomeye, Censys o Criminal IP, para que sin autorización de las empresas estos indexen la información de sus activos que están expuestos en Internet y la coloquen a disposición de los usuarios que poseen cuentas en estas plataformas, exponiendo así la información de puertos, servicios o incluso vulnerabilidades a los que están expuestas las organizaciones? Sin duda, esta es la pregunta que se hacen todos, cuando conocen estas plataformas.

La respuesta es realmente sencilla, estos motores de búsquedas se basan en el principio de buscar todo aquello que tenga un IP Publica, es decir todo lo que está expuesto en la red de Internet, por lo que su uso es completamente legal, ya que se limita a mostrar información que ya de por si está expuesta. En cambio, lo que no es legal es acceder a los servidores que se muestran en los resultados, ya que puedes estar cometiendo delitos de ciberdelincuencia.

Estas plataformas tratan de ofrecer a sus usuarios ciertas reservas, brindando un servicio cuidadosamente limitado y sus resultados dependen del tipo de cuenta que se crea con ellos. Pero igual el uso legítimo y malicioso depende del usuario final.

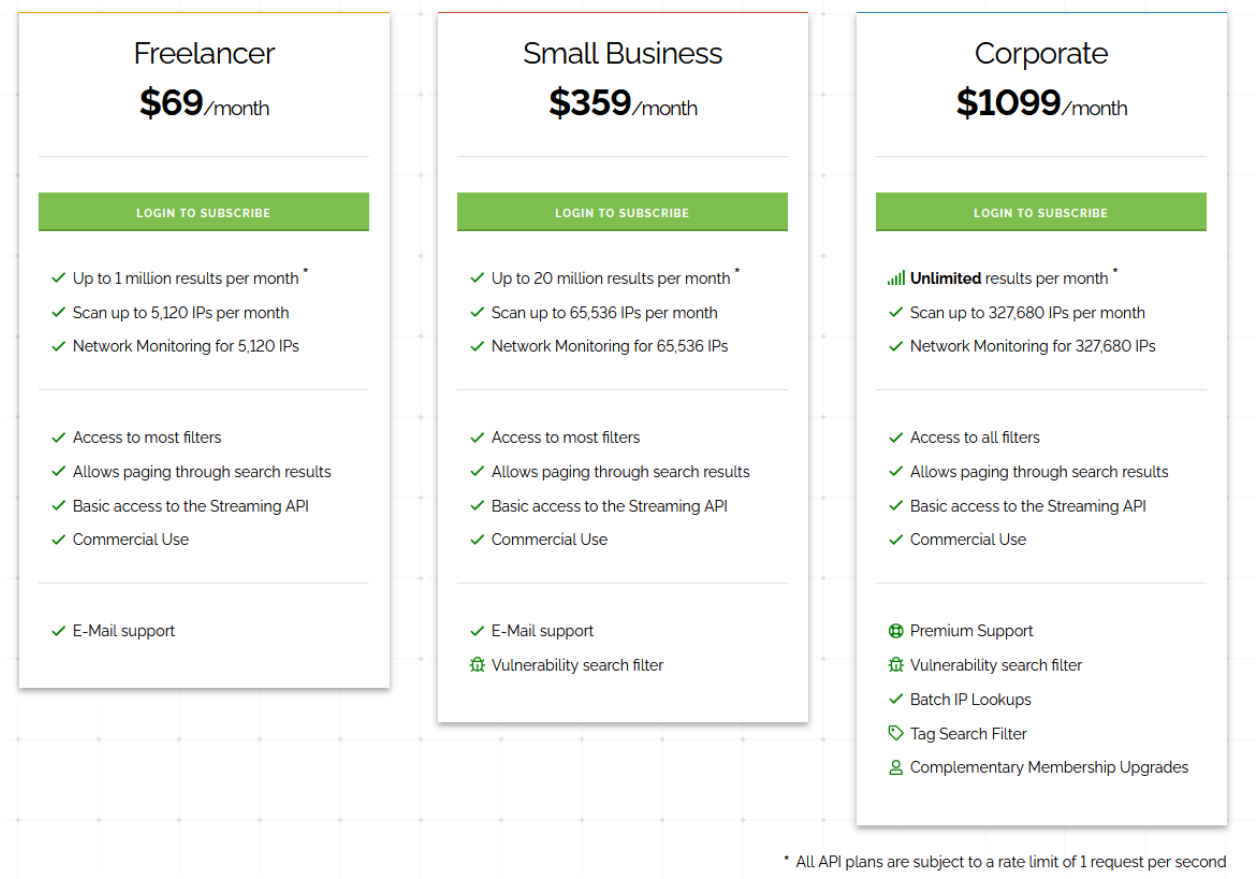
Otro tema a tener en cuenta es la jurisdicción donde operan estas plataformas, que deben ser legales, de lo contrario estos buscadores ya se habrían cerrado.

DESARROLLO DEL PROYECTO

Selección De La Fuente De Información

Según lo expuesto ya en el marco conceptual, el presente trabajo se hará con la herramienta SHODAN, para ello se obtiene un API adecuada para poder extraer la información requerida, a pesar del tipo de licenciamiento de dicha herramienta. Ver **Figura 10**

Figura 10 – Licenciamiento Shodan

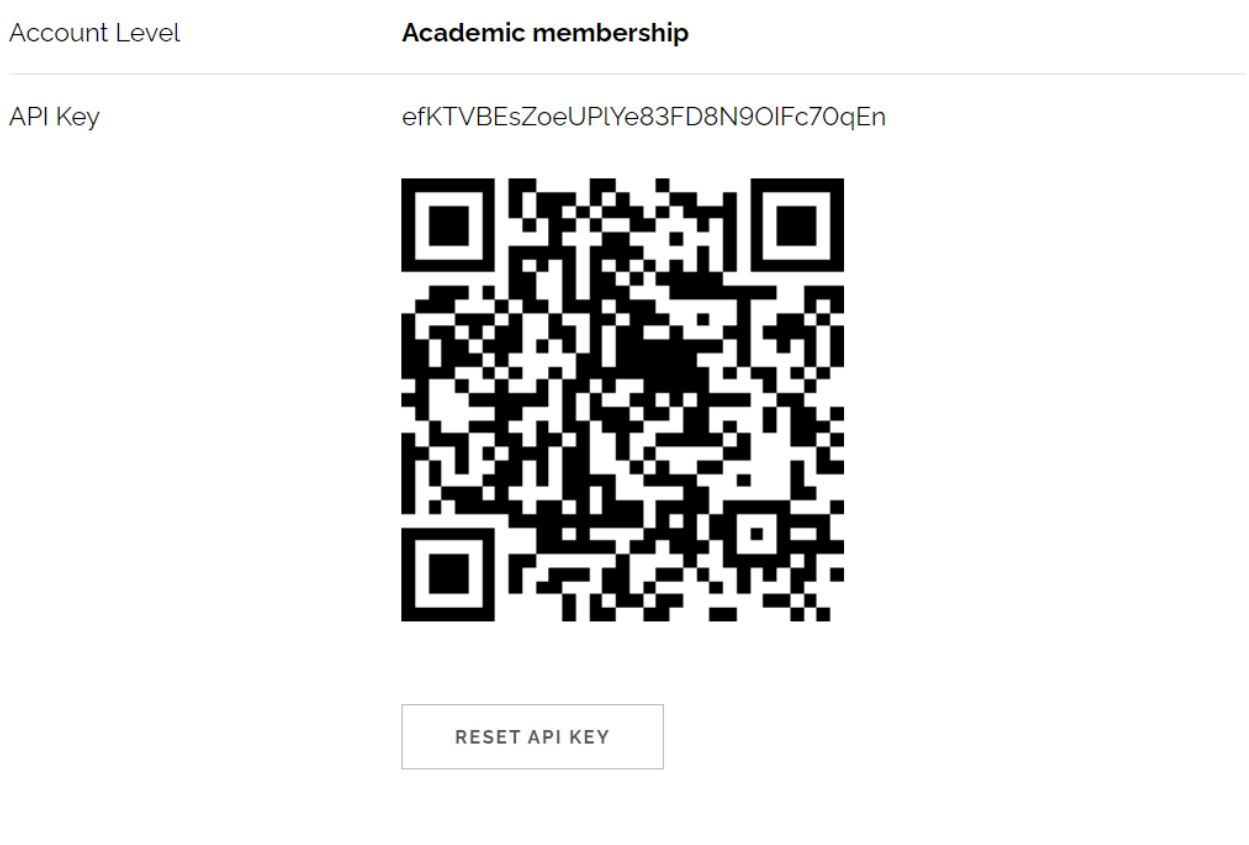


Es necesario escoger un licenciamiento adecuado que permite el uso de **"Filtros para la Búsqueda de Vulnerabilidades"**, solo presente en las licencias Small Business y Corporate ofrecidas por Shodan[5].

[5] https://account.shodan.io/billing

Como se puede notas en la figura anterior, el licenciamiento “Small Business” de Shodan es demasiado costoso. Sin embargo, la herramienta ofrece la posibilidad que otorgar este privilegio sin costos alguno, registrándose a la plataforma con una cuenta de tipo educativa, en mi caso personal contaba ya con una licencia de este tipo generada en el año 2010 con su respectiva API. Ver **Figura 11.**

Figura 11 – Registro Académico de Shodan



Obtención Automatizada De Datos.

Una vez obtenida la API adecuada esta se registra a través de Kali Linux[6] que es una herramienta usada por los profesionales de Ciberseguridad y también por los Ciberdelincuentes, esto con el fin de crear los programas necesarios (Scripts) que permitan sacar de manera automatizada la información requerida.

Lo primero es instalar Shodan en Kali Linux y luego registrar la API Key, para ellos se utiliza los siguientes comandos (Ver **Figura 12)**:

```
pip install shodan
shodan init
```

Figura 12 – Registro de API Shodan en Kali Linux

El siguiente paso es crear el script necesario para sacar la información de Shodan del Top 20 de las vulnerabilidades expuestas por País, por Producto, por Ciudad, por Puerto y Sistema Operativo de los diferentes países de Sur América. (Ver **Figura 13).**

Esta información es almacenada en un archivo plano de manera mensual, para el presente trabajo se trabajará con los datos obtenidos en 12 últimos meses; de marzo del 2022 al marzo del 2023, para la correcta ubicación del archivo este se nombra con el código del país y la fecha en que fue generado.

[6] https://www.kali.org/

Figura 13 – Muestra del Script para la obtención de datos

```
#!/bin/bash

_fecha=$(date +"%m%d%Y")
echo "Argentina......"
_destino1="/home/jca/shodan-stats/shodan_AR_"$_fecha".txt"
shodan stats has_vuln:true country:AR --limit 20 > $_destino1
shodan stats --facets region has_vuln:true country:AR --limit 20 >> $_destino1
shodan stats --facets city has_vuln:true country:AR --limit 20 >> $_destino1
shodan stats --facets product has_vuln:true country:AR --limit 20 >> $_destino1
shodan stats --facets port has_vuln:true country:AR --limit 20 >> $_destino1
shodan stats --facets os has_vuln:true country:AR --limit 20 >> $_destino1
```

La ejecución del script se hace los primeros días de cada mes, viendo su ejecución como se muestra a continuación: . (Ver **Figura 14).**

Figura 14 – Ejecución del Script “Stats.sh”

```
┌──(root㉿kali-jca)-[/home/jca/shodan-stats]
└─# sh stats.sh
Argentina......
Bolivia......
Brasil......
Chile......
Colombia......
Ecuador......
Guayana Francesa......
Guayana......
Isla Falkland......
Paraguay......
Peru......
Surinam......
Uruguay......
Venezuela......
Panama......
```

Los archivos generados por el Script, se mueven a una carpeta del mes en que se ejecutó, como se muestra en la **Figura 15** se aprecia los archivos generados el 1 de abril del año 2023.

Figura 15 – Archivos generados por el Script “Stats.sh”

```
┌──(root㉿kali-jca)-[/home/jca/shodan-stats/Abril23]
└─# dir
shodan_AR_04012023.txt  shodan_EC_04012023.txt  shodan_PE_04012023.txt
shodan_BO_04012023.txt  shodan_FK_04012023.txt  shodan_PY_04012023.txt
shodan_BR_04012023.txt  shodan_GF_04012023.txt  shodan_SR_04012023.txt
shodan_CL_04012023.txt  shodan_GY_04012023.txt  shodan_UY_04012023.txt
shodan_CO_04012023.txt  shodan_PA_04012023.txt  shodan_VE_04012023.txt
```

Cada uno de los archivos contiene la información requerida para el presente proyecto, tomemos por ejemplo uno de Colombia, generado el 1 de abril del 2023: (Ver **Figura 16).**

Figura 16 – Extracto de información obtenida por Colombia abril 2023

```
Top 1 Results for Facet: country
CO                            41,661

Top 20 Results for Facet: city
Bogotá                        22,611
Colombia                       3,473
Medellín                       3,266
Barrio San Luis                1,846
Cali                           1,456
Barranquilla                   1,259
Bucaramanga                      677
Tocancipá                        508
Pereira                          482
Ibagué                           441
Cúcuta                           368
Pasto                            317
Cartagena                        305
Villavicencio                    283
Popayán                          261
Manizales                        243
Santa Marta                      215
Montelíbano                      179
Armenia                          178
Montería                         162

Top 20 Results for Facet: product
Apache httpd                  16,119
```

Tabulación De Información Obtenida

Es necesario tabular la información obtenida con el fin de interpretar adecuadamente los datos registrados, para ello utilizaremos PowerBI[7] herramienta de la empresa Microsoft que permite el análisis de datos para proporcionar visualizaciones interactivas lo que permitirá la interpretación de la información obtenida.

Para poder hacer la migración de los archivos planos obtenidos a PowerBi, es necesario formatéalos en Excel utilizando la funcionalidad de diseño de tablas, esto se realizará por cada país de sur América con la información obtenida de cada una de ellas.

Una de las tablas más importantes se llama “General_Vulnera” que contiene el total de vulnerabilidades mes a mes (de marzo 2022 a marzo 2023) por cada uno de los países sur americanos: (Ver **Figura 17).**

Figura 17 – Imagen de la tabla “General_Vulnera”

Pais	año	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Argentina	2022			125.387	133.179	127.116	119.682	135.872	157.279	117.127	152.985	175.174	121.486
Bolivia	2022			29.142	28.247	26.475	26.578	29.218	36.310	19.780	30.576	37.436	28.175
Brasil	2022			534.422	567.966	532.852	493.276	524.047	644.476	387.876	554.394	690.934	468.122
Chile	2022			40.238	41.888	39.464	38.131	41.657	48.823	35.159	46.641	54.166	43.062
Colombia	2022			36.841	38.066	36.214	34.898	38.521	44.580	29.600	38.316	43.651	36.052
Ecuador	2022			14.052	14.818	14.485	13.767	14.186	16.014	11.101	13.970	13.920	12.576
Paraguay	2022			7.311	7.620	7.131	6.784	7.258	8.199	5.358	7.296	8.849	6.036
Peru	2022			14.654	15.208	15.748	16.318	18.236	20.054	14.916	19.353	22.188	18.918
Uruguay	2022			10.030	11.180	10.182	9.370	10.336	14.928	7.689	12.142	16.819	10.254
Venezuela	2022			8.840	9.350	8.689	8.544	9.080	11.140	6.797	4.793	13.797	10.897
Panama	2022			5.538	5.667	5.117	5.291	5.962	6.813	5.122	7.211	9.685	9.136
Argentina	2023	134.177	142.926	115.815									
Bolivia	2023	23.965	25.465	25.586									
Brasil	2023	478.162	509.673	444.448									
Chile	2023	41.717	41.997	40.257									
Colombia	2023	36.789	38.344	36.705									
Ecuador	2023	12.761	13.329	12.388									
Paraguay	2023	6.367	6.840	5.632									
Peru	2023	18.968	18.918	18.479									
Uruguay	2023	9.264	10.305	9.579									
Venezuela	2023	10.141	9.820	8.540									
Panama	2023	7.720	7.918	9.040									

Tomemos como ejemplo el país de Argentina, las imágenes que siguen a continuación corresponden a las tablas: “Ciudad_AR” (Ver **Figura 18)** que se trata de las vulnerabilidades expuestas mes a mes de las ciudades principales de Argentina.

[7] https://powerbi.microsoft.com/es-es/

Figura 18 – Imagen extracto de tabla “Ciudad_AR”

Ciudades	Año	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto
Buenos Aires	2022			30,755	35.682	37.907	35.639	38.200	42.348
Buenos Aires	2023	50.900	53.427	43.949					
Rosario	2022			12,364	13.131	12.534	12.189	19.970	22.996
Rosario	2023	21.399	18.924	24.575					
Mar del Plata	2022			3,625	4.217	4.382	4.085	3.019	3.453
Mar del Plata	2023	2.783	3.095	1.453					
Santa Catalina - Dique Lujan	2022			3,54	2.994	2.201	2.519	2.134	2.900
Santa Catalina - Dique Lujan	2023	1.834	1.016	1.531					
Córdoba	2022			2,666	2.925	3.035	3.013	2.452	2.888
Córdoba	2023	2.069	2.218	2.211					
Monte Caseros	2022			2,338	2.177	2.016	2.287	2.023	2.232
Monte Caseros	2023	1.549	1.761	811					
San Miguel de Tucumán	2022			2,287	2.433	2.673	2.172	2.012	1.880
San Miguel de Tucumán	2023	784		801					
Mendoza	2022			2,275	2.733	2.796	2.549	2.628	3.123
Mendoza	2023	1.796	1.860	1.469					
San Justo	2022			2,163	1.801	1.053	1.139	965	1.600
San Justo	2023	720							
Santa Fe	2022			2,114	1.845	1.540	884	1.044	1.064
Santa Fe	2023	810	782	1.118					
La Plata	2022			2,094	2.179	2.167	2.178	2.236	2.535
La Plata	2023		2.294	1.822					
Pinamar	2022			1,829	1.282		853		1.355
Canals	2022			1,738	2.071	1.933	1.504	1.778	2.389
Canals	2023	1.174	1.800						
San Luis	2022			1,656	1.770	1.682	1.755	1.470	1.412
San Luis	2023	1.317	1.335	1.276					
Médanos	2022			1,448	1.620	1.268	1.230		1.892

“Productos_AR” (Ver **Figura 19)** se trata de las vulnerabilidades expuestas mes a mes clasificadas por productos expuestas en Argentina.

Figura 19 – Imagen extracto de tabla “Productos_AR”

Productos	Año	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto
lighttpd	2022			48.297	51.473	48.145	44.904	43.544	51.500
lighttpd	2023	32.575	41.081	12.863					
Apache httpd	2022			38.963	40.509	38.402	36.840	39.265	44.054
Apache httpd	2023	38.015	38.488	37.764					
Microsoft IIS httpd	2022			8.178	8.409	8.195	7.928	12.946	14.124
Microsoft IIS httpd	2023	12.292	12.332	11.812					
OpenSSH	2022			5.749	6.163	6.011	5.639	5.240	6.267
OpenSSH	2023	5.384	5.453	5.081					
uc-httpd	2022			1.889	1.929	1.786	1.623	1.590	2.247
uc-httpd	2023	1.377	1.327	1.179					
GoAhead Embedded Web Server	2022			1.314	1.433	1.414	1.270	694	369
GoAhead Embedded Web Server	2023	1.126	1.118	1.005					
Remote Desktop Protocol	2022			1.030	1.293	1.224	1.003	935	1.222
Remote Desktop Protocol	2023	1.073	1.068	859					
Exim smtpd	2022			682	912	815	721	9.876	11.778
Exim smtpd	2023	13.697	13.719	13.429					
Squid http proxy	2022			525	563	701	561	561	834
Squid http proxy	2023	498	496	475					
PostgreSQL	2022			477	504	469	435	406	484
PostgreSQL	2023	519	509	468					
nginx	2022			384	401	376	356	395	532
nginx	2023	420	386	384					
ProFTPD	2022			354	382	366	319	1.191	1.254

“Puertos_AR” (Ver **Figura 20)** se trata de las vulnerabilidades expuestas mes a mes clasificadas por número de puerto expuestas en Argentina.

Figura 20 – Imagen extracto de tabla “Puerto_AR”

Puertos	Año	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto
80	2022			46,682	48.333	45.837	44.065	46.465	52.897
80	2023	40.864	44.741	31.969					
443	2022			29,586	31.490	30.256	29.268	32.199	36.810
443	2023	30.304	32.636	24.668					
81	2022			5,045	5.438	4.554	3.648	3.539	4.327
81	2023	2.063	2.249	1.791					
22	2022			4,723	5.027	4.878	4.590	4.193	4.972
22	2023	4.135	4.045	3.716					
2082	2022			4,489	4.923	4.893	4.460	4.312	4.797
2082	2023	5.295	5.218	5.107					
8888	2022			4,155	4.084	3.898	4.007	3.770	4.149
8888	2023	2.565	3.328	1.627					
2083	2022			4,072	4.367	4.394	4.006	4.069	4.492
2083	2023	5.014	4.982	4.928					
8080	2022			4,033	4.476	4.255	3.939	4.185	5.041
8080	2023	3.882	3.586	3.283					
2087	2022			2,216	2.396	2.383	2.246	2.353	2.357
2087	2023	2.747	2.796	2.837					
8181	2022			1,805	1.986	2.027	1.787	1.296	1.117
8181	2023	1.209	1.216	1.083					
8081	2022			1,407	1.499	1.432	1.228	1.407	1.717

“Operativos_AR” ” (Ver **Figura 21)** se trata de las vulnerabilidades expuestas mes a mes clasificadas por sistemas operativos expuestas en Argentina.

Figura 21 – Imagen extracto de tabla “Operativos_AR”

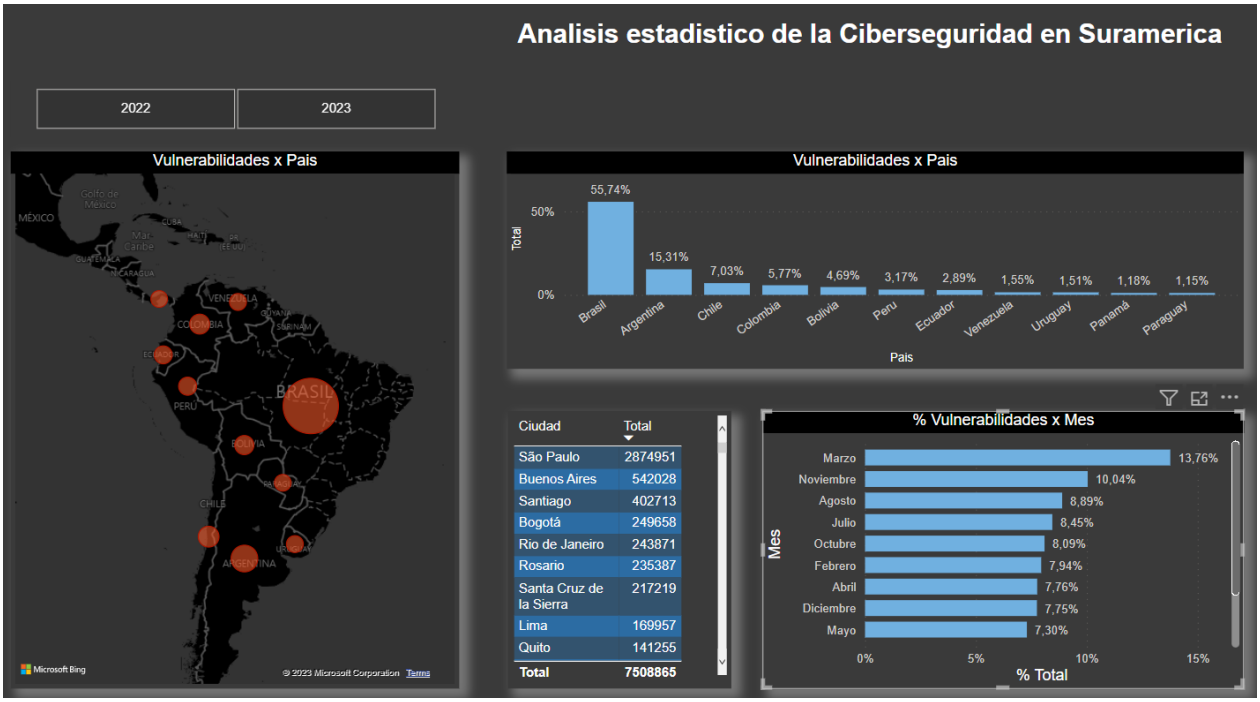
Sistemas Operativos	Año	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto
Debian	2022			41	42	43	44	48	
Debian	2023	42	40	33					
Windows Server 2003	2022			25	27	25	22	18	
Windows Server 2004	2023	17	16	17					
Windows 10 Pro 19043	2022			22	15	20	14	11	
Windows 10 Pro 19042	2022			19	14	8	6	6	
Windows Server 2008 R2 Standard	2022			12	13	132	133	128	
Windows Server 2008 R2 Standard	2023	174	163	128					
Windows 10 Pro 19044	2022			9	22	26	31	26	
Windows 10 Pro 19045	2023	30	26	22					
Windows 7 Professional	2022			8	6	53	53	44	
Windows 7 Professional	2023	54	65	37					
Windows Server 2008 R2 Enterprise	2022			7	8	48	68	67	
Windows Server 2008 R2 Enterprise	2023	111	102	88					
Windows 10 Pro 19041	2022			4	3				
Windows 7 Professional 7600	2022			4	-			3	
Windows 7 Ultimate 7601 Service Pack 1	2022			4	6	8	5	3	
Windows 10 Home Single Language 19043	2022			3	4	4	4	4	
Windows 8.1 Single Language 9600	2022			3	4				
Windows 10 Enterprise 19042	2022			2	-		2	5	
Windows 10 Enterprise 19044	2022			2	6	4	4	7	

Las imágenes anteriores muestran los extraído por el país de Argentina, esta misma información se hizo también por Bolivia, Brasil, Chile, Colombia, Ecuador, Panamá, Perú, Paraguay, Uruguay y Venezuela; lo que nos permitirá analizar la información y extraer las conclusiones del presente proyecto.

ANALISIS DE RESULTADOS OBTENIDOS

Resultados Generales

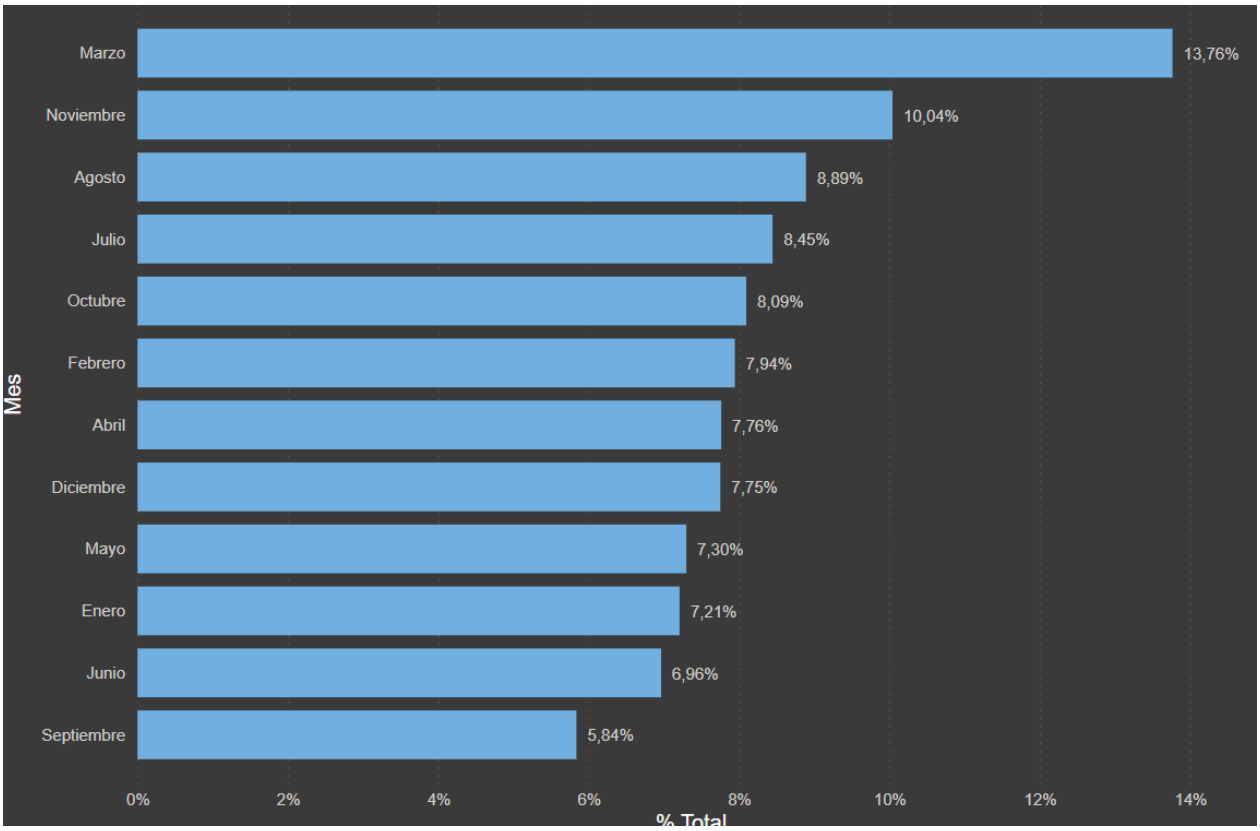
Figura 22 – Análisis estadísticos de la Ciberseguridad en Suramérica marzo 2022 a marzo 2023



Como se puede apreciar en la figura anterior (Ver **Figura 22)**, Brasil es el país que más vulnerabilidades expone de manera abierta a través de Internet en el último año, seguido de Argentina, Chile, Colombia, Bolivia, Perú, Ecuador, Venezuela, Uruguay, Panamá y Paraguay. La mayor parte de los riesgos se registran en las ciudades capitales.

Aunque no uniforme, se registra un aumento de las vulnerabilidades mes a mes (Ver **Figura 23)**, lo que evidencia que las empresas en Sur América pasan por alto o desconocen esta información que conlleva a no tener controles para aplicar medidas de control que cierren las brechas a las nuevas amenazas cibernéticas públicamente expuestas.

Figura 23 – Vulnerabilidades Expuestas mes a mes marzo 2022 a marzo 2023



Esta misma información se puede apreciar en lo que se registró en el año 2022 entre marzo y diciembre (Ver **Figura 24)** y lo registrado en el año 2023 entre enero y marzo (Ver **Figura 25).**

Figura 24 – Vulnerabilidades Expuestas entre marzo y diciembre de 2022

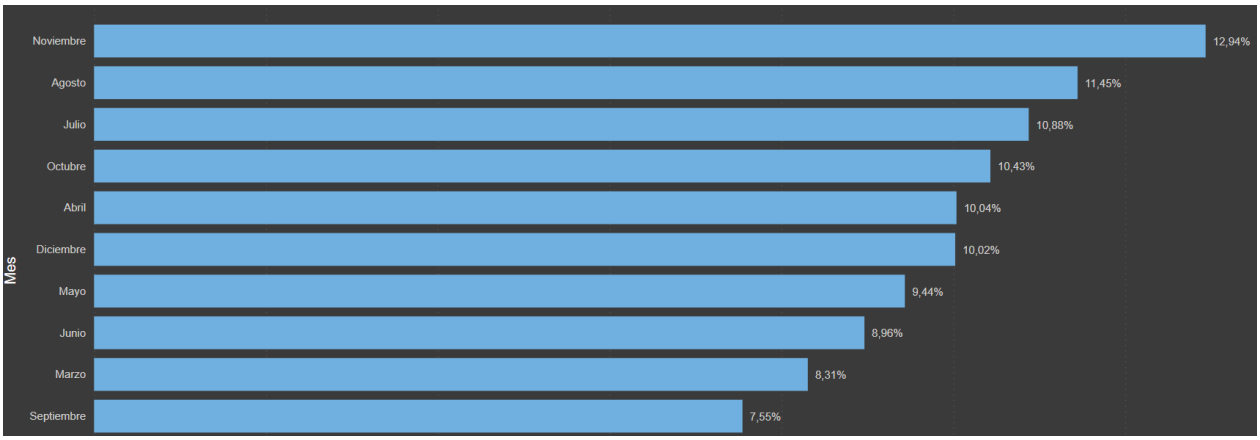
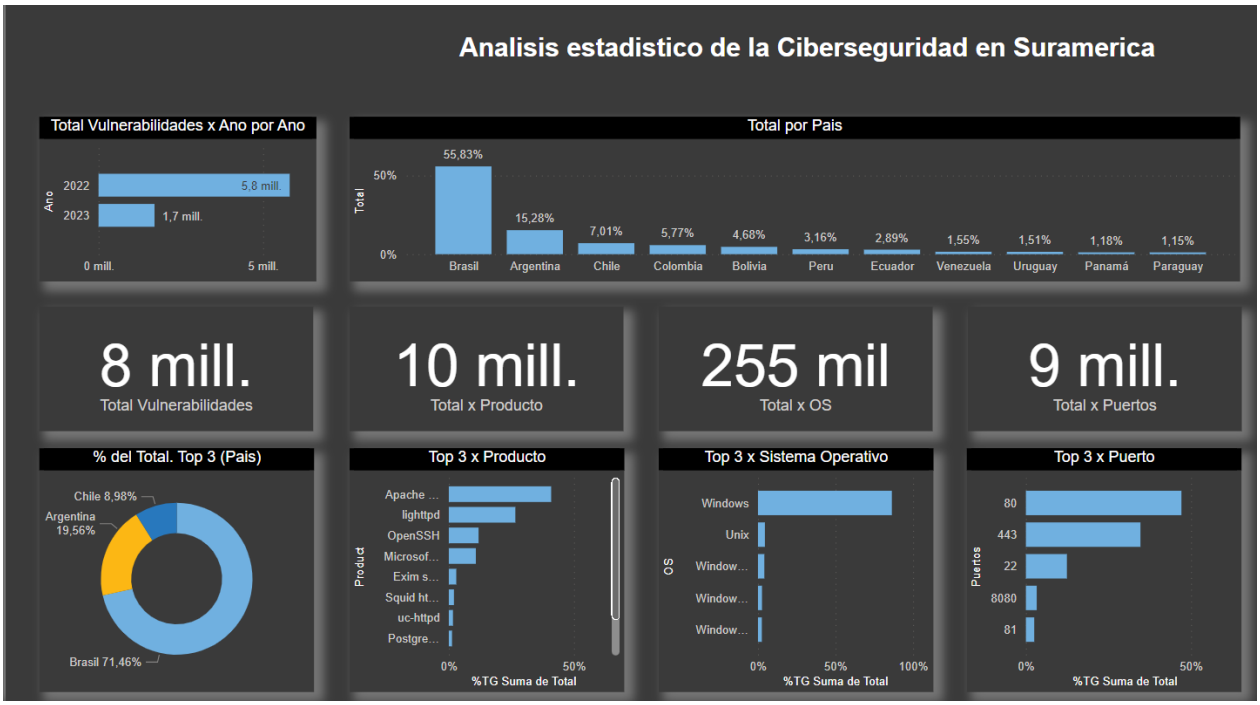


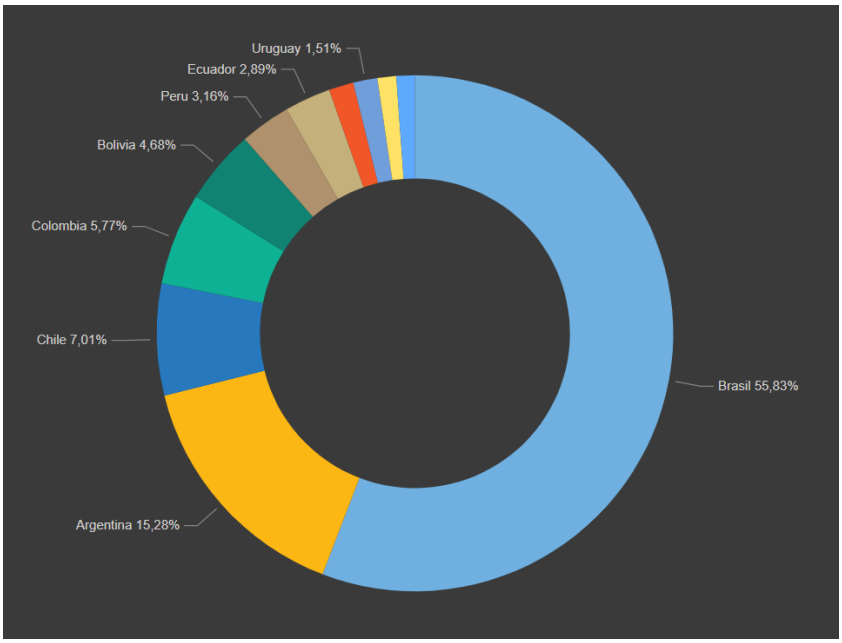
Figura 25 – Vulnerabilidades Expuestas entre enero y marzo de 2023

Figura 26 – Análisis estadísticos de la Ciberseguridad - Detallado



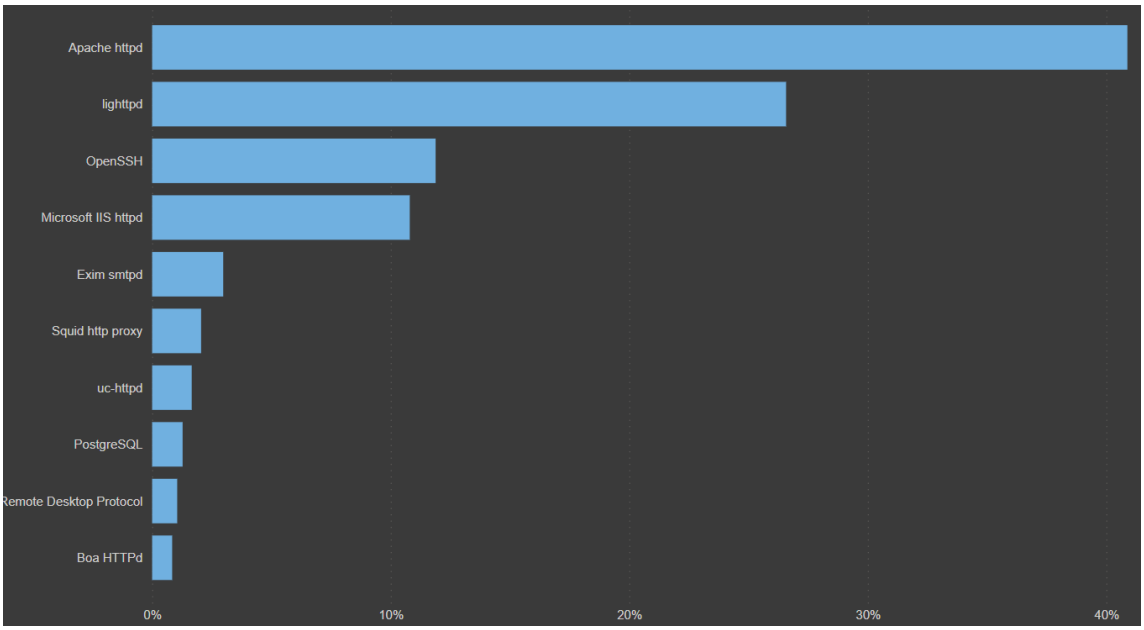
Como se puede apreciar en la figura anterior (Ver **Figura 26)**, se registraron en promedio 8 millones de vulnerabilidades clasificadas por país entre marzo de 2022 y marzo 2023, lo cual se detalla en la **Figura 27.**

Figura 27 – Vulnerabilidades por país – marzo 2022 a marzo 2023



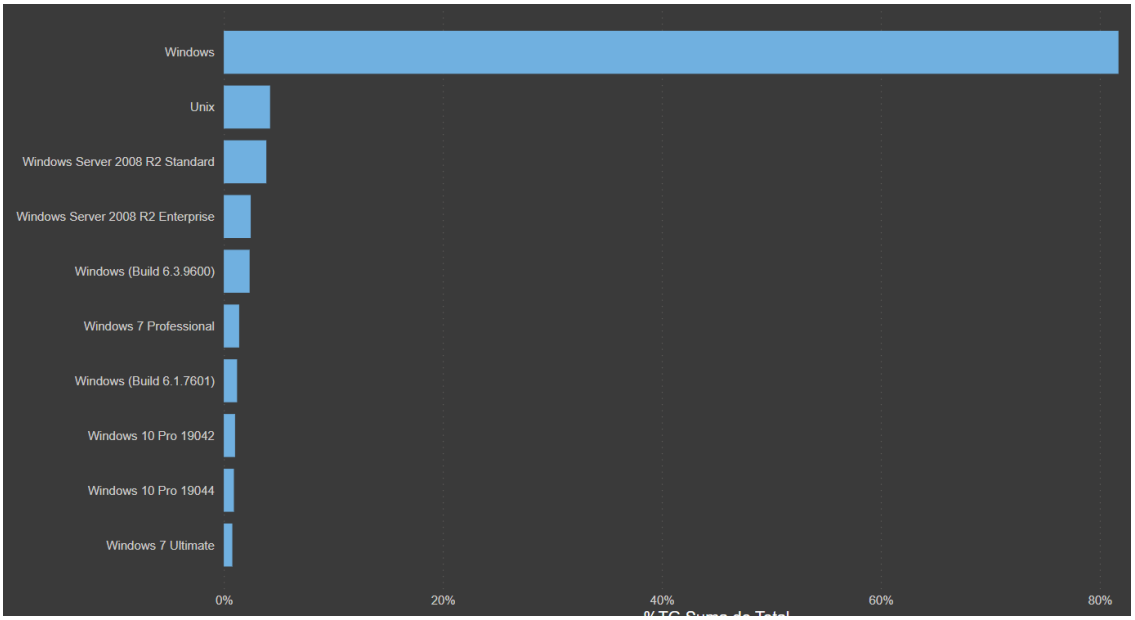
Se puede apreciar que se registraron un promedio de 10 millones de vulnerabilidades clasificadas por producto (ver **Figura 28)**, siendo el producto más vulnerable: “Apache http”, seguido de “Llighttpd”, “Openssh” y “Microsoft ISS Http”. Lo que implica que el mayor vector vulnerable en las empresas de Sur América, son sus portales Web.

Figura 28 – Vulnerabilidades por producto – marzo 2022 a marzo 2023



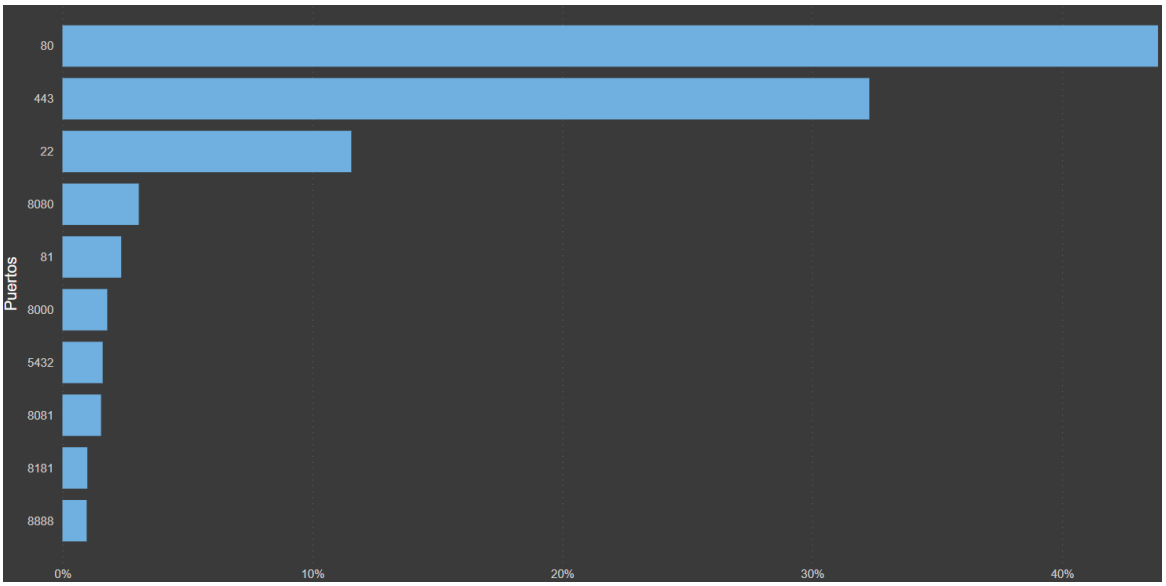
Se aprecia el registro promedio de 255 millones de vulnerabilidades clasificadas por Sistema Operativo (Ver **Figura 29)**, Windows sin duda se expone como el sistema más riesgoso a través de las fuentes abiertas, debido a la falta o lenta interacción de las empresas en cerrar las brechas que día a día se exponen sobre este sistema.

Figura 29 – Vulnerabilidades por sistema operativo – marzo 2022 a marzo 2023



Se aprecia un promedio de 9 millones de vulnerabilidades clasificadas por puerto (ver **Figura 30)**, siendo los puertos más vulnerables los 80 y 443 que corresponde a portales Web y puerto 22 que corresponde accesos remotos sobre los equipos expuestos. Los activos de información aquí expuesto no aseguran sus sistemas adecuadamente.

Figura 30 – Vulnerabilidades por sistema puerto – marzo 2022 a marzo 2023

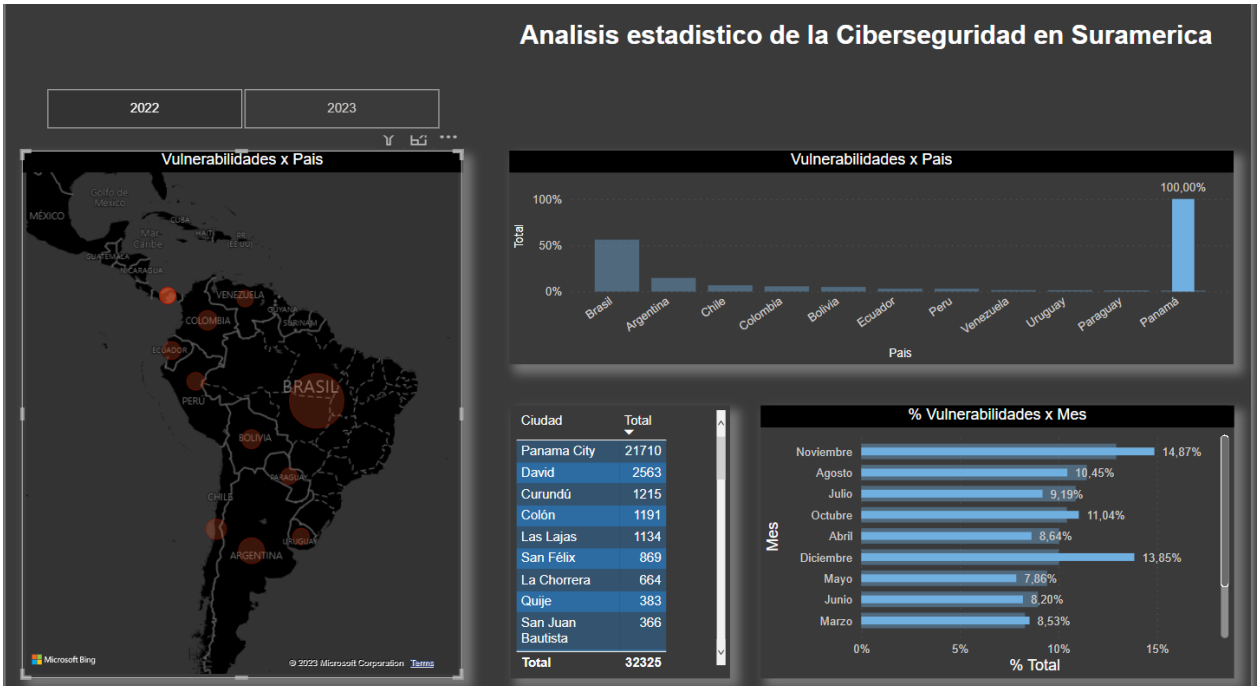


Resultados por país.

Con el fin de que el presente trabajo sirva para desvelar la problemática que las fuentes abiertas representan, se mostrara los resultados discriminados por país desde marzo del 2022 a marzo de 2023, de igual forma a través del siguiente enlace: https://github.com/jca6185/VulOsint-Latam.git se publicara la herramienta usada para la visualización de los resultados aquí mostrados para poder ser consultados por el investigador.

Panamá

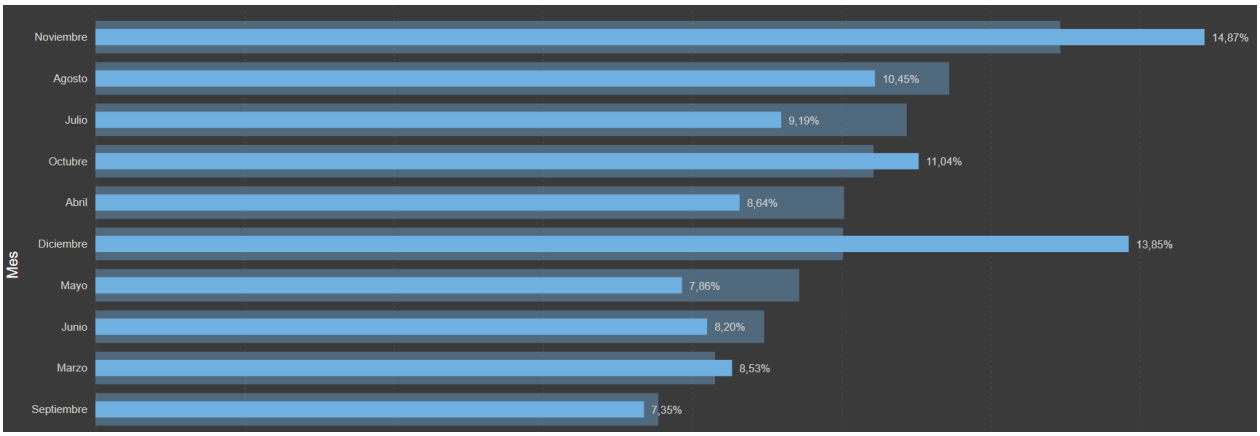
Figura 31 – Análisis estadísticos de la Ciberseguridad en Panamá marzo 2022 a marzo 2023



Como se puede destacar en la figura anterior (ver **Figura 31)** las vulnerabilidades mostradas por mes en Panamá son muy variables de un mes a otro, siendo noviembre y diciembre los meses con más vulnerabilidades mostradas, aunque de un mes a otro se nota la diminución de vulnerabilidades debido a la corrección de algunas de ellas, se nota también el crecimiento de un mes a otro que se debe a la aparición de nuevas vulnerabilidades.

Se destaca que no es mucho el impacto que se realiza en Panamá a la hora de corregir vulnerabilidades (ver **Figura 32)**, ello se debe al desconocimiento de muchas de las vulnerabilidades expuestas a través de fuentes abiertas.

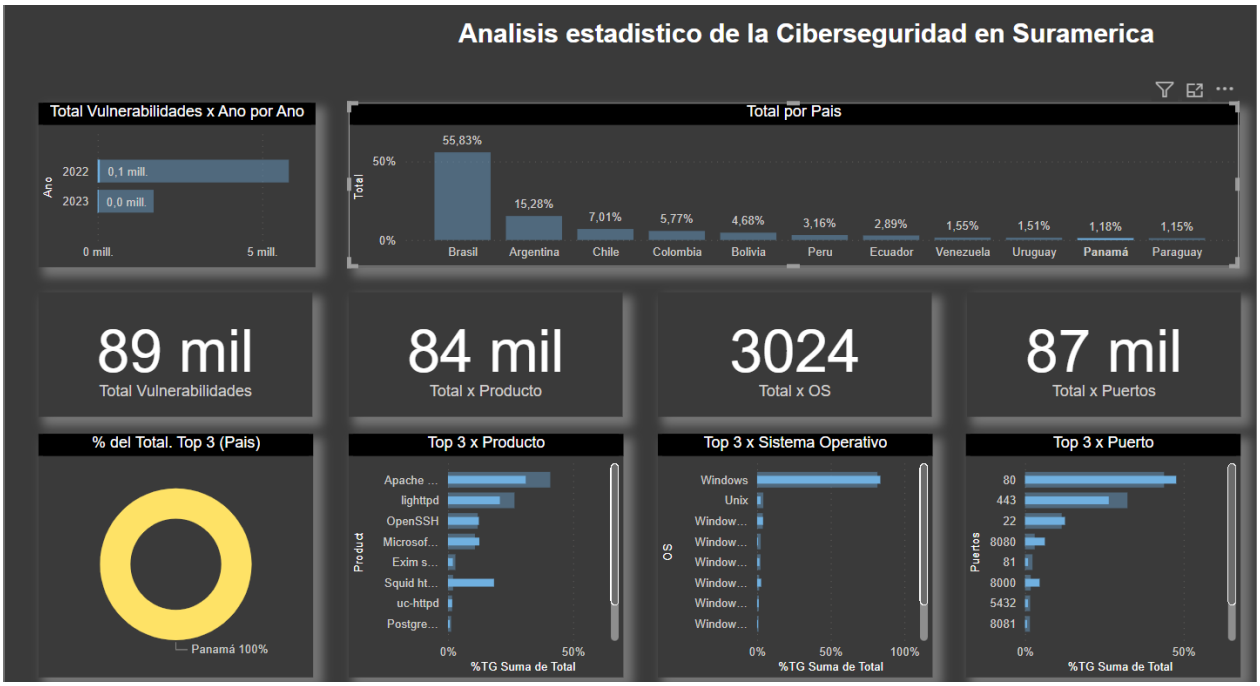
Figura 32 – Vulnerabilidades Mes a Mes – Panamá de marzo 2022 a marzo 2023



Las 5 ciudades que más vulnerabilidades reporto en el periodo de tiempo analizado, fueron en orden de importancia: Ciudad de Panamá, David, Curundú, Colón y Las Lajas. Esto destaca que son las ciudades con más activos de información expuesto en Internet.

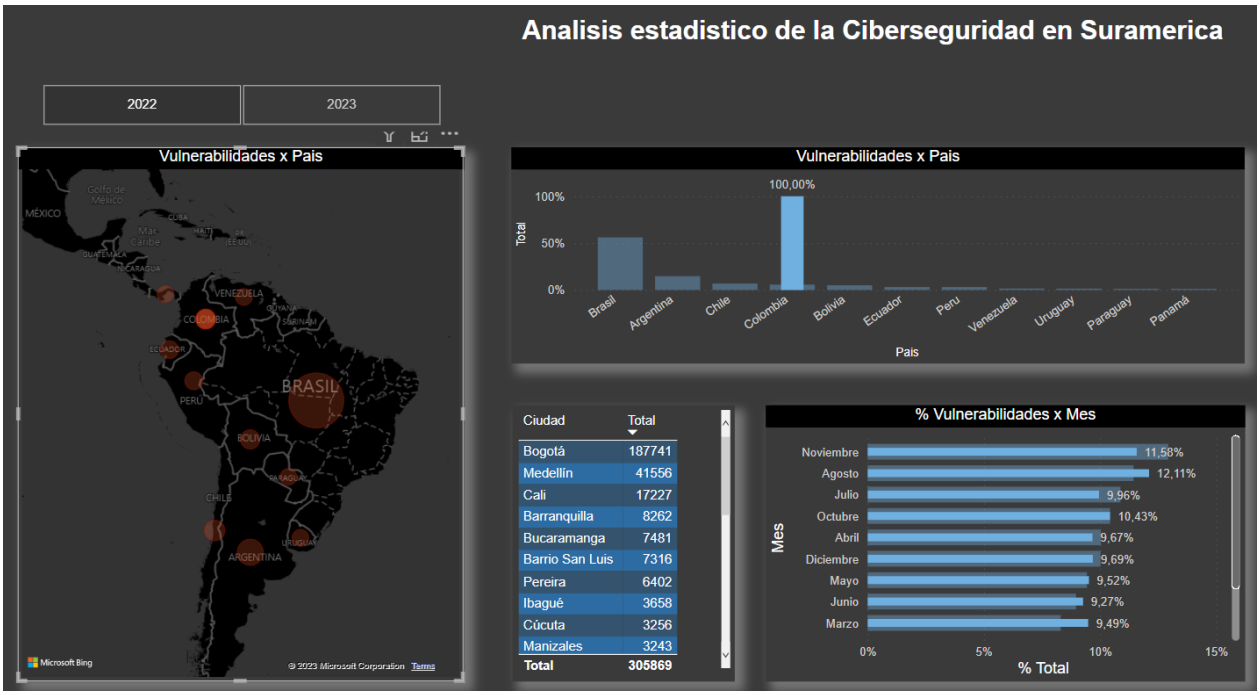
Como se puede apreciar en la siguiente grafica (ver **Figura 33)**, en Panamá se reportaron 89 mil vulnerabilidades entre Marzo del 2022 a Marzo del 2023, 84 Mil corresponde a los productos más vulnerables entre los que se destaca los servicios de Apache, Ligthttpd y Squid todos ellos servicios globalmente accesibles y que pueden ser vistos por ciberdelincuentes, 3.024 corresponde al Sistema Operativo donde se destaca Windows que en su mayor parte se atribuye a sistemas obsoletos como es el caso de Windows 7, 2000, 2003 etc, sistemas no parchados y/o sistemas no licenciados. Por último 87 mil corresponde a los puertos más vulnerables entre los que se destaca el puerto 80 y 443 que corresponde a portales web y puerto 22 que corresponde a accesos remotos.

Figura 33 – Análisis estadísticos de la Ciberseguridad – Detallado - Panamá



Colombia

Figura 34 – Análisis estadísticos de la Ciberseguridad en Colombia marzo 2022 a marzo 2023



Como se puede destacar en la figura anterior (ver **Figura 34)** las vulnerabilidades mostradas por mes en Colombia son muy variables de un mes a otro, siendo noviembre y agosto los meses con más vulnerabilidades mostradas, aunque de un mes a otro se nota la diminución de vulnerabilidades debido a la corrección de algunas de ellas, se nota también el crecimiento de un mes a otro que se debe a la aparición de nuevas vulnerabilidades.

Se destaca que no es mucho el impacto que se realiza en Colombia a la hora de corregir vulnerabilidades (ver **Figura 35)**, ello se debe al desconocimiento de muchas de las vulnerabilidades expuestas a través de fuentes abiertas.

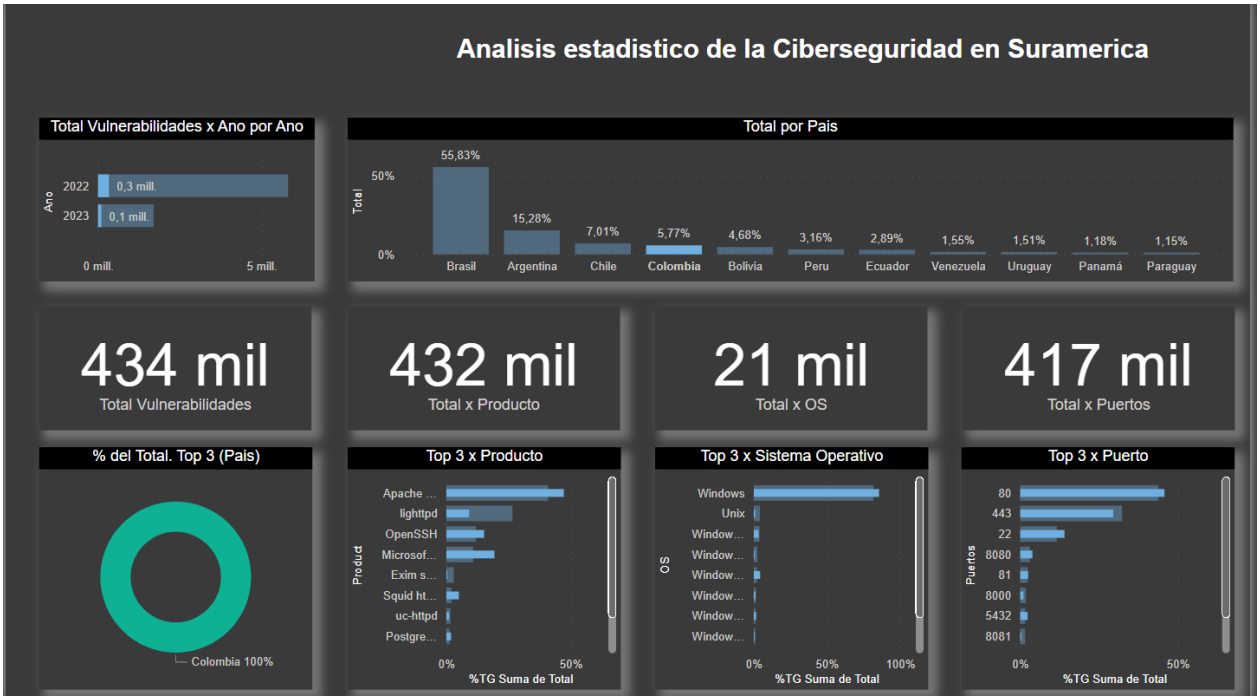
Figura 35 – Vulnerabilidades Mes a Mes – Colombia de marzo 2022 a marzo 2023

Las 5 ciudades que más vulnerabilidades reporto en el periodo de tiempo analizado, fueron en orden de importancia: Bogotá, Medellín, Cali, Barranquilla y Bucaramanga. Esto destaca que son las ciudades con más activos de información expuesto en Internet.

Como se puede apreciar en la siguiente grafica (ver **Figura 36)**, en Colombia se reportaron 434 mil vulnerabilidades entre Marzo del 2022 a Marzo del 2023, 432 mil corresponde a los productos más vulnerables entre los que se destaca los servicios de Apache, Microsoft y OpenSsh todos ellos servicios globalmente accesibles y que pueden ser vistos por ciberdelincuentes, 21 mil corresponde al Sistema Operativo donde se destaca Windows que en su mayor parte se atribuye a sistemas obsoletos como es el caso de Windows 7, 2000, 2003

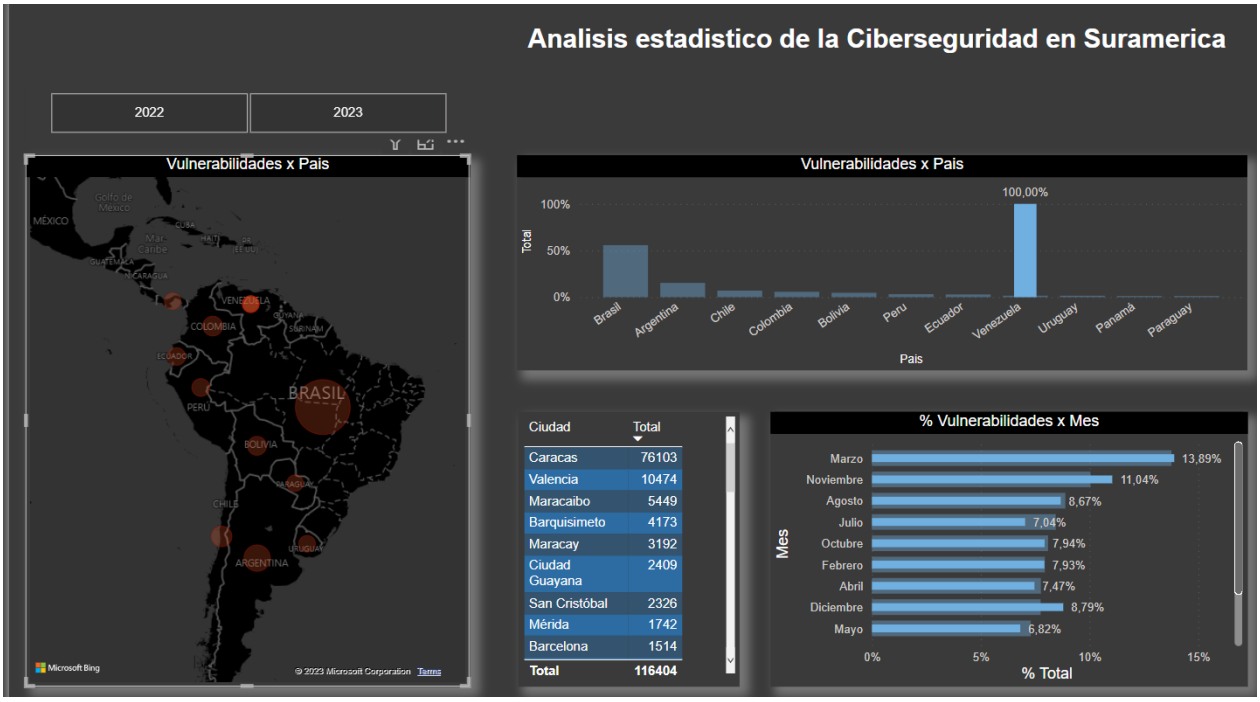
etc., sistemas no parchados y/o sistemas no licenciados. Por último 417 mil corresponde a los puertos más vulnerables entre los que se destaca el puerto 80 y 443 que corresponde a portales web y puerto 22 que corresponde a accesos remotos.

Figura 36 – Análisis estadísticos de la Ciberseguridad – Detallado – Colombia



Venezuela

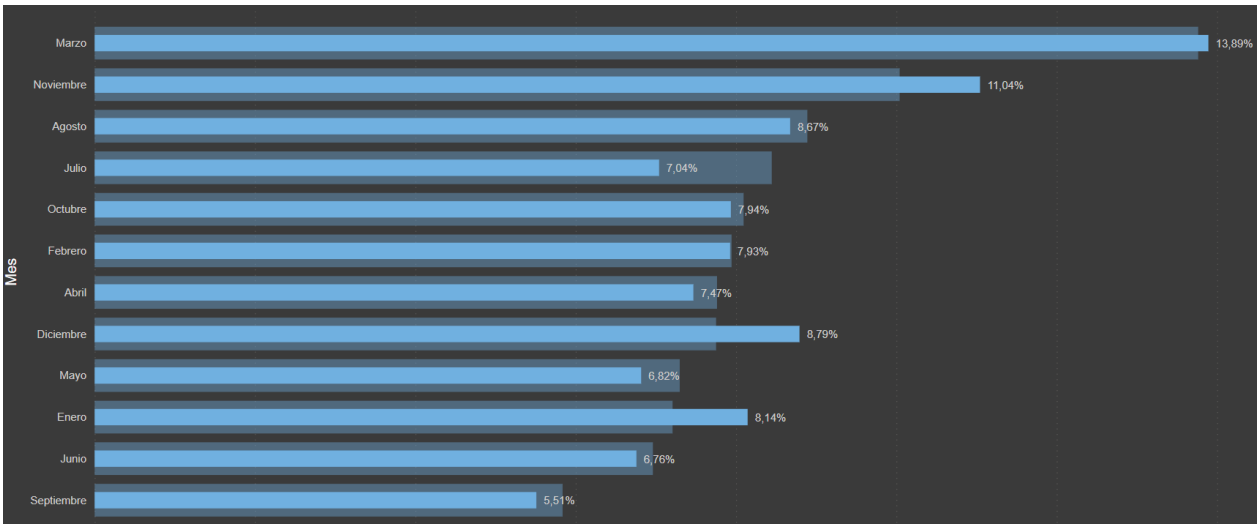
Figura 37 – Análisis estadísticos de la Ciberseguridad en Venezuela marzo 2022 a marzo 2023



Como se puede destacar en la figura anterior (ver **Figura 37)** las vulnerabilidades mostradas por mes en Venezuela son muy variables de un mes a otro, siendo marzo y noviembre los meses con más vulnerabilidades mostradas, aunque de un mes a otro se nota la diminución de vulnerabilidades debido a la corrección de algunas de ellas, se nota también el crecimiento de un mes a otro que se debe a la aparición de nuevas vulnerabilidades.

Se destaca que no es mucho el impacto que se realiza en Venezuela a la hora de corregir vulnerabilidades (ver **Figura 38)**, ello se debe al desconocimiento de muchas de las vulnerabilidades expuestas a través de fuentes abiertas.

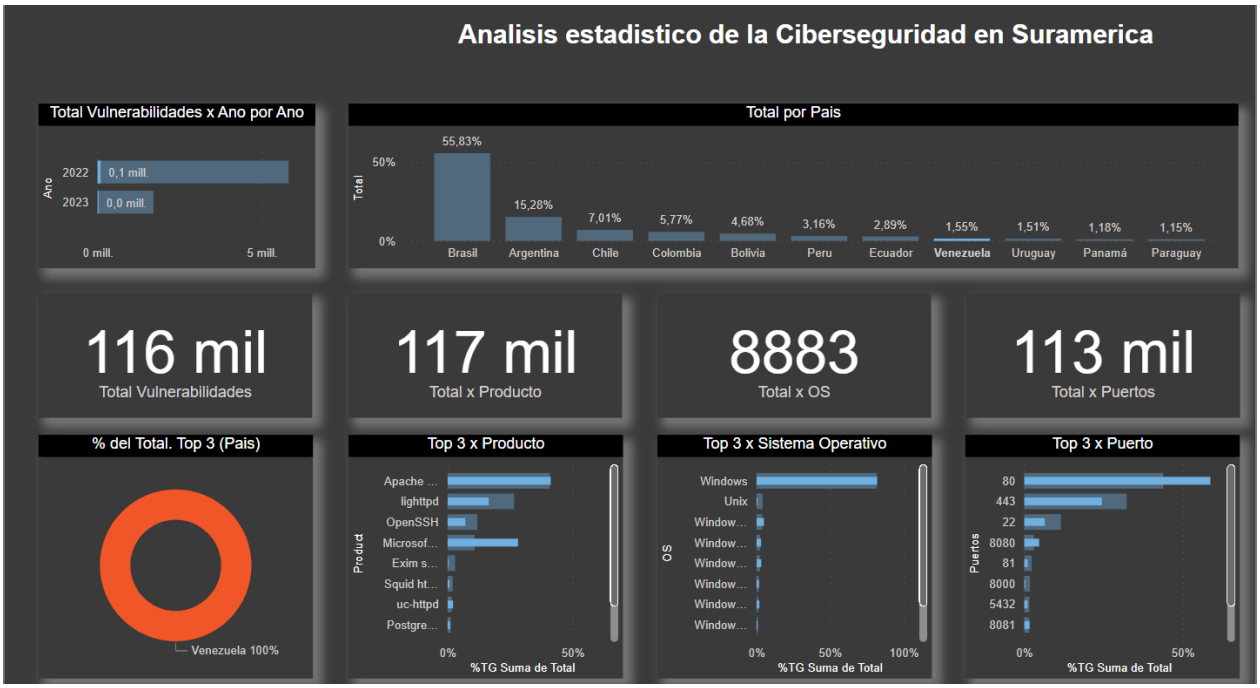
Figura 38 – Vulnerabilidades Mes a Mes – Venezuela de marzo 2022 a marzo 2023



Las 5 ciudades que más vulnerabilidades reporto en el periodo de tiempo analizado, fueron en orden de importancia: Caracas, Valencia, Maracaibo, Barquisimeto y Maracay. Esto destaca que son las ciudades con más activos de información expuesto en Internet.

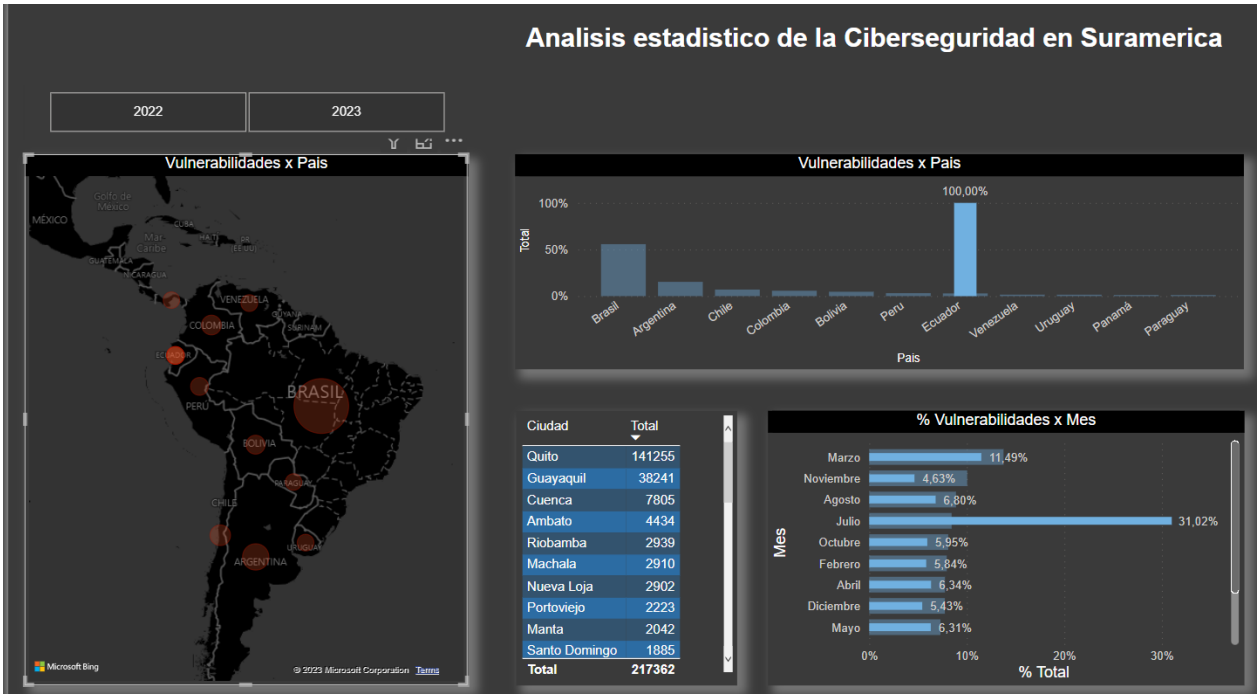
Como se puede apreciar en la siguiente grafica (ver **Figura 39)**, en Venezuela se reportaron 116 mil vulnerabilidades entre Marzo del 2022 a Marzo del 2023, 117 mil corresponde a los productos más vulnerables entre los que se destaca los servicios de Apache, Ligthttpd y Microsoft todos ellos servicios globalmente accesibles y que pueden ser vistos por ciberdelincuentes, 8.833 corresponde al Sistema Operativo donde se destaca Windows que en su mayor parte se atribuye a sistemas obsoletos como es el caso de Windows 7, 2000, 2003 etc., sistemas no parchados y/o sistemas no licenciados. Por último 113 mil corresponde a los puertos más vulnerables entre los que se destaca el puerto 80 y 443 que corresponde a portales web y puerto 22 que corresponde a accesos remotos.

Figura 39 – Análisis estadísticos de la Ciberseguridad – Detallado – Venezuela



Ecuador

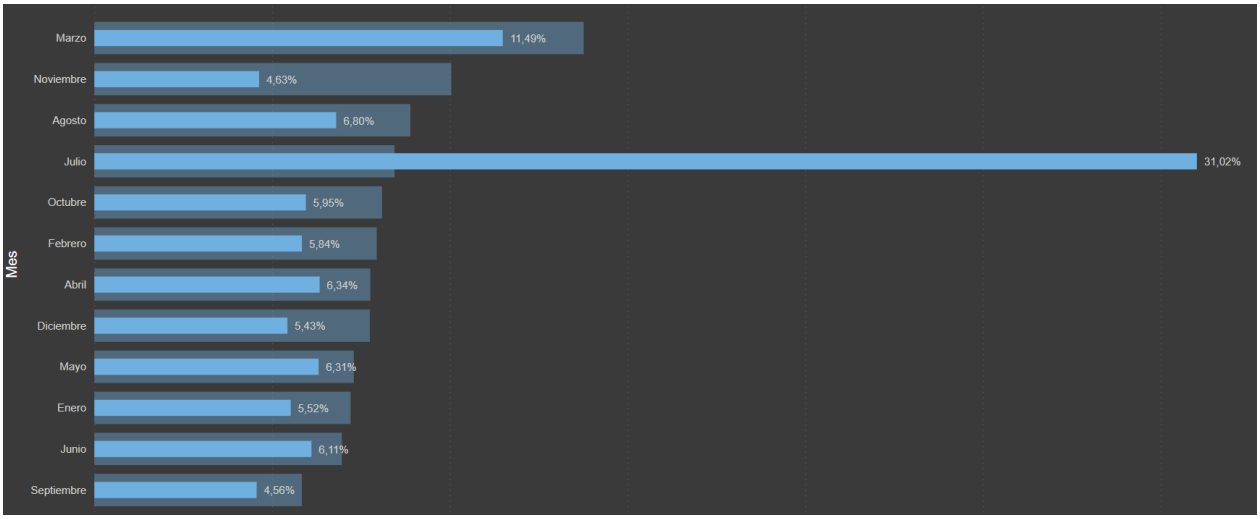
Figura 40 – Análisis estadísticos de la Ciberseguridad en Ecuador marzo 2022 a marzo 2023



Como se puede destacar en la figura anterior (ver **Figura 40)** las vulnerabilidades mostradas por mes en Ecuador son muy variables de un mes a otro, siendo julio el mes con más vulnerabilidades mostradas, aunque de un mes a otro se nota la diminución de vulnerabilidades debido a la corrección de algunas de ellas, se nota también el crecimiento de un mes a otro que se debe a la aparición de nuevas vulnerabilidades.

Se destaca que no es mucho el impacto que se realiza en Ecuador a la hora de corregir vulnerabilidades (ver **Figura 41)**, ello se debe al desconocimiento de muchas de las vulnerabilidades expuestas a través de fuentes abiertas.

Figura 41 – Vulnerabilidades Mes a Mes – Ecuador de marzo 2022 a marzo 2023

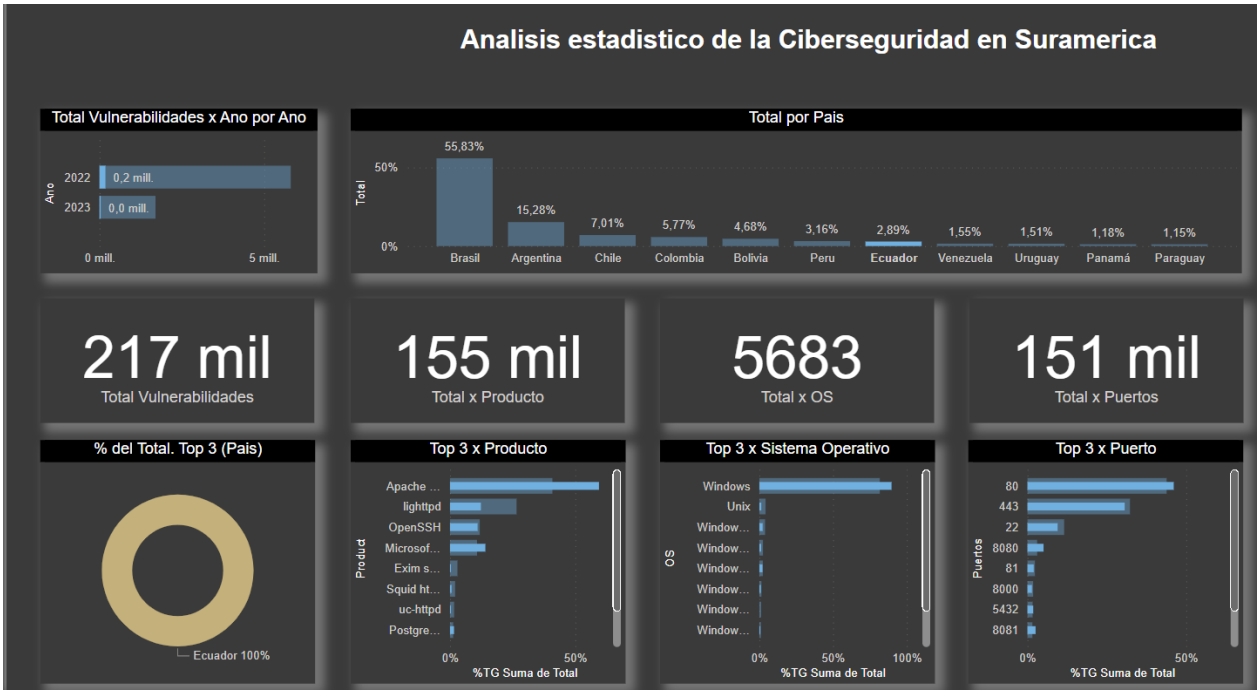


Las 5 ciudades que más vulnerabilidades reporto en el periodo de tiempo analizado, fueron en orden de importancia: Quito, Guayaquil, Cuenca, Ambato y Riobamba. Esto destaca que son las ciudades con más activos de información expuesto en Internet.

Como se puede apreciar en la siguiente grafica (ver **Figura 42)**, en Ecuador se reportaron 217 mil vulnerabilidades entre Marzo del 2022 a Marzo del 2023, 155 mil corresponde a los productos más vulnerables entre los que se destaca los servicios de Apache, Ligthttpd y Microsoft todos ellos servicios globalmente accesibles y que pueden ser vistos por ciberdelincuentes, 5.683 corresponde al Sistema Operativo donde se destaca Windows que en

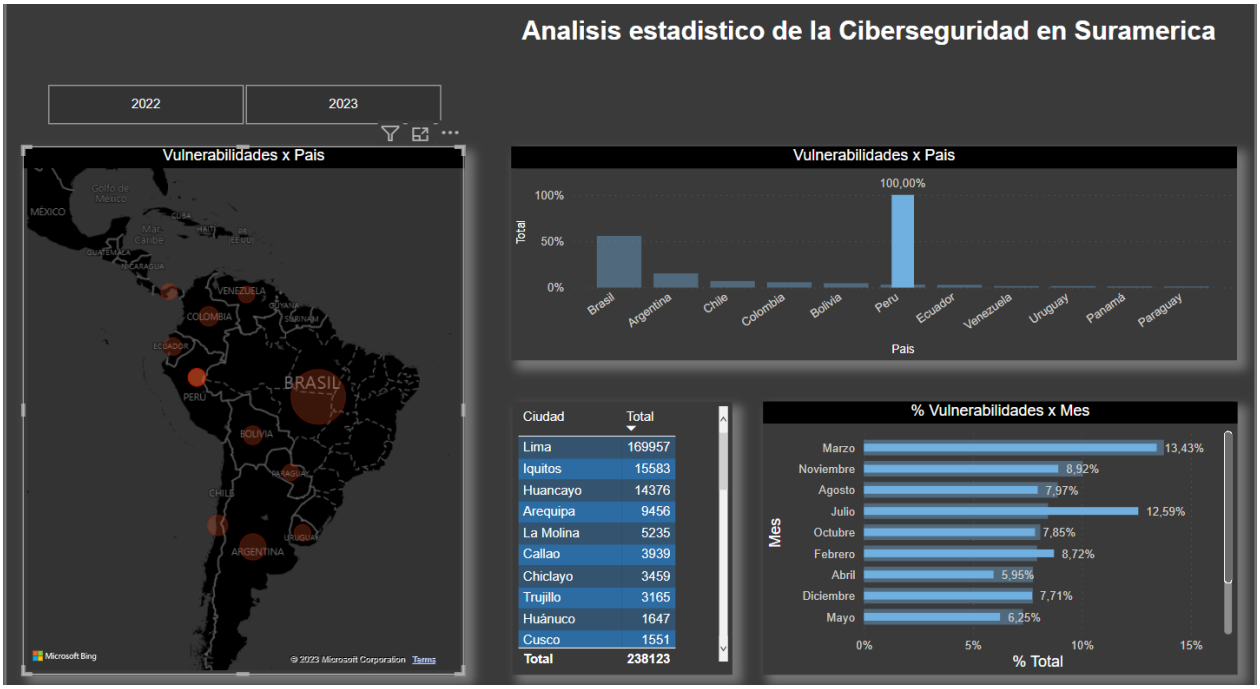
su mayor parte se atribuye a sistemas obsoletos como es el caso de Windows 7, 2000, 2003 etc., sistemas no parchados y/o sistemas no licenciados. Por último 151 mil corresponde a los puertos más vulnerables entre los que se destaca el puerto 80 y 443 que corresponde a portales web y puerto 22 que corresponde a accesos remotos.

Figura 42 – Análisis estadísticos de la Ciberseguridad – Detallado – Ecuador



Perú

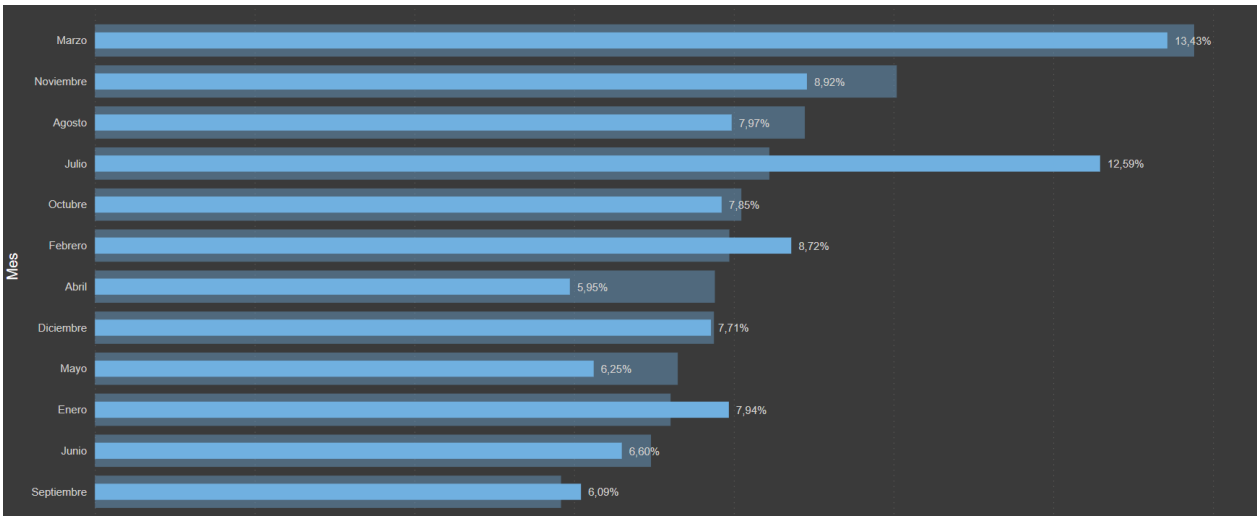
Figura 43 – Análisis estadísticos de la Ciberseguridad en Perú marzo 2022 a marzo 2023



Como se puede destacar en la figura anterior (ver **Figura 43)** las vulnerabilidades mostradas por mes en Perú son muy variables de un mes a otro, siendo marzo y julio los meses con más vulnerabilidades mostradas, aunque de un mes a otro se nota la diminución de vulnerabilidades debido a la corrección de algunas de ellas, se nota también el crecimiento de un mes a otro que se debe a la aparición de nuevas vulnerabilidades.

Se destaca que no es mucho el impacto que se realiza en Perú a la hora de corregir vulnerabilidades (ver **Figura 44)**, ello se debe al desconocimiento de muchas de las vulnerabilidades expuestas a través de fuentes abiertas.

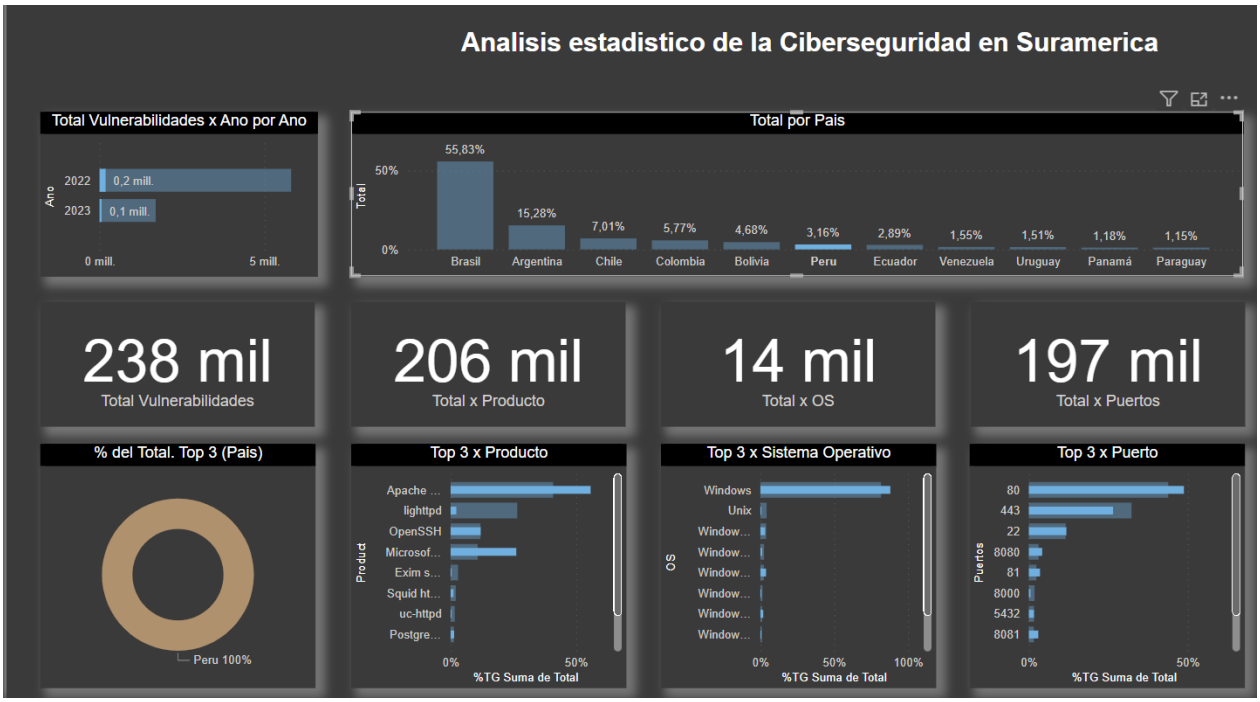
Figura 44 – Vulnerabilidades Mes a Mes – Perú de marzo 2022 a marzo 2023



Las 5 ciudades que más vulnerabilidades reporto en el periodo de tiempo analizado, fueron en orden de importancia: Lima, Iquitos, Huancayo, Arequipa y la Molina. Esto destaca que son las ciudades con más activos de información expuesto en Internet.

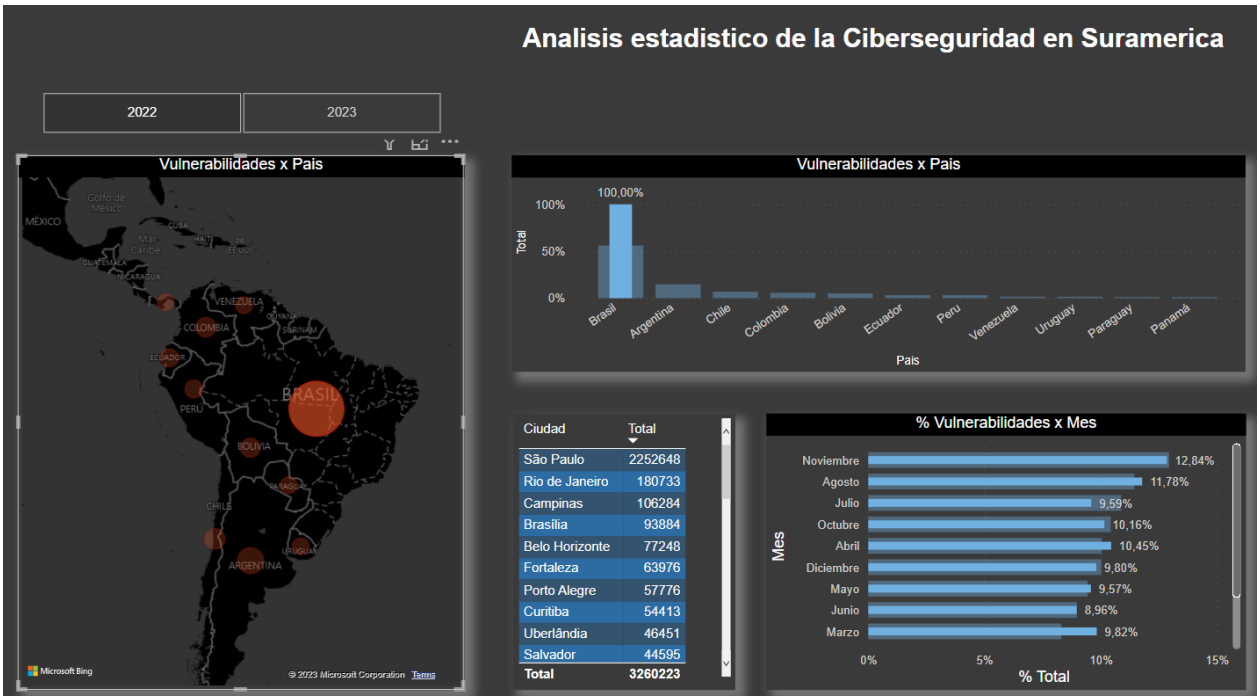
Como se puede apreciar en la siguiente grafica (ver **Figura 45)**, en Perú se reportaron 238 mil vulnerabilidades entre Marzo del 2022 a Marzo del 2023, 206 mil corresponde a los productos más vulnerables entre los que se destaca los servicios de Apache, Microsoft y OpenSsh todos ellos servicios globalmente accesibles y que pueden ser vistos por ciberdelincuentes, 14 mil corresponde al Sistema Operativo donde se destaca Windows que en su mayor parte se atribuye a sistemas obsoletos como es el caso de Windows 7, 2000, 2003 etc., sistemas no parchados y/o sistemas no licenciados. Por último 197 mil corresponde a los puertos más vulnerables entre los que se destaca el puerto 80 y 443 que corresponde a portales web y puerto 22 que corresponde a accesos remotos.

Figura 45 – Análisis estadísticos de la Ciberseguridad – Detallado – Perú



Brasil

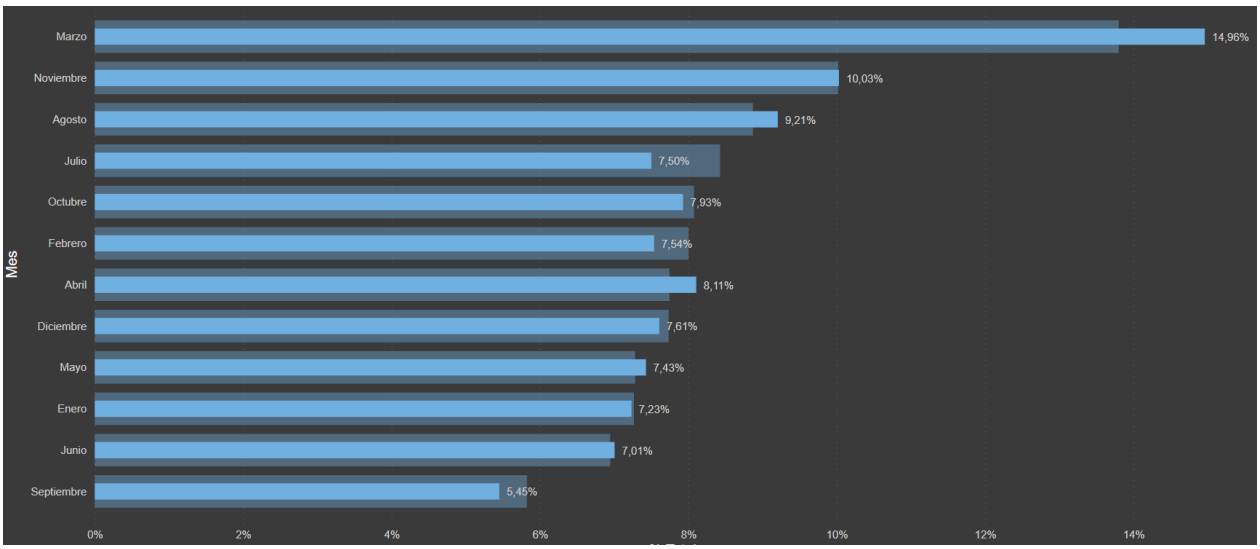
Figura 46 – Análisis estadísticos de la Ciberseguridad en Brasil marzo 2022 a marzo 2023



Como se puede destacar en la figura anterior (ver **Figura 46)** las vulnerabilidades mostradas por mes en Brasil son muy variables de un mes a otro, siendo noviembre y agosto los meses con más vulnerabilidades mostradas, aunque de un mes a otro se nota la diminución de vulnerabilidades debido a la corrección de algunas de ellas, se nota también el crecimiento de un mes a otro que se debe a la aparición de nuevas vulnerabilidades.

Se destaca que no es mucho el impacto que se realiza en Brasil a la hora de corregir vulnerabilidades (ver **Figura 47)**, ello se debe al desconocimiento de muchas de las vulnerabilidades expuestas a través de fuentes abiertas.

Figura 47 – Vulnerabilidades Mes a Mes – Brasil de marzo 2022 a marzo 2023

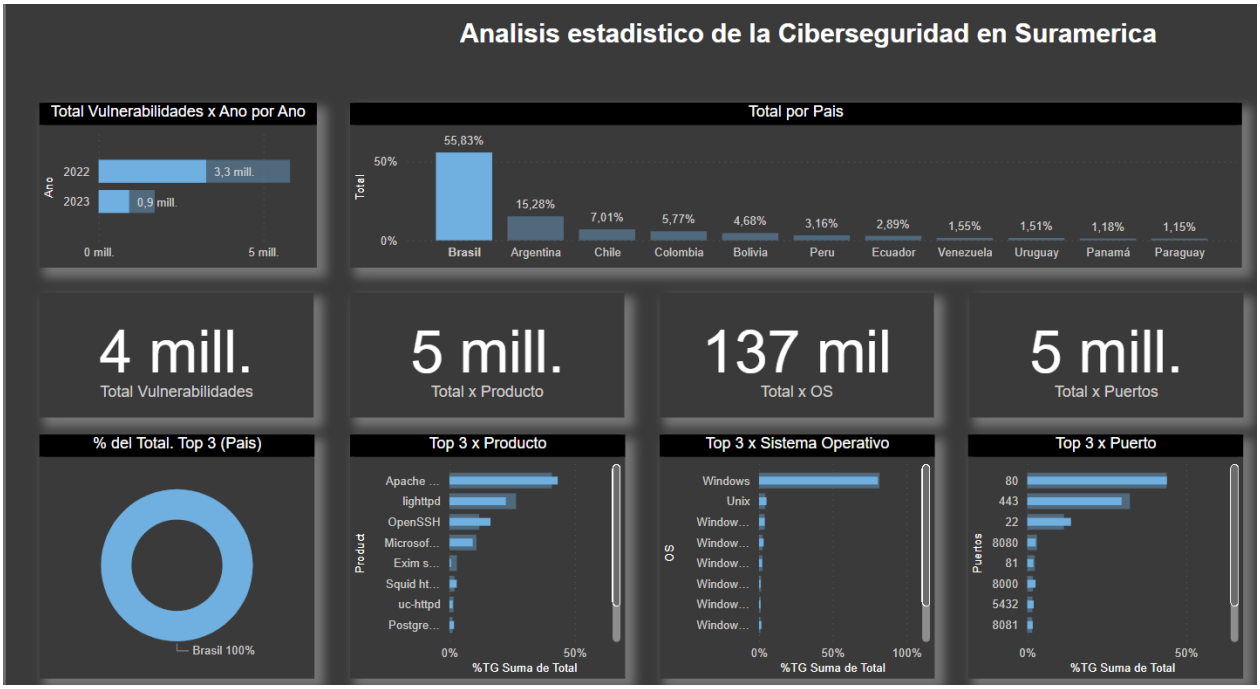


Las 5 ciudades que más vulnerabilidades reporto en el periodo de tiempo analizado, fueron en orden de importancia: Sao Paulo, Rio de Janeiro, Campinas, Brasilia y Belo Horizonte. Esto destaca que son las ciudades con más activos de información expuesto en Internet.

Como se puede apreciar en la siguiente grafica (ver **Figura 48)**, en Brasil se reportaron 4 millones de vulnerabilidades entre Marzo del 2022 a Marzo del 2023, 5 millones corresponde a los productos más vulnerables entre los que se destaca los servicios de Apache, Lighttp y

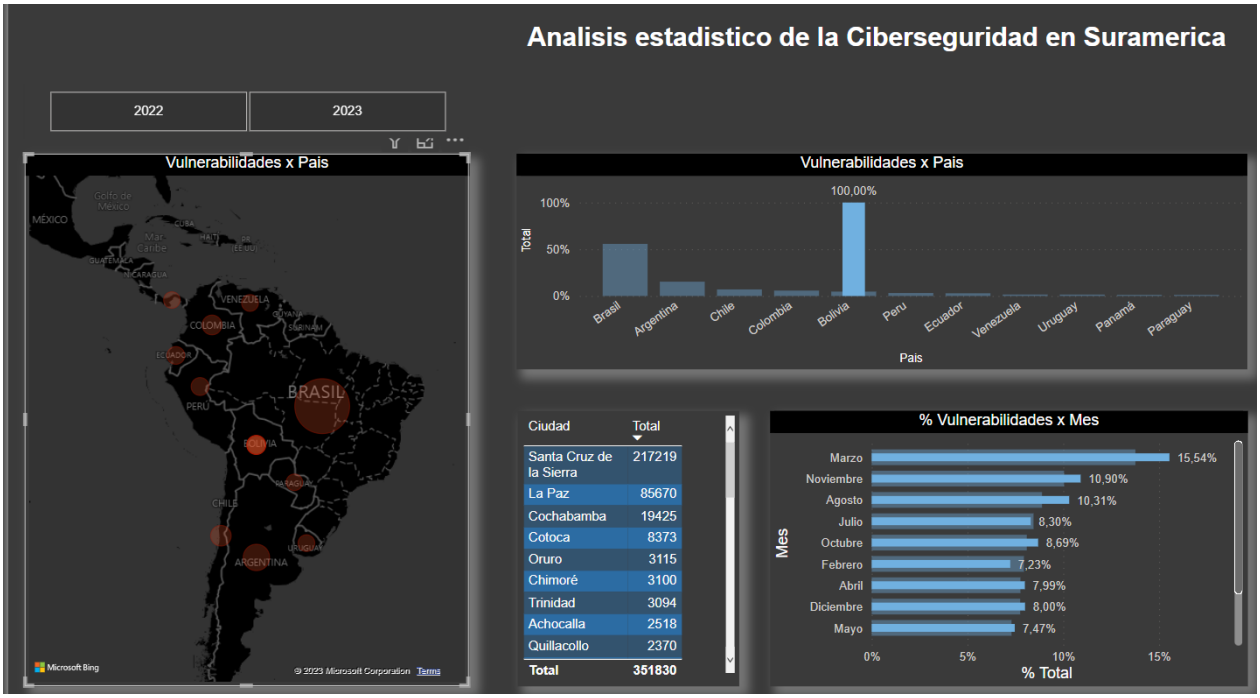
OpenSsh todos ellos servicios globalmente accesibles y que pueden ser vistos por ciberdelincuentes, 137 mil corresponde al Sistema Operativo donde se destaca Windows que en su mayor parte se atribuye a sistemas obsoletos como es el caso de Windows 7, 2000, 2003 etc., sistemas no parchados y/o sistemas no licenciados. Por último 5 millones corresponde a los puertos más vulnerables entre los que se destaca el puerto 80 y 443 que corresponde a portales web y puerto 22 que corresponde a accesos remotos.

Figura 48 – Análisis estadísticos de la Ciberseguridad – Detallado – Brasil



Bolivia

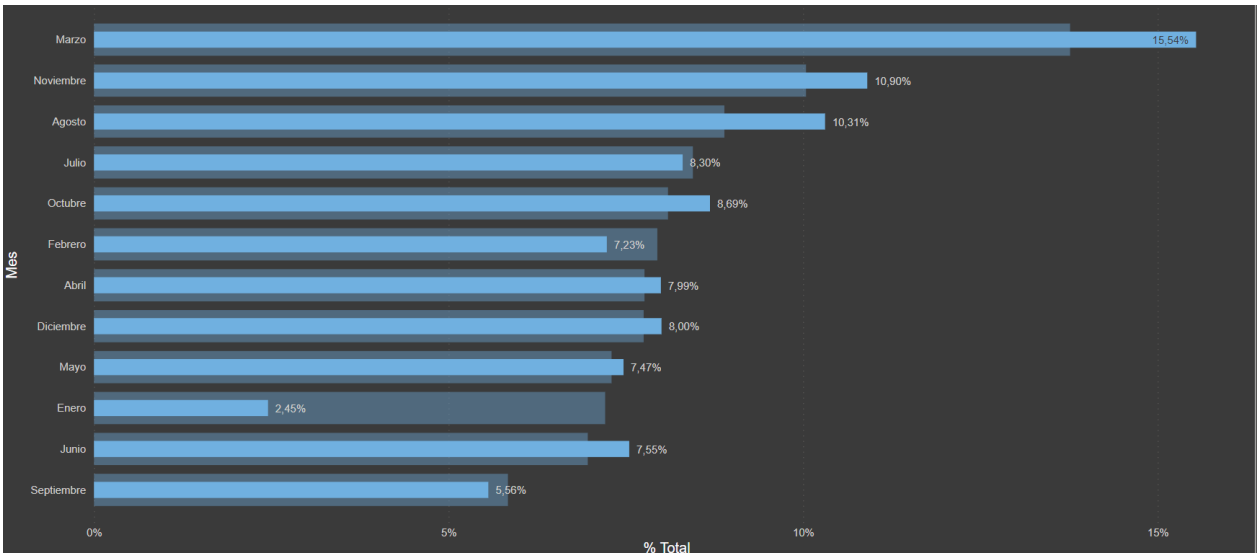
Figura 49 – Análisis estadísticos de la Ciberseguridad en Bolivia marzo 2022 a marzo 2023



Como se puede destacar en la figura anterior (ver **Figura 49)** las vulnerabilidades mostradas por mes en Bolivia son muy variables de un mes a otro, siendo marzo, noviembre y agosto los meses con más vulnerabilidades mostradas, aunque de un mes a otro se nota la diminución de vulnerabilidades debido a la corrección de algunas de ellas, se nota también el crecimiento de un mes a otro que se debe a la aparición de nuevas vulnerabilidades.

Se destaca que no es mucho el impacto que se realiza en Bolivia a la hora de corregir vulnerabilidades (ver **Figura 50)**, ello se debe al desconocimiento de muchas de las vulnerabilidades expuestas a través de fuentes abiertas.

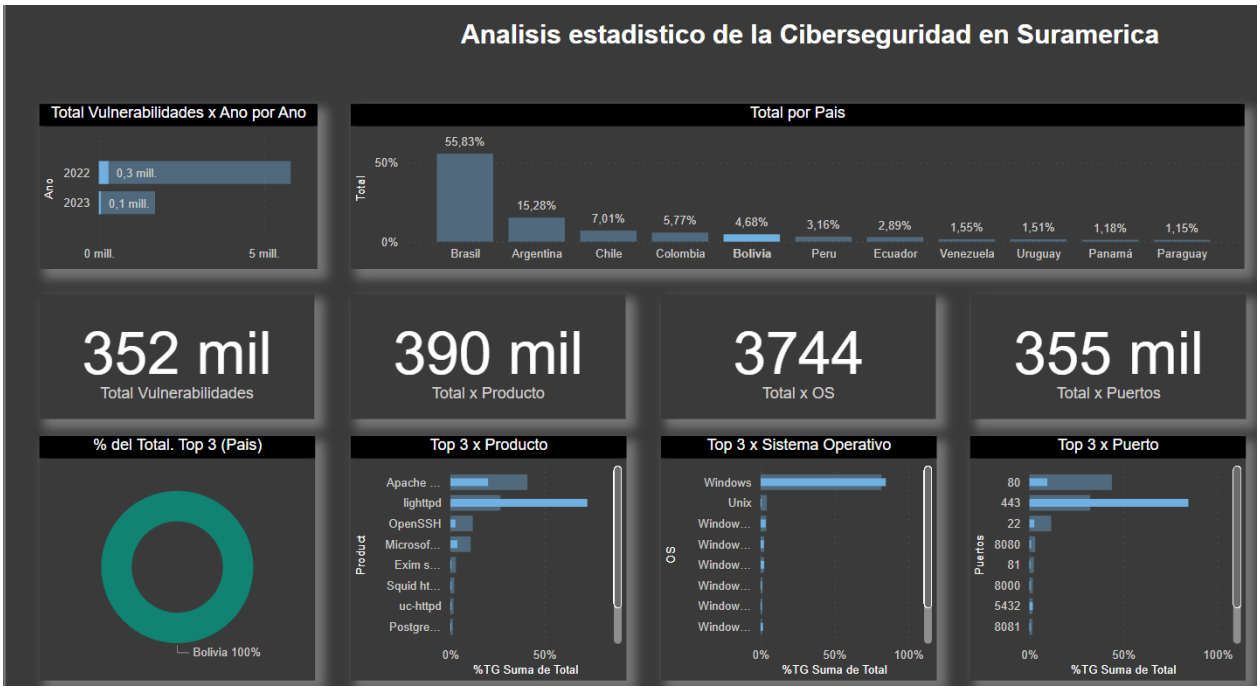
Figura 50 – Vulnerabilidades Mes a Mes – Bolivia de marzo 2022 a marzo 2023



Las 5 ciudades que más vulnerabilidades reporto en el periodo de tiempo analizado, fueron en orden de importancia: Santa Cruz de la Sierra, La Paz, Cochabamba, Cotoca y Oruro. Esto destaca que son las ciudades con más activos de información expuesto en Internet.

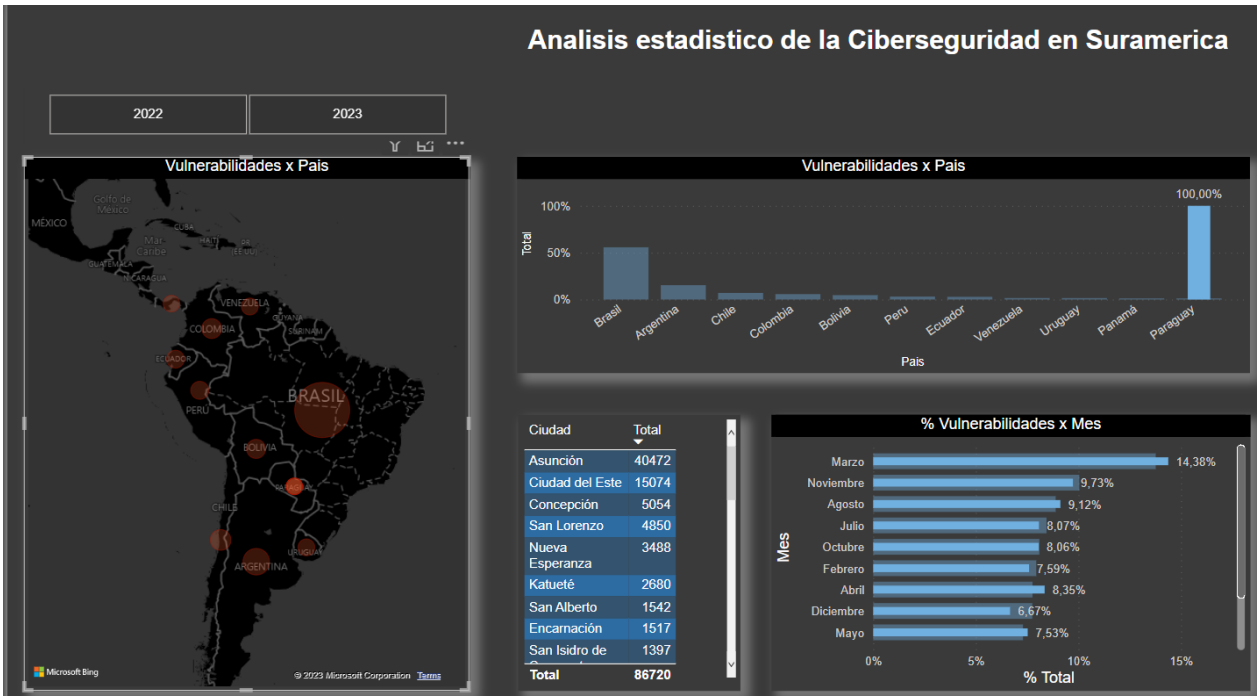
Como se puede apreciar en la siguiente grafica (ver **Figura 51)**, en Bolivia se reportaron 352 mil vulnerabilidades entre Marzo del 2022 a Marzo del 2023, 390 mil corresponde a los productos más vulnerables entre los que se destaca los servicios de Apache, Lighttp, OpenSsh y Microsoft todos ellos servicios globalmente accesibles y que pueden ser vistos por ciberdelincuentes, 3.744 corresponde al Sistema Operativo donde se destaca Windows que en su mayor parte se atribuye a sistemas obsoletos como es el caso de Windows 7, 2000, 2003 etc., sistemas no parchados y/o sistemas no licenciados. Por último 355 mil corresponde a los puertos más vulnerables entre los que se destaca el puerto 80 y 443 que corresponde a portales web y puerto 22 que corresponde a accesos remotos.

Figura 51 – Análisis estadísticos de la Ciberseguridad – Detallado – Bolivia



Paraguay

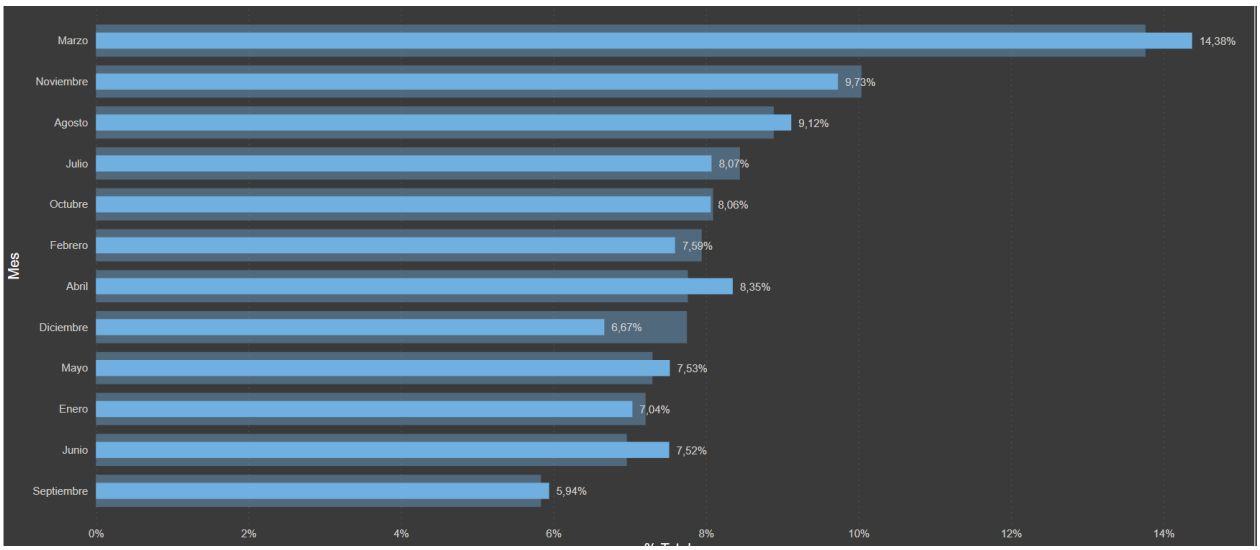
Figura 52 – Análisis estadísticos de la Ciberseguridad en Paraguay marzo 2022 a marzo 2023



Como se puede destacar en la figura anterior (ver **Figura 52)** las vulnerabilidades mostradas por mes en Paraguay son muy variables de un mes a otro, siendo marzo, noviembre y agosto los meses con más vulnerabilidades mostradas, aunque de un mes a otro se nota la diminución de vulnerabilidades debido a la corrección de algunas de ellas, se nota también el crecimiento de un mes a otro que se debe a la aparición de nuevas vulnerabilidades.

Se destaca que no es mucho el impacto que se realiza en Bolivia a la hora de corregir vulnerabilidades (ver **Figura 53)**, ello se debe al desconocimiento de muchas de las vulnerabilidades expuestas a través de fuentes abiertas.

Figura 53 – Vulnerabilidades Mes a Mes – Paraguay de marzo 2022 a marzo 2023

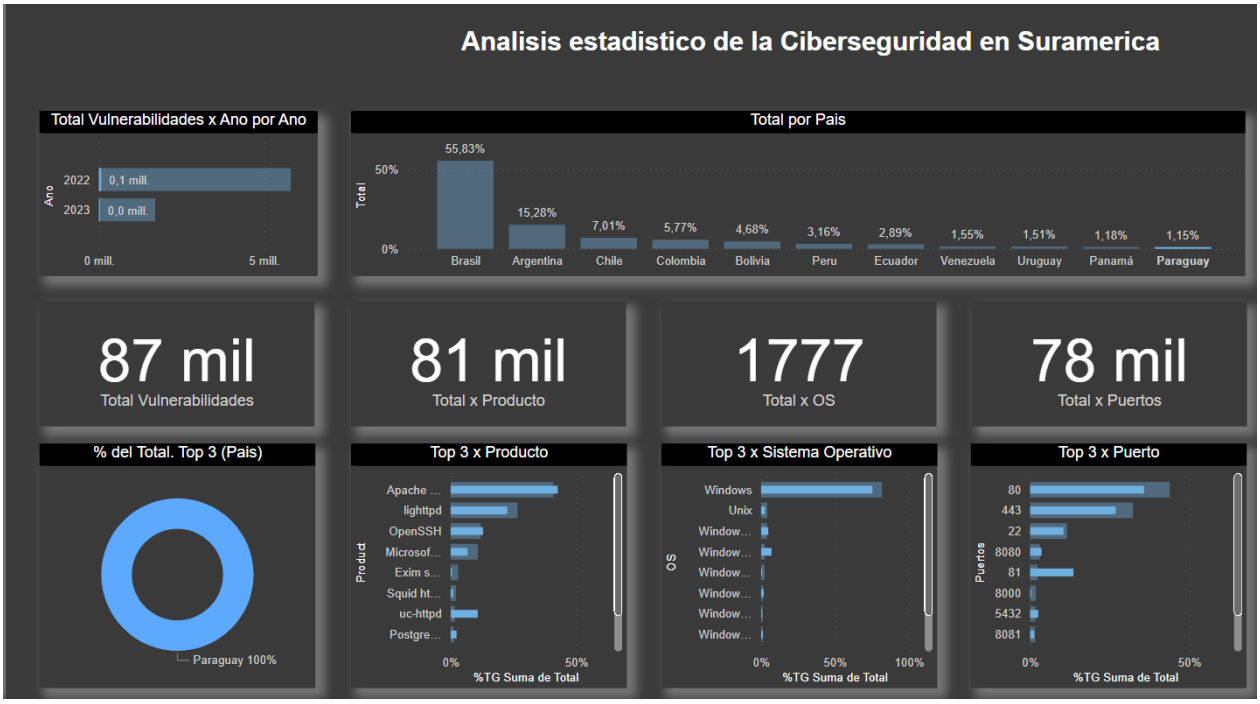


Las 5 ciudades que más vulnerabilidades reporto en el periodo de tiempo analizado, fueron en orden de importancia: Asunción, Ciudad del Este, Concepción, San Lorenzo y Nueva Esperanza. Esto destaca que son las ciudades con más activos de información expuesto en Internet.

Como se puede apreciar en la siguiente grafica (ver **Figura 54)**, en Paraguay se reportaron 87 mil vulnerabilidades entre Marzo del 2022 a Marzo del 2023, 81 mil corresponde a los productos más vulnerables entre los que se destaca los servicios de Apache, Lighttp y

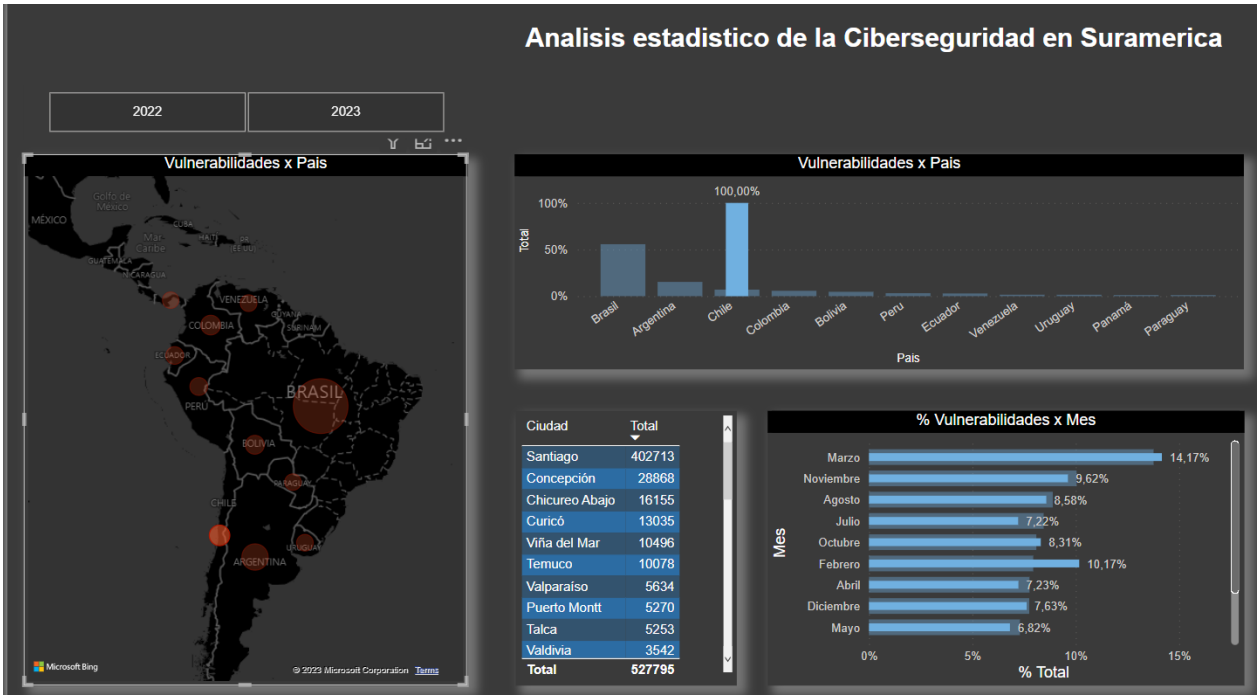
OpenSsh todos ellos servicios globalmente accesibles y que pueden ser vistos por ciberdelincuentes, 1.777 corresponde al Sistema Operativo donde se destaca Windows que en su mayor parte se atribuye a sistemas obsoletos como es el caso de Windows 7, 2000, 2003 etc., sistemas no parchados y/o sistemas no licenciados. Por último 78 mil corresponde a los puertos más vulnerables entre los que se destaca el puerto 80, 443 y 81 que corresponde a portales web y puerto 22 que corresponde a accesos remotos.

Figura 54 – Análisis estadísticos de la Ciberseguridad – Detallado – Paraguay



Chile

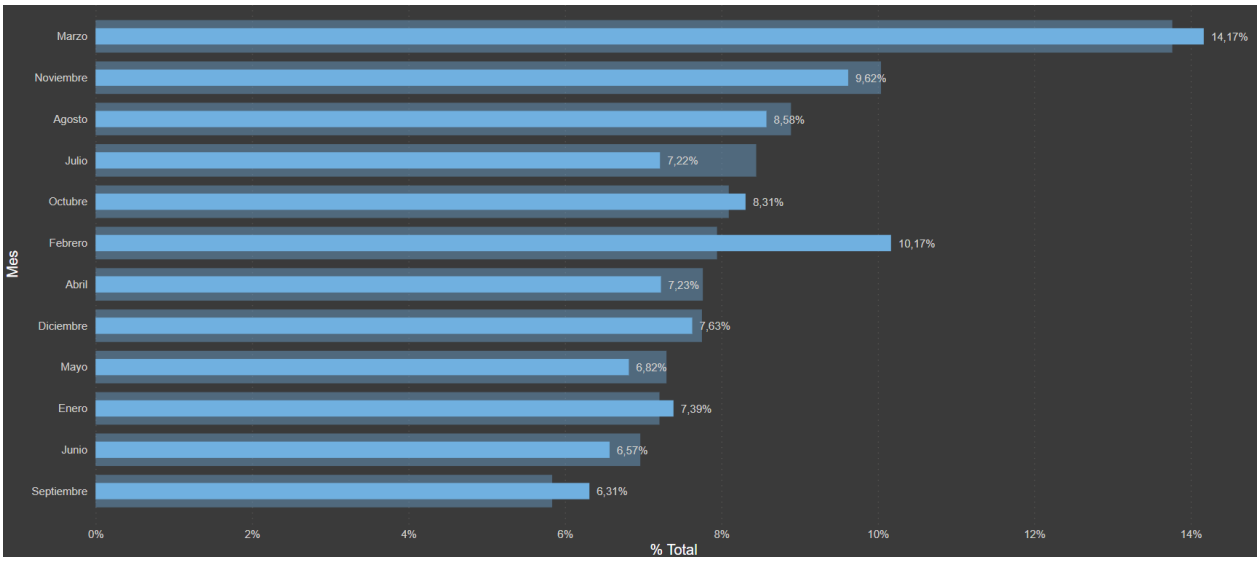
Figura 55 – Análisis estadísticos de la Ciberseguridad en Chile marzo 2022 a marzo 2023



Como se puede destacar en la figura anterior (ver **Figura 55)** las vulnerabilidades mostradas por mes en Chile son muy variables de un mes a otro, siendo marzo, noviembre y febrero los meses con más vulnerabilidades mostradas, aunque de un mes a otro se nota la diminución de vulnerabilidades debido a la corrección de algunas de ellas, se nota también el crecimiento de un mes a otro que se debe a la aparición de nuevas vulnerabilidades.

Se destaca que no es mucho el impacto que se realiza en Chile a la hora de corregir vulnerabilidades (ver **Figura 56)**, ello se debe al desconocimiento de muchas de las vulnerabilidades expuestas a través de fuentes abiertas.

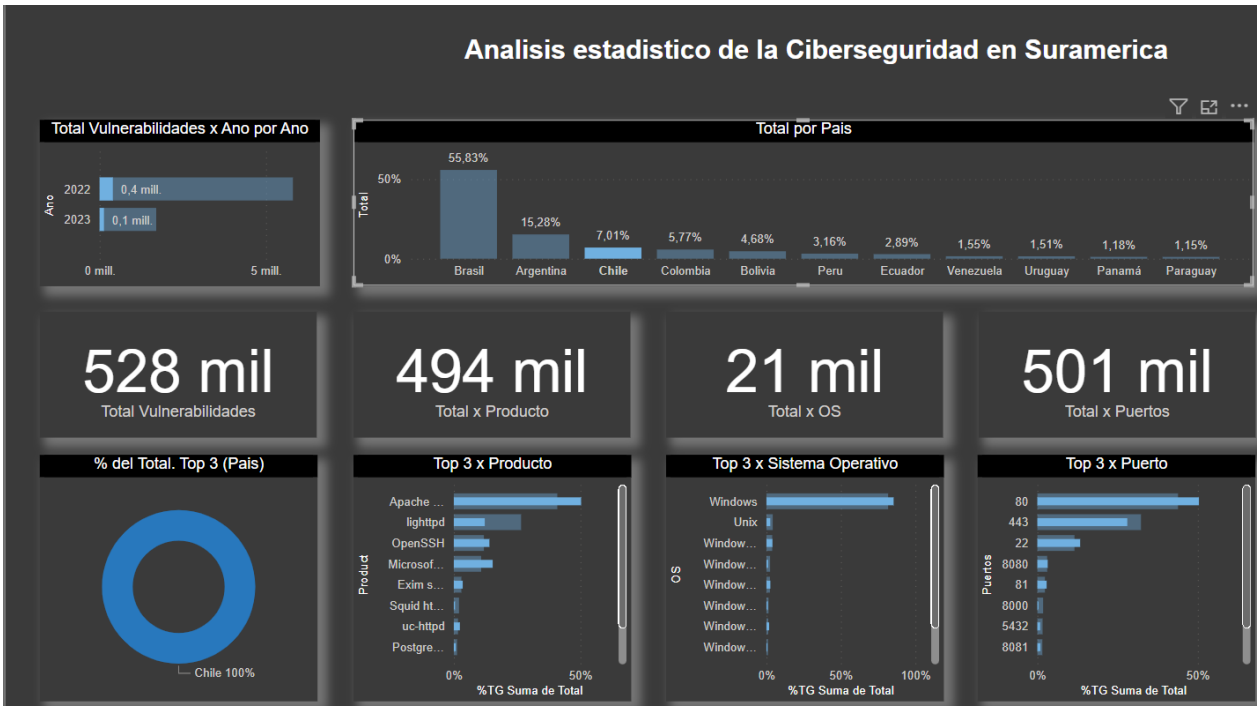
Figura 56 – Vulnerabilidades Mes a Mes – Chile de marzo 2022 a marzo 2023



Las 5 ciudades que más vulnerabilidades reporto en el periodo de tiempo analizado, fueron en orden de importancia: Santiago, Concepción, Chicureo Abajo, Curicó y Villa del Mar. Esto destaca que son las ciudades con más activos de información expuesto en Internet.

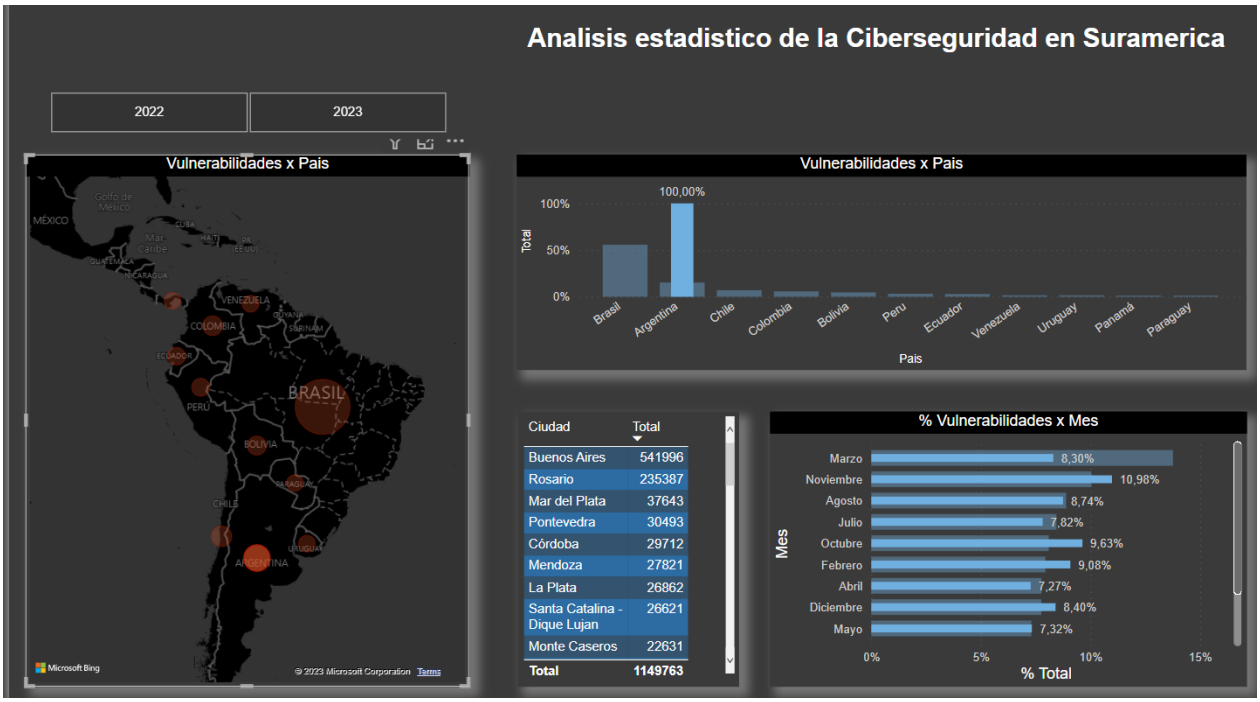
Como se puede apreciar en la siguiente grafica (ver **Figura 57)**, en Chile se reportaron 528 mil vulnerabilidades entre Marzo del 2022 a Marzo del 2023, 494 mil corresponde a los productos más vulnerables entre los que se destaca los servicios de Apache, Lighttp, OpenSsh y Microsoft, todos ellos servicios globalmente accesibles y que pueden ser vistos por ciberdelincuentes, 21 mil corresponde al Sistema Operativo donde se destaca Windows que en su mayor parte se atribuye a sistemas obsoletos como es el caso de Windows 7, 2000, 2003 etc., sistemas no parchados y/o sistemas no licenciados. Por último 501 mil corresponde a los puertos más vulnerables entre los que se destaca el puerto 80 y 443 que corresponde a portales web y puerto 22 que corresponde a accesos remotos.

Figura 57 – Análisis estadísticos de la Ciberseguridad – Detallado – Chile



Argentina

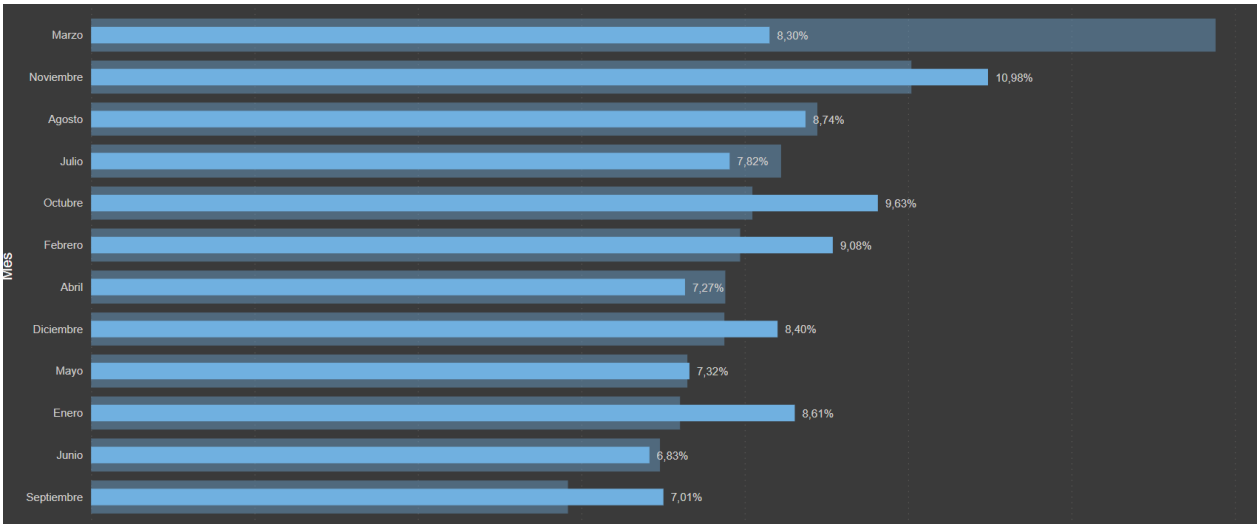
Figura 58 – Análisis estadísticos de la Ciberseguridad en Argentina marzo 2022 a marzo 2023



Como se puede destacar en la figura anterior (ver **Figura 58)** las vulnerabilidades mostradas por mes en Argentina son muy variables de un mes a otro, siendo noviembre, octubre y febrero los meses con más vulnerabilidades mostradas, aunque de un mes a otro se nota la diminución de vulnerabilidades debido a la corrección de algunas de ellas, se nota también el crecimiento de un mes a otro que se debe a la aparición de nuevas vulnerabilidades.

Se destaca que no es mucho el impacto que se realiza en Argentina a la hora de corregir vulnerabilidades (ver **Figura 59)**, ello se debe al desconocimiento de muchas de las vulnerabilidades expuestas a través de fuentes abiertas.

Figura 59 – Vulnerabilidades Mes a Mes – Argentina de marzo 2022 a marzo 2023

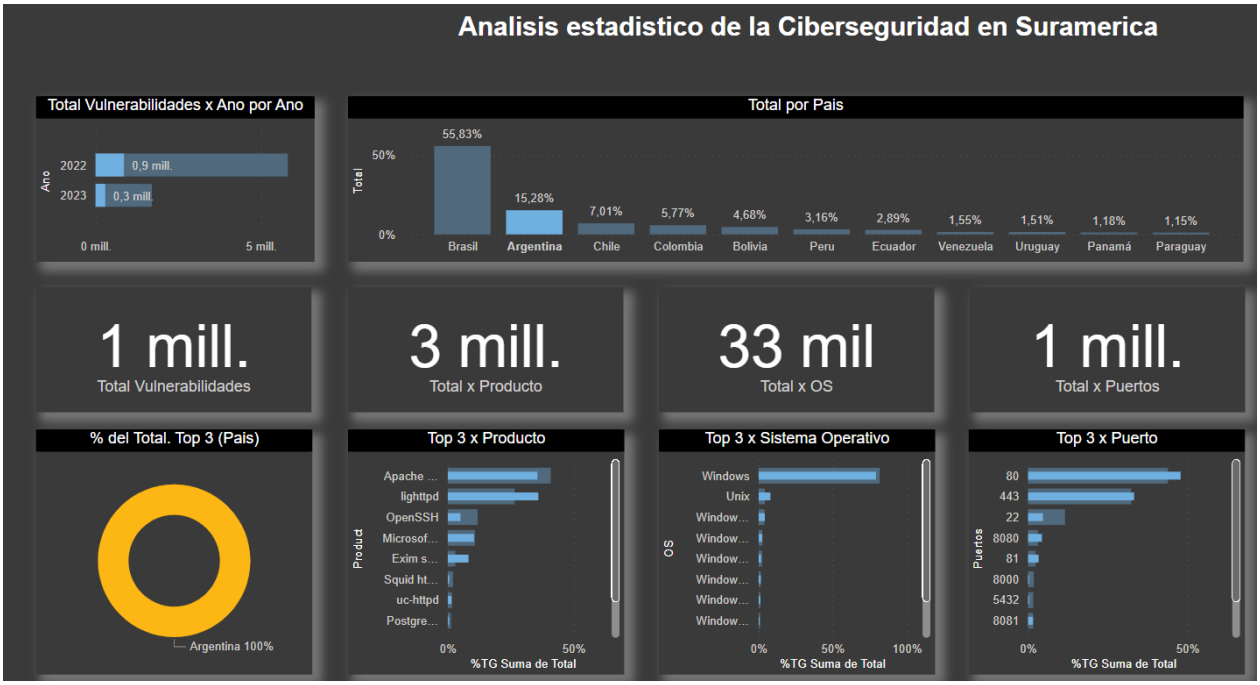


Las 5 ciudades que más vulnerabilidades reporto en el periodo de tiempo analizado, fueron en orden de importancia: Buenos Aires, Rosario, Mar del Plata, Pontevedra y Córdoba. Esto destaca que son las ciudades con más activos de información expuesto en Internet.

Como se puede apreciar en la siguiente grafica (ver **Figura 60)**, en Argentina se reportaron 1 millón de vulnerabilidades entre Marzo del 2022 a Marzo del 2023, 3 millones corresponde a los productos más vulnerables entre los que se destaca los servicios de Apache, Lighttp, OpenSsh y Microsoft, todos ellos servicios globalmente accesibles y que pueden ser vistos por ciberdelincuentes, 33 mil corresponde al Sistema Operativo donde se destaca

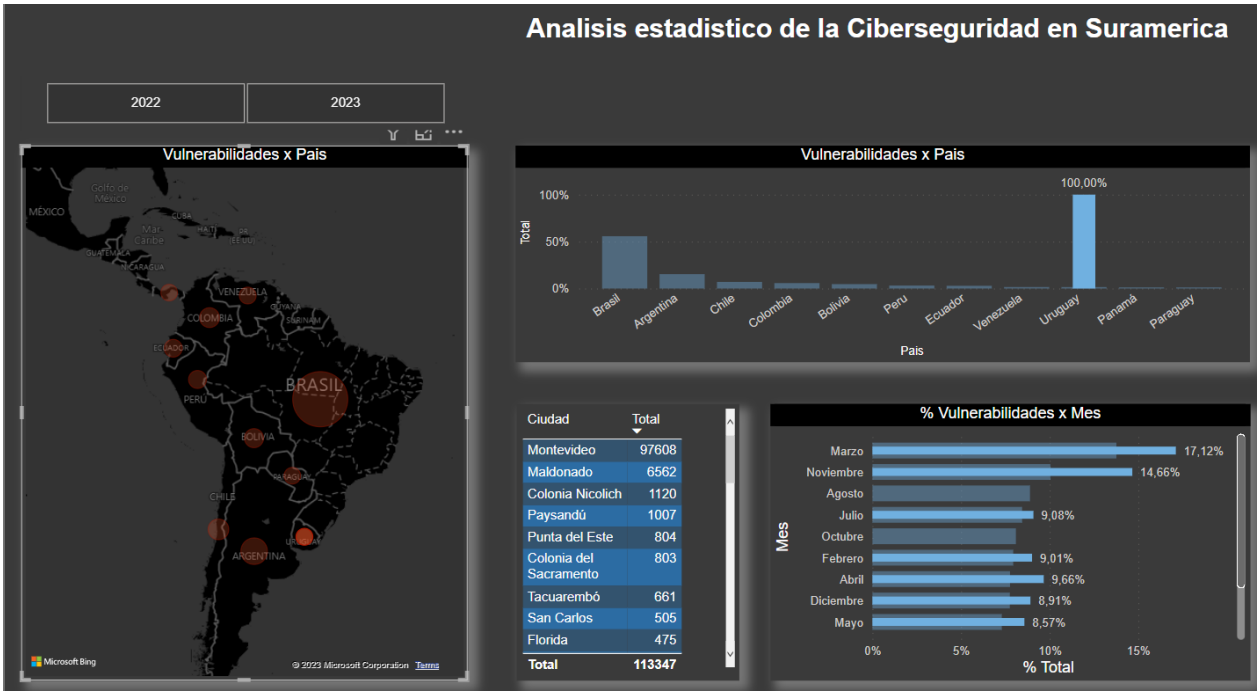
Windows que en su mayor parte se atribuye a sistemas obsoletos como es el caso de Windows 7, 2000, 2003 etc., sistemas no parchados y/o sistemas no licenciados. Por último 1 millón corresponde a los puertos más vulnerables entre los que se destaca el puerto 80 y 443 que corresponde a portales web y puerto 22 que corresponde a accesos remotos.

Figura 60 – Análisis estadísticos de la Ciberseguridad – Detallado – Argentina



Uruguay

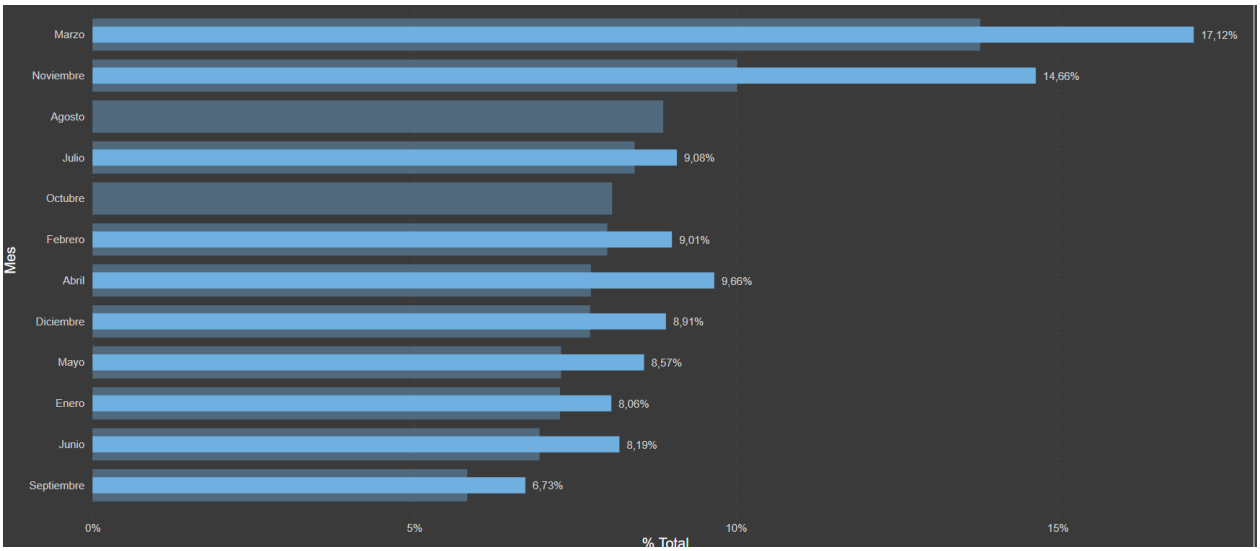
Figura 61 – Análisis estadísticos de la Ciberseguridad en Uruguay marzo 2022 a marzo 2023



Como se puede destacar en la figura anterior (ver **Figura 61)** las vulnerabilidades mostradas por mes en Uruguay son muy variables de un mes a otro, siendo marzo y noviembre los meses con más vulnerabilidades mostradas, aunque de un mes a otro se nota la diminución de vulnerabilidades debido a la corrección de algunas de ellas, se nota también el crecimiento de un mes a otro que se debe a la aparición de nuevas vulnerabilidades. En los meses de agosto y octubre no se obtuvo información debido a que la fuente utilizada (Shodan) no la suministro.

Se destaca que no es mucho el impacto que se realiza en Uruguay a la hora de corregir vulnerabilidades (ver **Figura 62)**, ello se debe al desconocimiento de muchas de las vulnerabilidades expuestas a través de fuentes abiertas.

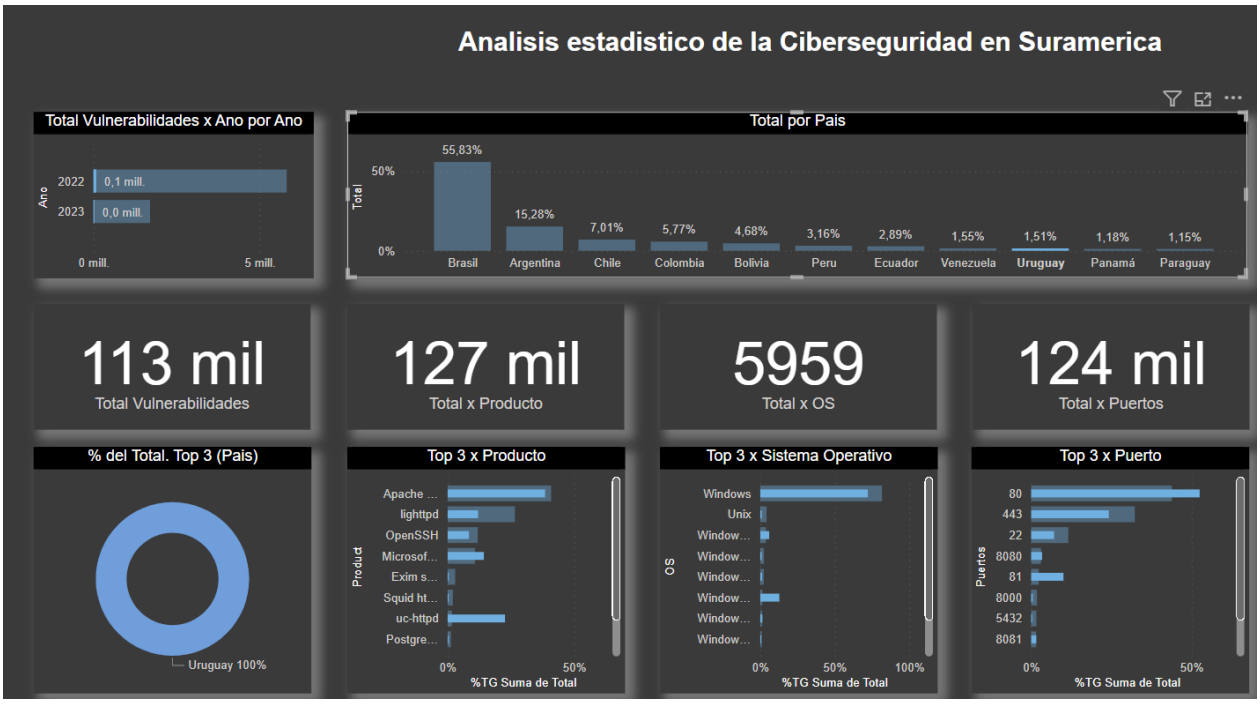
Figura 62 – Vulnerabilidades Mes a Mes – Uruguay de marzo 2022 a marzo 2023



Las 5 ciudades que más vulnerabilidades reporto en el periodo de tiempo analizado, fueron en orden de importancia: Montevideo, Maldonado, Colonia Nicolich, Paysandú y Punta del Este. Esto destaca que son las ciudades con más activos de información expuesto en Internet.

Como se puede apreciar en la siguiente grafica (ver **Figura 63)**, en Uruguay se reportaron 113 mil vulnerabilidades entre Marzo del 2022 a Marzo del 2023, 127 mil corresponde a los productos más vulnerables entre los que se destaca los servicios de Apache, Lighttp, OpenSsh, Microsoft y Uc-http, todos ellos servicios globalmente accesibles y que pueden ser vistos por ciberdelincuentes, 5959 corresponde al Sistema Operativo donde se destaca Windows que en su mayor parte se atribuye a sistemas obsoletos como es el caso de Windows 7, 2000, 2003 etc., sistemas no parchados y/o sistemas no licenciados. Por último 124 mil corresponde a los puertos más vulnerables entre los que se destaca el puerto 80, 443 y 81 que corresponde a portales web y puerto 22 que corresponde a accesos remotos.

Figura 63 – Análisis estadísticos de la Ciberseguridad – Detallado – Uruguay



COMPROBACIÓN DE RESULTADOS

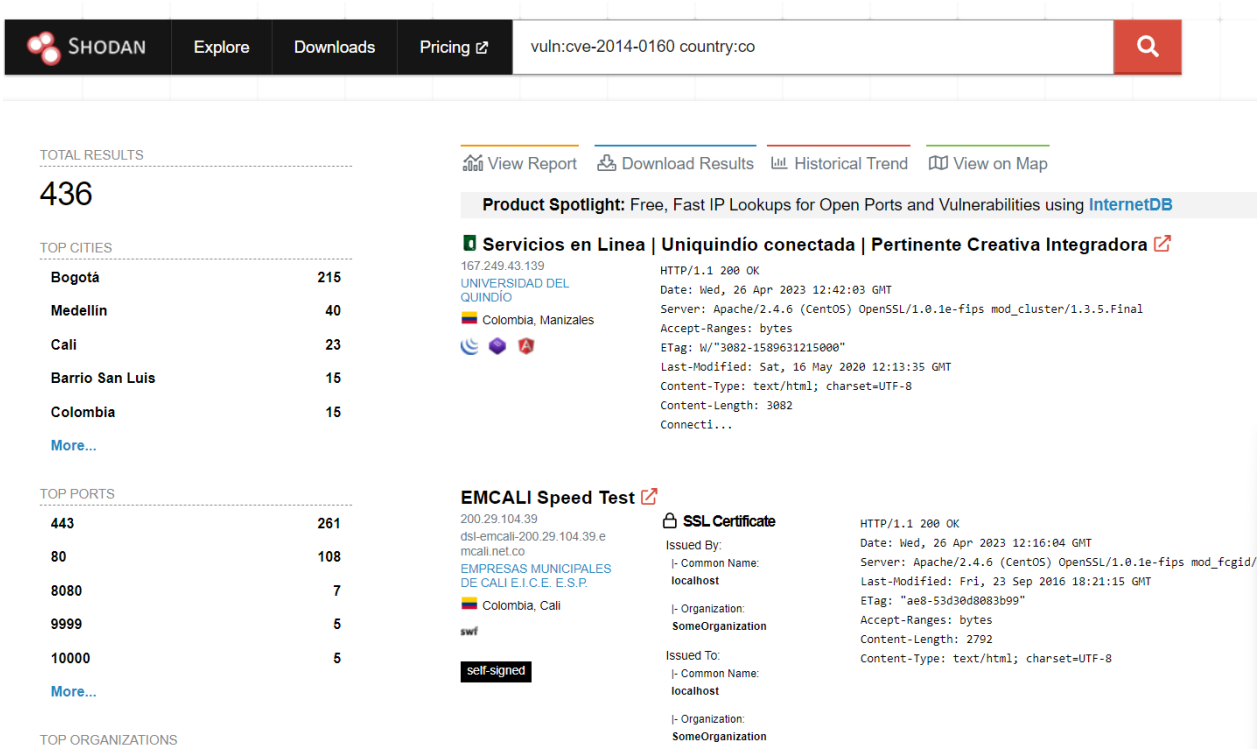
Con el fin de comprobar los resultados de las estadísticas mostradas anteriormente y verificar si validez, vimos que desde Panamá hasta Argentina dentro de los servicios más vulnerables se destacaba el Http[8] y Https[9] que corresponden a los puertos 80 y 443 respectivamente. Estos puertos se asocian normalmente a portales web se asocia no solo a paginas informativas, sino también a páginas de ingreso como son: aplicaciones Web transaccionales, DVR, Switches, routers, Firewall, Etc. Lo que lo convierte en un vector atractivo de ataque para un ciberdelincuente.

Como prueba de concepto, dentro de los diferentes resultados mostrados anteriormente, se tomaron dos servicios relacionados con el puerto 80 y 443, en primera medida se trata del servicio TLS[10] que permite navegar a través de la página web de forma segura donde las comunicaciones son cifradas y los DVR[11] se trata de dispositivos digitales que sirven para grabar video de las cámaras que administra, muy utilizado como servicios de monitoreo de las empresas y hogares que ofrece sus resultados a través de un portal web.

Con relación al servicio TLS existe una vulnerabilidad critica descubierta en el año de 2014 que expone el contenido de lo que tiene la memoria Ram en el momento que se accede a ella de forma maliciosa. La vulnerabilidad fue catalogada como la CVE-2014-0160[12], tomando como ejemplo Colombia, consultamos la vulnerabilidad a través de Shodan mostrando los siguientes resultados: (ver **Figura 64)**

[8] https://es.wikipedia.org/wiki/Protocolo_de_transferencia_de_hipertexto
[9] https://es.wikipedia.org/wiki/Protocolo_seguro_de_transferencia_de_hipertexto
[10] https://es.wikipedia.org/wiki/Seguridad_de_la_capa_de_transporte
[11] https://es.wikipedia.org/wiki/Grabador_de_video_digital
[12] https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-0160

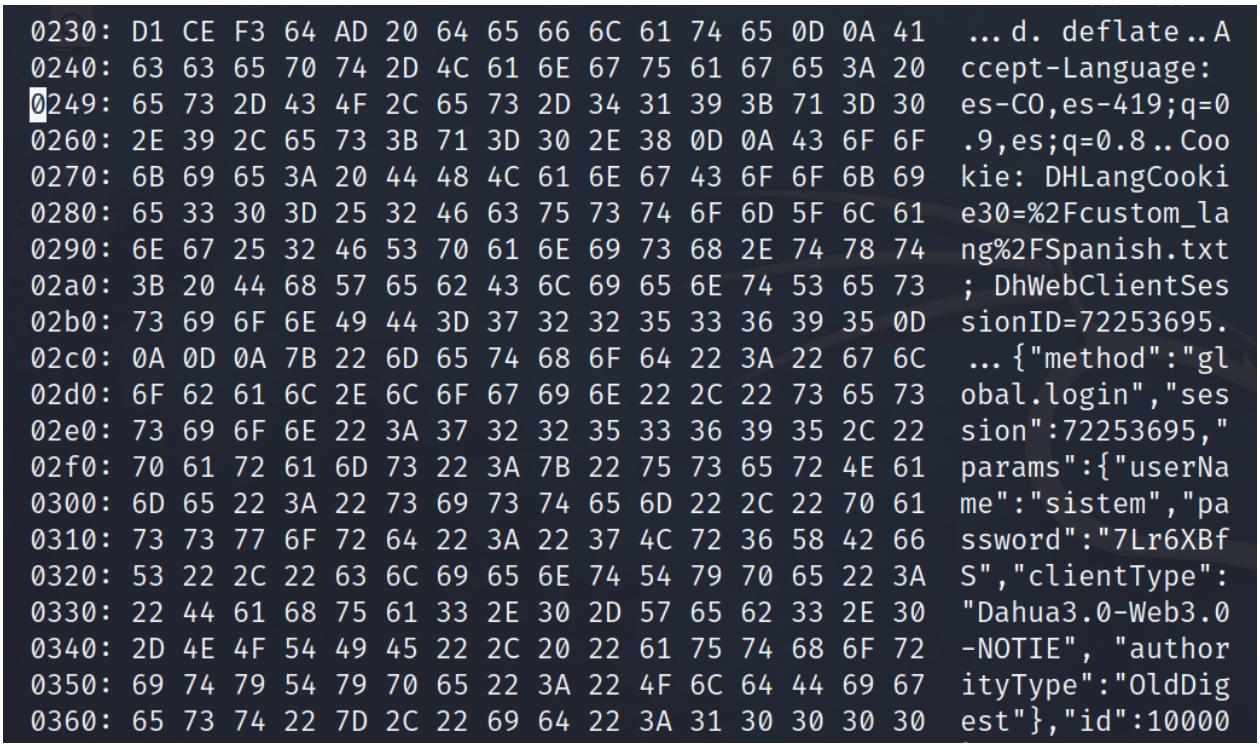
Figura 64 – Resultados vulnerabilidades CVE-2014-0160 en Colombia



Como se puede apreciar aparecen 436 activos de información que son afectados por la vulnerabilidad en cuestión, de los cuales 216 está ubicados en la ciudad de Bogotá, 40 en la ciudad de Medellín y 23 en la ciudad de Cali. Así mismo se confirma que hace parte de los puertos vulnerables como son el 443 y 80.

Ahora de los 436 activos se toma uno al azar y se explota la vulnerabilidad, confirmando efectivamente que la información mostrada por Shodan en verídica, se muestra en la memoria Ram del equipo atacado las credenciales de acceso. (ver **Figura 65)**

Figura 65 – Explotación vulnerabilidad CVE-2014-0160 en Colombia



Con relación a los DVR tomaremos como ejemplo los equipos Dahua[13] y Hikvision[14] que son las marcas más representativas en la comercialización de este tipo de hardware, para ello y basados en las estadísticas anteriores tomaremos el caso de Brasil, en el caso de Hikvision se muestra 15,614 equipos expuestos en Internet a través del puerto 80 (ver **Figura 66)** y en el caso de Dahua se muestra 1.419 equipos expuestos en Internet a través del puerto 80. (ver **Figura 67).**

[13] https://www.dahuasecurity.com/
[14] https://www.hikvision.com/es-la/

Figura 66 – Equipos Hikvision Expuestos en Brasil

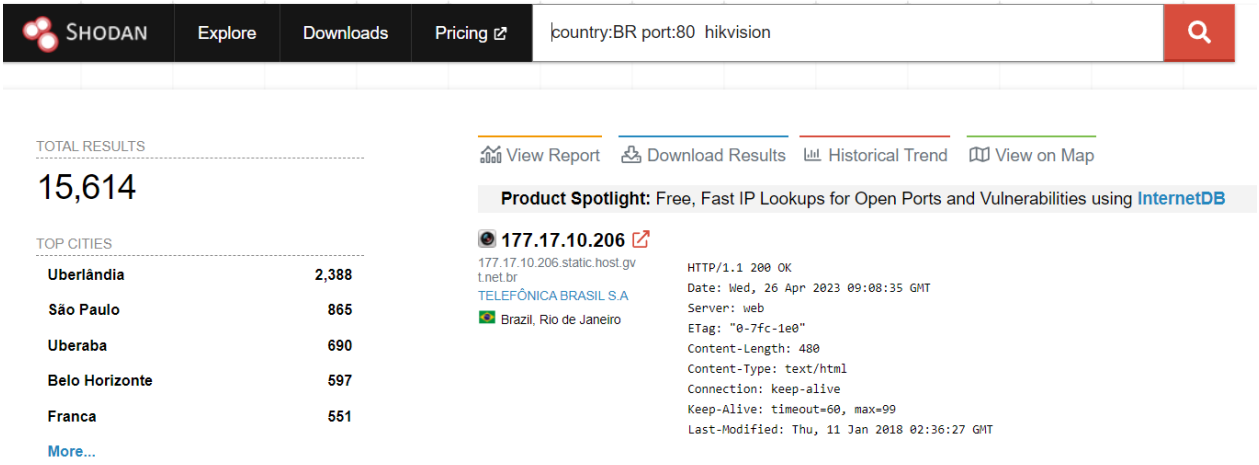
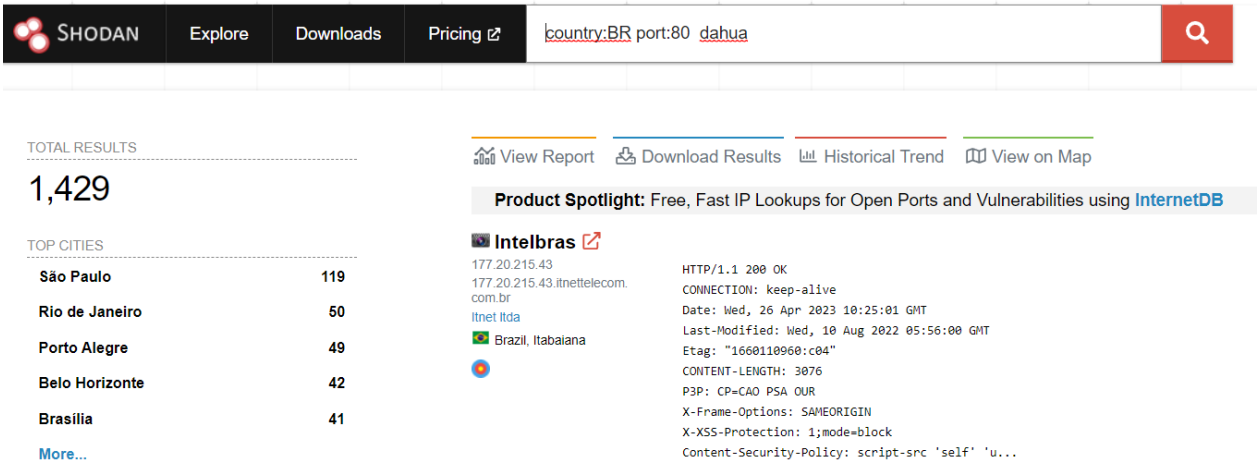


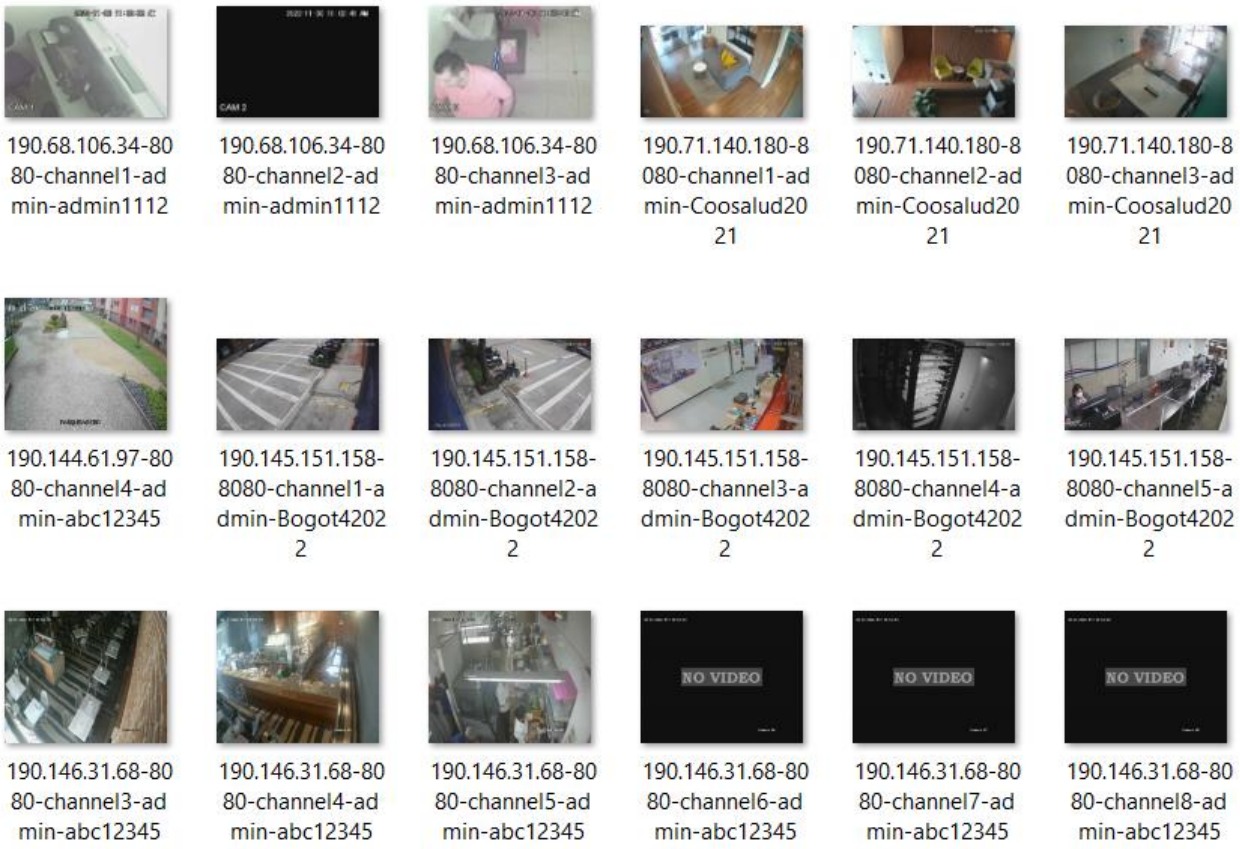
Figura 67 – Equipos Dahua Expuestos en Brasil



Buscando en Internet encontramos una herramienta conocida como Ingram[15] que expone los DVR con vulnerabilidades y permite acceder a su panel de control (ver **Figura 68),** lo que demuestra que no solo Shodan sirve para explotar vulnerabilidades conocidas, sino también como fuente de datos para que, de los resultados obtenidos, se descubra vulnerabilidades en el sistema.

[15] https://github.com/jorhelp/Ingram

Figura 68 – Equipos DVR expuesto en Brasil en Brasil



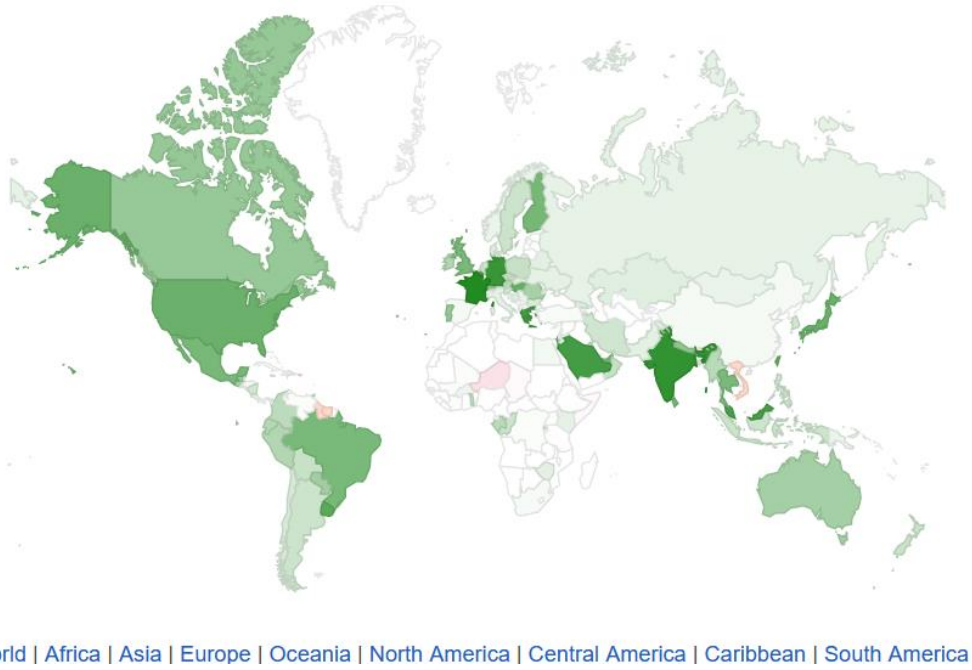
Las muestras de explotación anteriores solo se basaron en el volcado de memoria o en el acceso de los equipos, que se clasifica como un ataque a la confidencialidad de la información, pero se demuestra que herramientas como Shodan le sirve como fuente de datos no solo a los profesionales de la Ciberseguridad, sino también a los Ciberdelincuentes para comprometer sin mucho esfuerzo la Integridad, Confidencialidad y Disponibilidad de la información de los activos expuesto por dicha herramienta.

FUTURO DE LA SOLUCIÓN

No existe a la fecha una herramienta que permita visualizar esta información que permitiría sin duda la toma de decisiones de cualquier país en el mundo, a pesar que se hizo un poco de inteligencia de datos con las diferentes estadísticas sacadas mes a mes en la plataforma SHODAN sobre los principales países de Sur América, es posible ampliar la solución a nivel mundial a través de una plataforma que permite graficar mediante un Mapamundi no solo las vulnerabilidades de Shodan, sino también de las otras como Zoomeye, Censys y/o Criminal IP.

Imaginen este escenario, un usuario a través de un portal Web, visualiza un mapamundi (Ver **Figura 22)** donde le permite seleccionar cualquier región del mundo y te muestras las estadísticas de las vulnerabilidades actuales de esa región discriminadas por las diferentes plataformas mencionadas anteriormente.

Figura 69 – Mapamundi[16] Vulnerabilidades



[16] Imagen tomada de Google: https://www.google.com/intl/es/ipv6/statistics.html#tab=per-country-ipv6-adoption

Además de esto, se puede automatizar la tarea de recolección de información mes a mes y año tras año, para que la solución te permita conocer por ejemplo a petición del usuario las vulnerabilidades que tenía expuestas en el mes de junio del año 2021 de Ecuador, sin duda conllevaría a una herramienta que sería usada por los profesionales de Ciberseguridad.

Espero hacia futuro poder construir esta herramienta con una mezcla de Python e Inteligencia Artificial. Sin Embargo, invito a las futuras generaciones de graduados de la Especialización en Ciberseguridad para que adopten este proyecto y le den el futuro deseado que se pretende.

CONCLUSIONES

Como se puede apreciar en el presente trabajo, la búsqueda de activos de información expuestos en internet, se está convirtiendo en una técnica no solo usada por los profesionales de ciberseguridad, sino también por los ciberdelincuentes que sin mucho esfuerzo y gracias a las fuentes abiertas como Shodan, pueden llegar fácilmente a equipos vulnerables lo cual puede afectar la Confidencialidad, Privacidad y Disponibilidad de la Información.

Se puedo constatar que las empresas no son conscientes de la exposición de sus activos de información en Internet y sobre todo aquellos que por omisión o verificación poseen vulnerabilidades lo que hace que para la ciberdelincuencia en un atractivo menú de exploración y explotación, también se demuestra la falta de capacidad técnica para monitorear basado en sus activos de información la aparición de nuevas vulnerabilidades que puede comprometer a las organizaciones y que antes de que sean indexadas por las fuentes abiertas, están sean parchadas o corregidas, evitando así el compromiso total de la información digital de la empresa.

Por último, uno podría pensar que a medida que avanza la tecnología para un ciberdelincuente se vuelve más difícil irrumpir en otros sistemas; sin embargo, la realidad es otra, las técnicas de OSINT y la misma Inteligencia Artificial (IA) se convierte en las herramientas número uno que facilita no solo las tareas para los profesionales de la Ciberseguridad, si no también para la ciberdelincuencia como tal. Es por ello que las empresas tienen que cambiar la forma de pensar a la hora de proteger sus activos de información ante los adversarios digitales y por ello y de acuerdo a lo que dice el Ph.d. Eric Haseltine en su artículo “The Cyber Security Head Game”17: “Ganar la guerra cibernética, significa vencer la mente de tu adversario y no su tecnología” y ello se logra haciendo que las empresas sean conscientes de:

[17] https://www.psychologytoday.com/intl/blog/long-fuse-big-bang/202209/the-cyber-security-head-game

- Los cortafuegos, el antimalware, el cifrado, los controles de acceso y otras tecnologías de defensa cibernética no pueden garantizar la seguridad cibernética. Estas tecnologías a menudo fallan porque no abordan completamente el comportamiento humano, la mayor vulnerabilidad en cualquier sistema.
- Las defensas cibernéticas a veces se dirigen a las vulnerabilidades humanas, como las amenazas internas, pero casi nunca se dirigen a la psicología del adversario.
- La seguridad efectiva requiere que los defensores "se metan en la cabeza de los ciberdelincuentes" para crear confusión, duda y miedo que eliminen la motivación para atacar.

REFERENCIAS BIBLIOGRAFICAS

Bazzell Michael. (2023). *OSINT Techniques Resources For Uncovering Online Información*. LCCN. 10th edition.

Fernández Félix, Viñuela Yaiza. (2019). *Manual de Ciberinvestigación en Fuentes Abiertas – OSINT para analistas*. Creative Commons.

Matherly John. (2017). *Complete Guide to Shodan - Collect. Analyze. Visualize. Make Internet Intelligence Work for You*. Leanpub

Seisdedos Carlos, Aguilera Vicente. (2022). *Open Source INTelligence (OSINT) - Investigar personas e Identidades en Internet*. 0xword 2da Edición.

Arango Jhon, (2023). Herramienta de Visualización de Datos, https://github.com/jca6185/VulOsint-Latam.git

Universidad®
Católica
de Manizales

VIGILADA MINEDUCACIÓN

Obra de Iglesia
de la Congregación

Hermanas de la Caridad
Dominicas de La Presentación
de la Santísima Virgen

;

Universidad Católica de Manizales
Carrera 23 # 60-63 Av. Santander / Manizales - Colombia
PBX (6)8 93 30 50 - www.ucm.edu.co