IT ACADEMY

PROYECTO FINAL DATA ANALYST

Título:

Amenazas Cibernéticas: Desafíos del Mundo e Industria.

Realizado por Abel Ruiz
en IT Academy curso de Data Analyst

Dirigido por Alana Olivieri
que autoriza la evaluación

1.Evaluación de la Hipótesis

Resumen:

En este estudio se analiza la hipótesis de que los ciberataques criminales han incrementado a lo largo del tiempo, afectando principalmente a la Administración Pública, seguida por los sectores de Finanzas y Salud. Mediante técnicas de análisis de datos y visualización, se exploran las tendencias anuales y la distribución de los ataques, utilizando datos de eventos entre 2014 y 2023. Los resultados indican que la hipótesis es parcialmente válida, con un notable aumento en los ataques hacia la Administración Pública, mientras que los sectores de Finanzas y Salud presentan una incidencia menor y estable.

Introducción:

El incremento de ataques dirigidos a instituciones públicas y sectores estratégicos representa un desafío crítico en la gestión de seguridad y políticas públicas. Este estudio tiene como objetivo evaluar si la Administración Pública ha sido significativamente más afectada que otros sectores clave, durante el período 2014-2023.

Objetivo:

Verificar si los ataques criminales hacia la Administración Pública han incrementado en número y proporción respecto a otros sectores

Hipótesis:

Ha habido un incremento en los ataques hacia la Administración Pública, con tendencias superiores en el tieempo .

2.Metodología:

Datos Utilizados:

```
RangeIndex: 14041 entries, 0 to 14040
Data columns (total 17 columns):
```

Conjunto de datos conteniendo eventos con las siguientes columnas clave:

1.Fecha del Evento (event_date): Fecha o fecha estimada en que ocurrió el evento, en formato DD-MM-AAAA. Las fechas estimadas tienen una precisión de mes y se indican como el primer día de ese mes.
2.Año (year): Año en que ocurrió el evento, en formato AAAA.

3.Actor (actor): Variable de texto que indica el nombre de la organización o individuo responsable del evento; "desconocido" si no se sabe.

4.Tipo de Actor (actor_type): Variable categórica que indica la naturaleza del actor responsable del evento:

Criminal: Organización que accede ilícitamente a redes para obtener ganancias financieras.
Estado-Nación: Una agencia gubernamental, militar o afiliada a ellos.
Terrorista: Un actor no estatal que busca influir en las condiciones políticas o militares atacando a civiles.
Hacktivista: Un individuo o grupo motivado por el activismo social o político.
Aficionado (Hobbyist): Un individuo motivado por la curiosidad o el prestigio.
Organización (sin especificar): Podría referirse a otro tipo de organización (corporación, etc.) no incluida en las categorías anteriores. *Es importante aclarar si esta categoría existe en tus datos.*

5.Organización (organization): Variable de texto que indica el nombre de la organización objetivo cuyas redes fueron violadas ilícitamente.

6.Código de la Clasificación Industrial de América del Norte (NAICS) (industry_code): Código NAICS de dos dígitos que define la organización objetivo.

7.Nombre de la Industria (industry): Variable de texto que indica el nombre de la categoría del código NAICS.

8.Motivo (motive): Variable categórica que indica los resultados deseados por el actor que comete el evento:

Protesta: La interrupción de servicios con el fin de enviar un mensaje político o social a la organización objetivo, o a un gobierno o población indirectamente.
Sabotaje: La destrucción intencional e irreparable de información, redes o dispositivos.
Espionaje: Acceso a redes con fines de inteligencia o vigilancia.
Financiero: Exfiltración de datos confidenciales para obtener ganancias financieras directas o indirectas.

9.Tipo de Evento (event_type): Variable categórica que indica si los efectos finales principales del evento fueron disruptivos, de explotación o una mezcla de ambos:

Disruptivo: Impide las operaciones normales de la organización objetivo.
De Explotación: Acceso o exfiltración ilícita de información confidencial, como información de identificación personal, información clasificada o datos financieros.
Mixto: El evento incorpora elementos disruptivos y de explotación, como un ataque de ransomware.

10.Subtipo de Evento (event_subtype): Variable categórica que clasifica aún más la naturaleza de un evento en función de la parte de la infraestructura de TI de la organización objetivo que se vio más gravemente afectada, independientemente de las tácticas o técnicas utilizadas para lograr el resultado final.

Eventos Disruptivos:

Manipulación de Mensajes: Interferencia con la capacidad de la organización objetivo para presentar o comunicar información con precisión a su base de clientes, electorado u otra audiencia.
Denegación de Servicios Externa: Ejecutada desde dispositivos fuera de la red de la organización objetivo para degradar o negar su capacidad de comunicarse con otros sistemas.
Denegación de Servicios Interna: Ejecutada desde el interior de la red de una organización objetivo para degradar o negar el acceso a otras partes de la red de TI.
Ataque de Datos: La manipulación, destrucción o cifrado de datos en la red de una organización objetivo.

Ataque Físico: El uso de componentes de TI, como los sistemas SCADA, para manipular, degradar o destruir sistemas físicos.

Eventos de Explotación:

Explotación de Sensores: El robo de datos de un dispositivo periférico, como un lector de tarjetas de crédito, un televisor inteligente o un monitor de bebés.

Explotación de Host Final: El robo de datos almacenados en las computadoras de escritorio, portátiles o dispositivos móviles de los usuarios.

Explotación de la Infraestructura de Red: El robo de datos a través del acceso directo a equipos de red, como routers, switches y módems.

Explotación del Servidor de Aplicaciones: El uso de una mala configuración o vulnerabilidad para obtener acceso a los datos en una aplicación del lado del servidor (por ejemplo, una base de datos) o en el servidor mismo.

Explotación de Datos en Tránsito: La adquisición de datos que se mueven entre dispositivos.

11Descripción del Evento (description): Variable de texto que consta de 1-3 oraciones que detallan el evento.

12País Objetivo (country): Variable de texto que consta del código de país ISO de 3 letras para la ubicación de la organización objetivo.

13País del Actor (attacking_country): Variable de texto que consta del código de país ISO de 3 letras para la ubicación del actor.

Preprocesamiento de Datos:

Eliminación de duplicados.

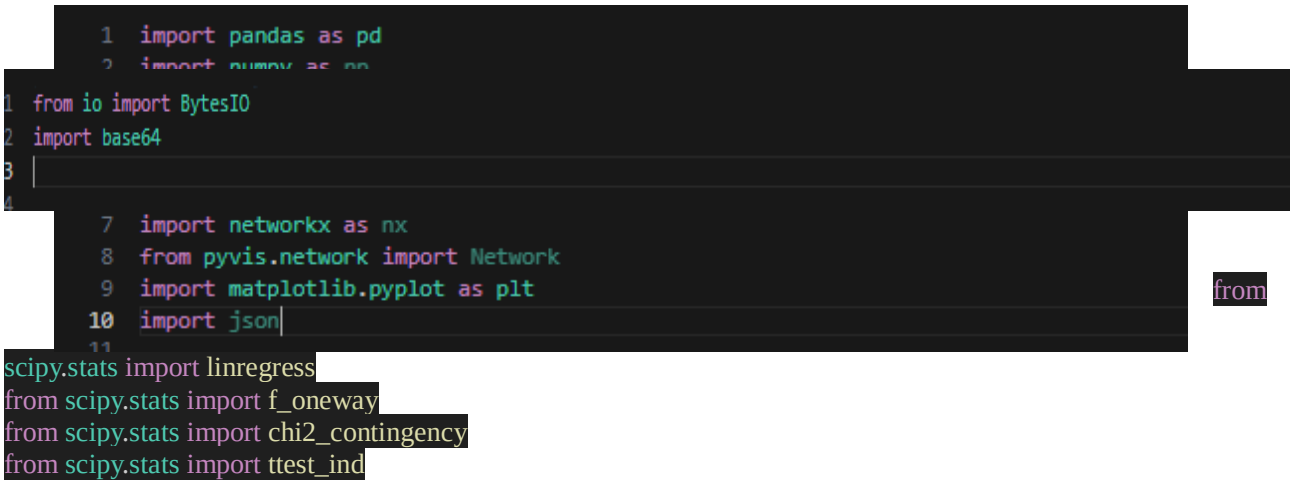
Normalización de nombres .

Agrupación .

Cálculos.

Test estadísticos .

Python



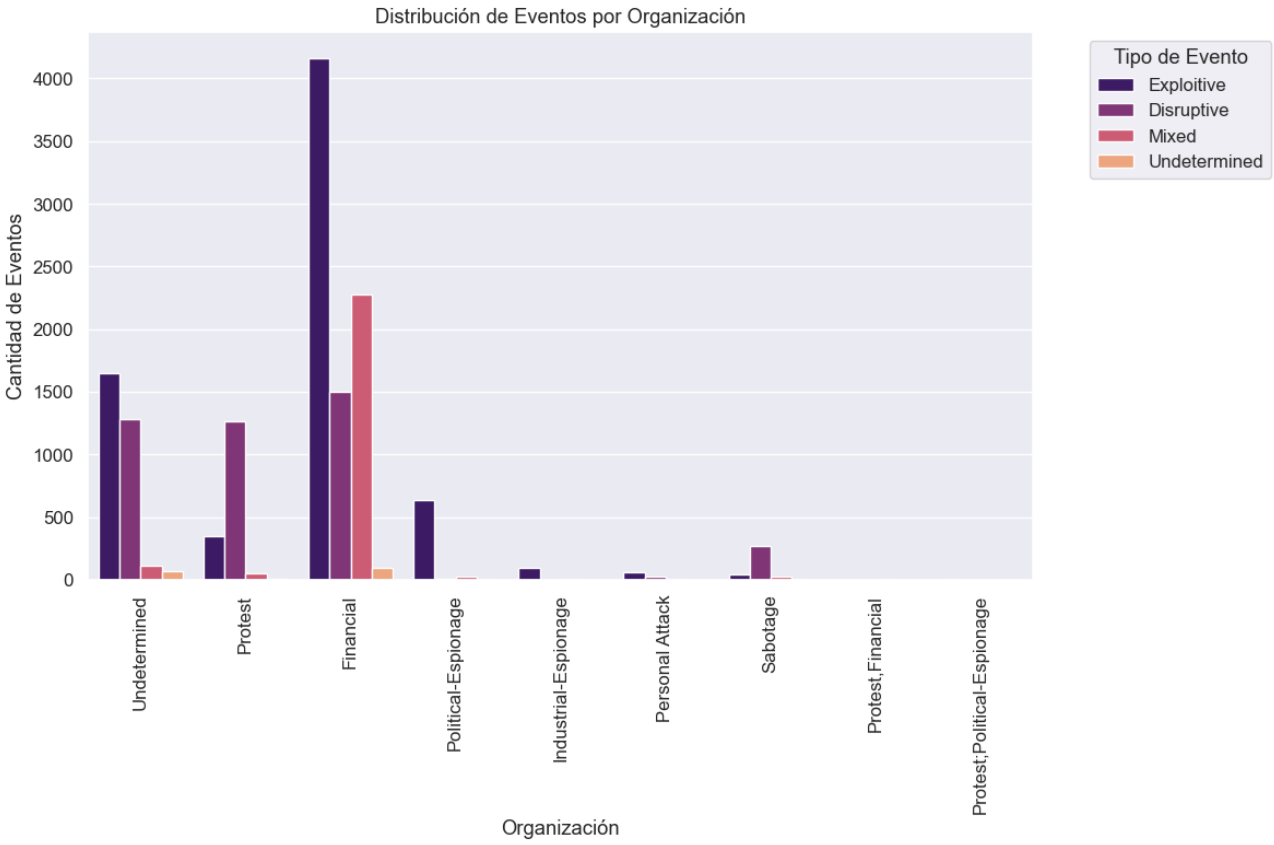
```python
import pandas as pd
import numpy as np
from io import BytesIO
import base64

import networkx as nx
from pyvis.network import Network
import matplotlib.pyplot as plt
import json

from scipy.stats import linregress
from scipy.stats import f_oneway
from scipy.stats import chi2_contingency
from scipy.stats import ttest_ind
```

3.Visualizaciones:

- Gráficos de líneas .
- Mapas de calor para identificar concentraciones .
- Mapas globales.
- Gráficos de barras.
- Circulares.



Análisis del Gráfico

1. Predominancia de Eventos Exploitativos :

- Tanto la categoría "Financial" como "Protest" muestran una alta incidencia de eventos exploitativos. Esto puede indicar que las organizaciones en estas categorías son objetivos preferidos para exploits debido a su valor financiero o impacto social.

2. Diversidad de Eventos en Diferentes Categorías :

- La distribución de tipos de eventos varía entre categorías. Por ejemplo, la categoría "Political-Espionage" tiene una mezcla de eventos exploitativos y mixtos, lo que sugiere objetivos variados y tácticas utilizadas.

3. Baja Incidencia en Algunas Categorías :

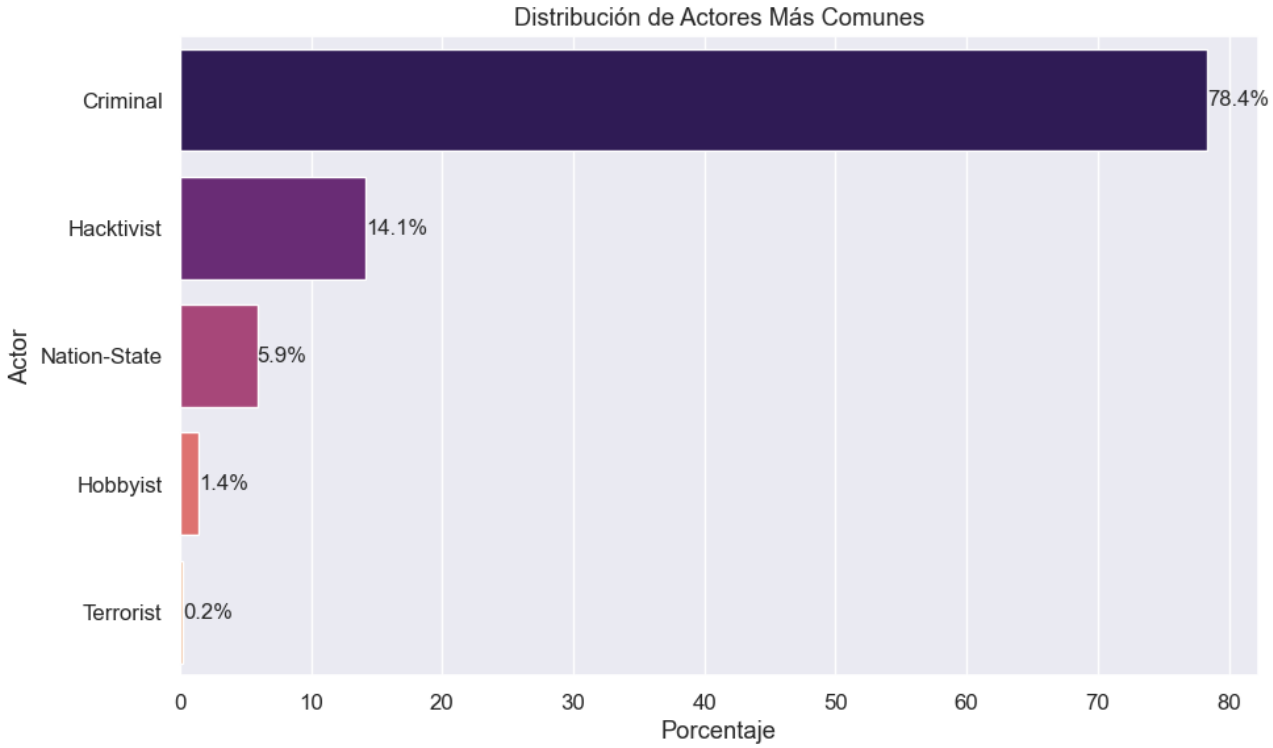
- Las categorías con un número bajo de eventos, como "Personal Attack" y "Sabotage", pueden no ser prioridades principales para los atacantes o pueden tener mejores medidas de protección.

4. Interés en Categorías Específicas :

- Las categorías "Financial" y "Protest" destacan por el número de eventos, lo que sugiere un alto interés por parte de los atacantes en estas áreas. Puede ser importante investigar más a fondo para entender las razones detrás de esta alta incidencia.

Conclusiones

El gráfico proporciona una visión clara de cómo se distribuyen los eventos entre diferentes organizaciones. La predominancia de ciertos tipos de eventos en categorías específicas puede ayudar a identificar áreas que requieren una mayor atención y recursos para mejorar la seguridad y prevenir futuros ataques.



1. Predominancia de Actores Criminales :

- Criminal : Con un 78.4%, los actores criminales son, de lejos, los más comunes en las actividades analizadas. Esto sugiere que las actividades delictivas dominan el panorama, lo

cual es una tendencia significativa y preocupante.

2. Presencia de Hacktivistas :

- Hacktivist : Los hacktivistas representan un 14.1% del total, lo cual es considerablemente menor que los actores criminales, pero aún significativo. Este grupo suele estar motivado por causas políticas o sociales y puede tener un impacto considerable.

3. Actores de Estado-Nación :

- Nation-State : Con un 5.9%, los actores de estado-nación representan una fracción menor, pero no insignificante. Estos actores suelen estar involucrados en actividades de espionaje y ciberataques estratégicos.

4. Hobbyistas :

- Hobbyist : Los hobbyistas constituyen solo el 1.4% del total. Este grupo incluye individuos que realizan actividades cibernéticas por curiosidad o como pasatiempo.

5. Terroristas :

- Terrorist : Con un 0.2%, los actores terroristas son los menos comunes en el contexto analizado. Aunque su proporción es baja, sus actividades pueden tener consecuencias graves.

Interpretación

1. Dominios de los Actores Criminales :

- La abrumadora mayoría de actores criminales sugiere que la actividad delictiva cibernética es la amenaza más significativa en el contexto analizado. Esto puede incluir delitos como el fraude, el robo de datos, y otras formas de cibercrimen.

2. Diversidad de Motivos :

- La presencia de hacktivistas y actores de estado-nación muestra que no todos los ciberataques están motivados por ganancias financieras. Los hacktivistas persiguen objetivos ideológicos, mientras que los actores de estado-nación pueden estar interesados

en el espionaje y la ventaja estratégica.

3. Implicaciones para la Seguridad :

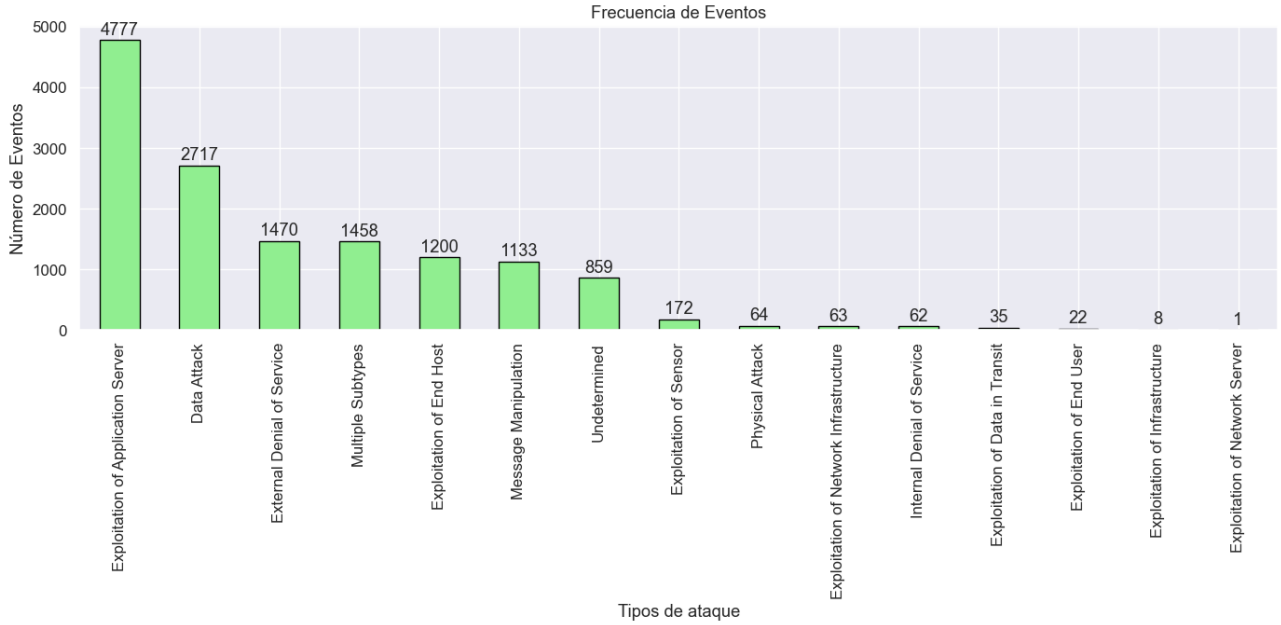
- La diversidad de actores implica que las medidas de seguridad cibernética deben ser amplias y adaptarse a diferentes tipos de amenazas. Las estrategias de defensa deben considerar tanto los ataques criminales como los motivados políticamente o estratégicamente.

4. Preocupaciones de Seguridad :

- Aunque los hobbyistas y terroristas representan una pequeña fracción, no deben ser ignorados. Los hobbyistas pueden descubrir vulnerabilidades que luego pueden ser explotadas por actores más peligrosos, y las actividades terroristas, aunque raras, pueden tener impactos severos.

Conclusión

El gráfico proporciona una visión clara de cómo se distribuyen los diferentes tipos de actores en las actividades analizadas. La predominancia de actores criminales es una señal de alerta que debe ser abordada con urgencia. Al mismo tiempo, la diversidad de otros actores destaca la necesidad de una estrategia de ciberseguridad multifacética y robusta.



1. Exploitation of Application Server :

- Con 4777 eventos, este tipo de ataque es el más frecuente.
- Los servidores de aplicaciones parecen ser un objetivo preferido para los atacantes, posiblemente debido a las vulnerabilidades explotables y la importancia crítica de estos servidores en las infraestructuras tecnológicas.

2. Data Attack :

- Con 2717 eventos, los ataques a datos son la segunda categoría más común.
- Los datos son uno de los activos más valiosos en la era digital, lo que hace que los ataques dirigidos a ellos sean altamente prioritarios para los delincuentes cibernéticos.

3. External Denial of Service (DDoS) :

- Con 1470 eventos, los ataques de denegación de servicio externos son bastante comunes.
- Estos ataques buscan interrumpir el acceso a servicios o redes, causando interrupciones significativas para las organizaciones afectadas.

4. Multiple Subtypes :

- Con 1458 eventos, esta categoría incluye ataques que pueden tener múltiples subtipos o combinaciones de técnicas.
- La diversidad de ataques en esta categoría indica que los atacantes pueden ser creativos y emplear múltiples métodos para comprometer sus objetivos.

5. Exploitation of End Host :

- Con 1200 eventos, los ataques dirigidos a los hosts finales también son frecuentes.
- Los dispositivos finales, como computadoras de escritorio, portátiles y móviles, pueden ser puntos de entrada vulnerables para los atacantes.

6. Message Manipulation :

- Con 1133 eventos, la manipulación de mensajes es un tipo significativo de ataque.
- Este tipo de ataque puede involucrar la interceptación y alteración de mensajes en tránsito, comprometiendo la integridad y confidencialidad de la comunicación.

7. Undetermined :

- Con 859 eventos, hay una categoría de ataques cuyo tipo no se ha determinado.
- Estos eventos subrayan la importancia de una investigación continua para identificar y clasificar correctamente los tipos de ataques.

8. Exploitation of Sensor :

- Con 172 eventos, los ataques a sensores son menos comunes pero todavía relevantes.
- Los sensores pueden ser componentes críticos en sistemas industriales y de IoT, y su compromiso puede tener consecuencias graves.

9. Physical Attack :

- Con 64 eventos, los ataques físicos son relativamente raros.
- Estos ataques pueden involucrar la manipulación física de dispositivos o infraestructuras y requieren acceso directo.

10. Exploitation of Network Infrastructure :

- Con 63 eventos, los ataques a la infraestructura de red son poco comunes.
- Sin embargo, comprometer la infraestructura de red puede tener un impacto significativo en las operaciones de una organización.

11. Internal Denial of Service :

- Con 62 eventos, los ataques de denegación de servicio internos son poco frecuentes.
- Estos ataques pueden originarse desde dentro de la organización, lo que sugiere la necesidad de monitoreo interno.

12. Exploitation of Data in Transit :

- Con 35 eventos, los ataques a los datos en tránsito son raros pero pueden comprometer la seguridad de la información en movimiento.
- Garantizar la seguridad de los datos en tránsito es crucial para mantener la confidencialidad y la integridad.

13. Exploitation of End User :

- Con 22 eventos, los ataques dirigidos a los usuarios finales son poco comunes en

comparación con otras categorías.

- Sin embargo, los usuarios finales son a menudo el eslabón más débil en la cadena de seguridad, y educarlos es esencial.

14. Exploitation of Infrastructure :

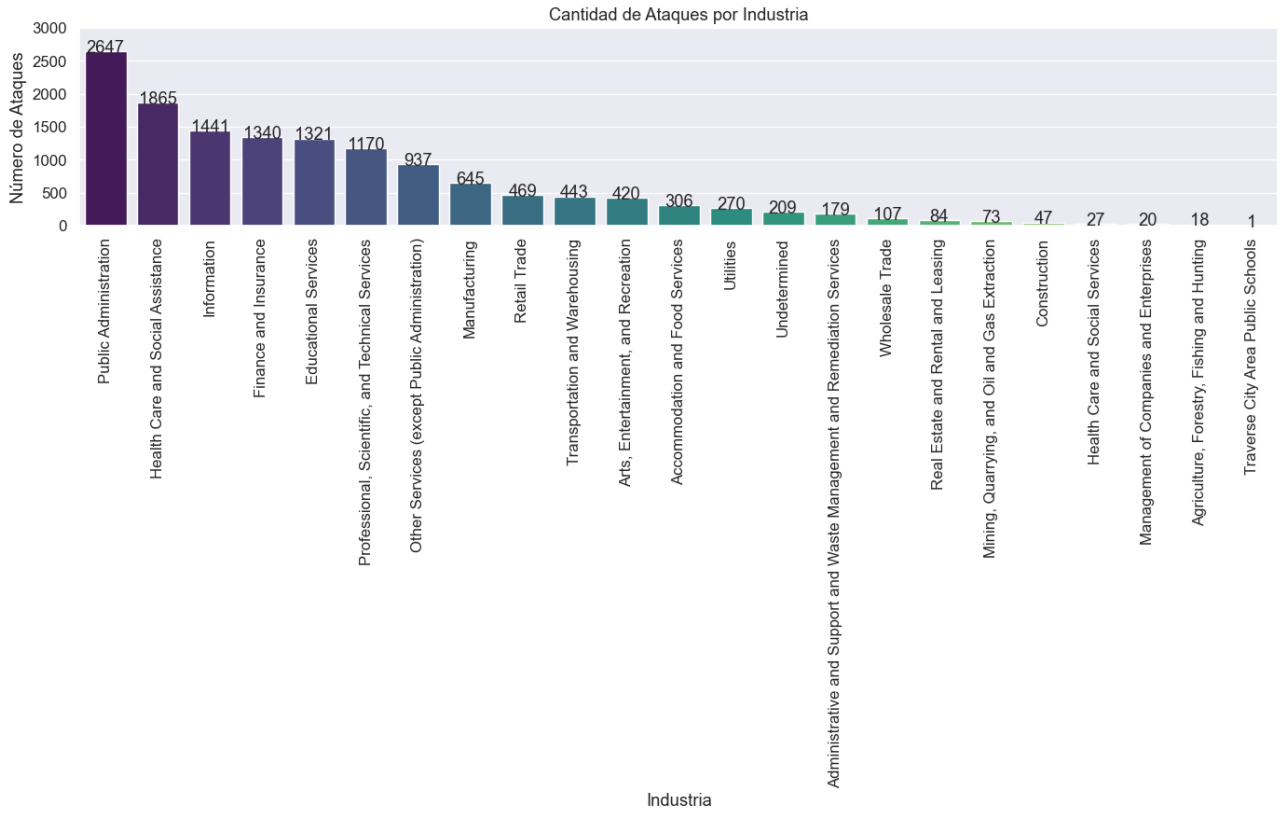
- Con 8 eventos, los ataques a la infraestructura son muy raros.
- Estos ataques pueden implicar la explotación de componentes de infraestructura crítica y requieren un alto nivel de sofisticación.

15. Exploitation of Network Server :

- Con solo 1 evento, los ataques a servidores de red son extremadamente raros en este conjunto de datos.
- La baja frecuencia puede deberse a la efectividad de las medidas de seguridad en torno a estos servidores o al tamaño del conjunto de datos.

Conclusión

Este gráfico proporciona una visión clara de la frecuencia de diferentes tipos de ataques, destacando cuáles son los más comunes y, por lo tanto, áreas donde las medidas de seguridad pueden necesitar fortalecerse.



1. Administración Pública :

Número de Ataques : 2647

La Administración Pública es la industria más afectada con la mayor cantidad de ataques. Esto puede deberse a la cantidad de datos sensibles manejados y la importancia de las infraestructuras gubernamentales.

2. Salud y Asistencia Social :

Número de Ataques : 1865

La industria de Salud y Asistencia Social también es altamente atacada, probablemente debido a la valiosa información de salud personal y la creciente digitalización de los registros médicos.

3. Información :

Número de Ataques : 1441

La industria de Información es un objetivo frecuente debido a la cantidad de datos valiosos y confidenciales que maneja.

4. Finanzas y Seguros :

Número de Ataques : 1340

La industria financiera es un blanco atractivo para los atacantes debido a los datos financieros sensibles y las posibles recompensas económicas.

5. Servicios Educativos :

Número de Ataques : 1321

Las instituciones educativas manejan datos personales y de investigación, lo que las hace vulnerables a los ataques.

6. Servicios Profesionales, Científicos y Técnicos :

Número de Ataques : 1170

Esta categoría incluye empresas que manejan propiedad intelectual y datos técnicos, lo que las hace atractivas para los atacantes.

7. Otros Servicios (excepto Administración Pública) :

Número de Ataques : 937

Aunque no especificados, otros servicios también son blancos de ataques debido a la diversidad de datos manejados.

8. Manufactura :

Número de Ataques : 645

La manufactura puede ser objetivo de ataques debido a la importancia de las cadenas de suministro y la propiedad intelectual.

9. Comercio al por Menor :

Número de Ataques : 469

El comercio minorista maneja información de transacciones y clientes, lo que lo hace vulnerable.

10. Transporte y Almacenamiento :

Número de Ataques : 443

La logística y el transporte son críticos, y los ataques pueden interrumpir las operaciones significativamente.

11. Artes, Entretenimiento y Recreación :

Número de Ataques : 420

Estos sectores también manejan datos de clientes y transacciones.

12. Alojamiento y Servicios de Alimentos :

Número de Ataques : 306

Los hoteles y restaurantes manejan datos de clientes que pueden ser objetivos atractivos.

13. Servicios Públicos :

Número de Ataques : 270

La infraestructura crítica de servicios públicos es vital y, por lo tanto, vulnerable a ataques.

14. Indeterminado :

Número de Ataques : 209

Eventos que no se han clasificado claramente, lo que sugiere la necesidad de más investigación.

15. Servicios Administrativos y de Apoyo y Gestión de Residuos y Servicios de Remediación :

Número de Ataques : 209

Estos servicios son esenciales y pueden manejar datos críticos.

16. Comercio al por Mayor :

Número de Ataques : 179

El comercio mayorista puede ser un objetivo debido a las transacciones y datos de clientes.

17. Bienes Raíces y Alquiler y Arrendamiento :

Número de Ataques : 107

Las transacciones y datos de clientes en bienes raíces son vulnerables.

18. Minería, Extracción de Petróleo y Gas :

Número de Ataques : 84

La minería y extracción de recursos naturales es vital para la economía y puede ser blanco de ataques.

19. Construcción :

Número de Ataques : 73

Los proyectos de construcción manejan datos críticos y pueden ser objetivos.

20. Servicios de Salud y Asistencia Social :

Número de Ataques : 47

Aunque una categoría separada, también es vulnerable debido a los datos de salud.

21. Gestión de Empresas y Compañías :

Número de Ataques : 27

Las empresas de gestión manejan datos estratégicos y financieros.

22. Agricultura, Silvicultura, Pesca y Caza :

Número de Ataques : 20

Los datos de producción y comercio agrícola son valiosos.

23. Traverse City Area Public Schools :

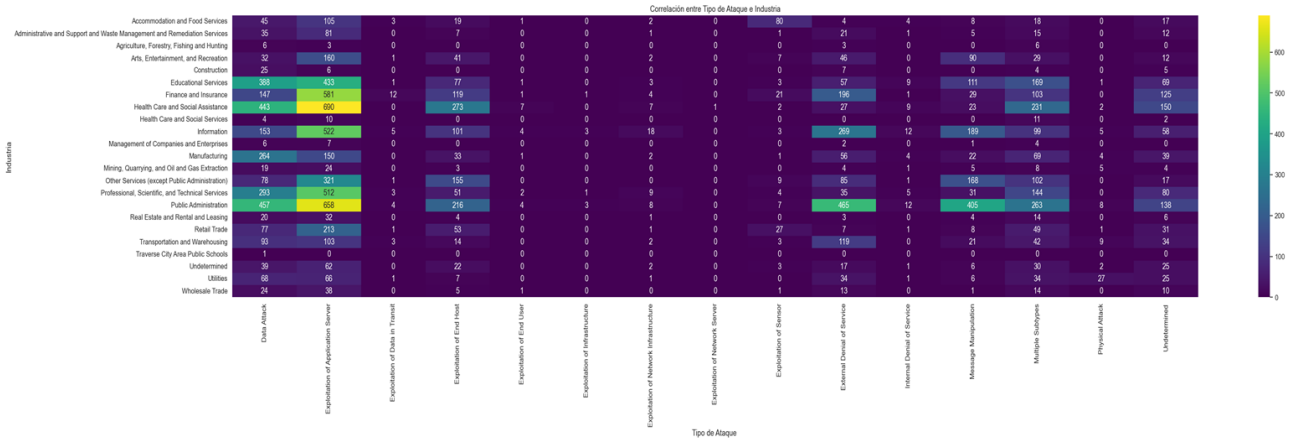
Número de Ataques : 18

Aunque específico, las escuelas públicas manejan datos de estudiantes y personal.

Conclusión

El gráfico proporciona una visión clara de cómo se distribuyen los ataques entre diferentes industrias, destacando cuáles sectores son más y menos afectados. La Administración Pública, Salud y Asistencia Social, Información, y Finanzas y Seguros son los más atacados, lo que refleja la valiosa información y la infraestructura crítica que manejan.

Este análisis puede ayudar a priorizar las medidas de seguridad cibernética y enfocar los esfuerzos en proteger las industrias más vulnerables.



Tipos de Ataques Frecuentes :

- **Exploitation of Application Server** : Este tipo de ataque es predominante en varias industrias, especialmente en Administración Pública, Finanzas y Seguros, y Servicios Profesionales, Científicos y Técnicos. Esto sugiere que los servidores de aplicaciones son un objetivo principal debido a sus vulnerabilidades y la importancia de los datos que manejan.
- Data Attack : Los ataques a datos son frecuentes en industrias como Administración Pública, Finanzas y Seguros, y Salud y Asistencia Social. La alta frecuencia de estos ataques refleja el valor crítico de los datos en estas industrias.

Variabilidad entre Industrias :

- **Administración Pública** : Muestra una alta frecuencia de varios tipos de ataques, incluidos los ataques a servidores de aplicaciones y datos. Esto puede deberse a la cantidad de datos sensibles y la infraestructura crítica que maneja esta industria.

- **Finanzas y Seguros :** Además de los ataques a servidores de aplicaciones y datos, esta industria también enfrenta una alta incidencia de ataques de denegación de servicio (DDoS). La estabilidad y disponibilidad de los servicios financieros son cruciales, lo que hace que estos ataques sean especialmente disruptivos.
- **Salud y Asistencia Social :** Los ataques a datos son comunes, destacando la importancia de proteger la información de salud personal. También hay una notable incidencia de ataques de explotación del usuario final (EUI).
- **Información :** Esta industria enfrenta una variedad de ataques, incluidos ataques a datos y servidores de aplicaciones, lo que refleja la importancia de los datos manejados.
- **Servicios Profesionales, Científicos y Técnicos :** Similar a la industria de Información, esta categoría enfrenta múltiples tipos de ataques debido a la naturaleza sensible de la información y los servicios que proporcionan.

Menor Frecuencia de Ataques en Algunas Industrias :

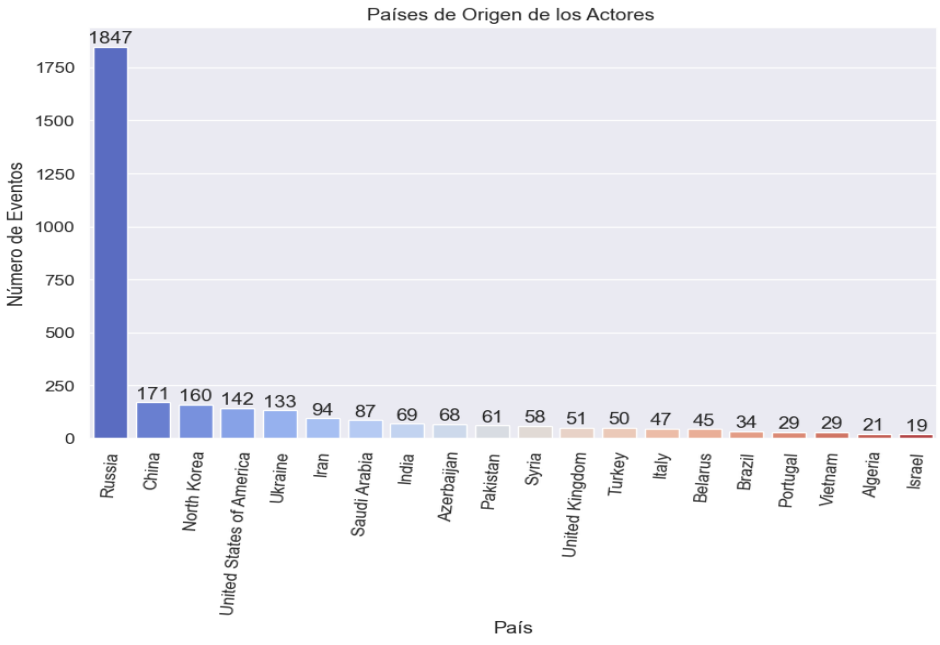
- **Agricultura, Silvicultura, Pesca y Caza :** Esta industria muestra una frecuencia baja de ataques en general, lo que puede deberse a la percepción de un menor valor de los datos o menor digitalización.
- **Construcción :** También presenta una baja frecuencia de ataques, posiblemente debido a una menor dependencia de sistemas digitales críticos en comparación con otras industrias.
- **Artes, Entretenimiento y Recreación :** Similar a las industrias anteriores, enfrenta una frecuencia relativamente baja de ataques.

Tipos de Ataques Menos Frecuentes :

- **Exploitation of End User :** Este tipo de ataque es relativamente raro en comparación con otros, aunque sigue siendo relevante en industrias como la Salud y Asistencia Social.
- **Physical Attack :** Los ataques físicos son los menos frecuentes, lo que sugiere que los atacantes prefieren métodos digitales que pueden ejecutarse de manera remota y anónima.
- **Exploitation of Data in Transit :** Similarmente, los ataques a datos en tránsito son menos comunes, aunque críticos, especialmente para comunicaciones seguras.

Conclusión

El mapa de calor proporciona una visión detallada de cómo se distribuyen los diferentes tipos de ciberataques entre diversas industrias. Las observaciones clave incluyen:
- Predominancia de ciertos tipos de ataques en industrias específicas, como los ataques a servidores de aplicaciones y datos.
- Variabilidad en la frecuencia de ataques entre diferentes industrias, lo que refleja las diferentes exposiciones y vulnerabilidades.
- Necesidad de medidas de seguridad específicas adaptadas a cada industria y tipo de ataque para mejorar la ciberseguridad y proteger datos sensibles y sistemas críticos.



Interpretación de los Datos

Alta Actividad en Rusia y China :

- La predominancia de actores rusos y chinos sugiere una alta actividad cibernética en estos países, probablemente impulsada por motivos económicos, políticos y de espionaje.

Diversidad de Orígenes :

- Aunque Rusia y China lideran en términos de número de eventos, hay una diversidad de países involucrados en actividades cibernéticas, lo que refleja la naturaleza global de las amenazas cibernéticas.

Estados Financiados y Cibercrimen :

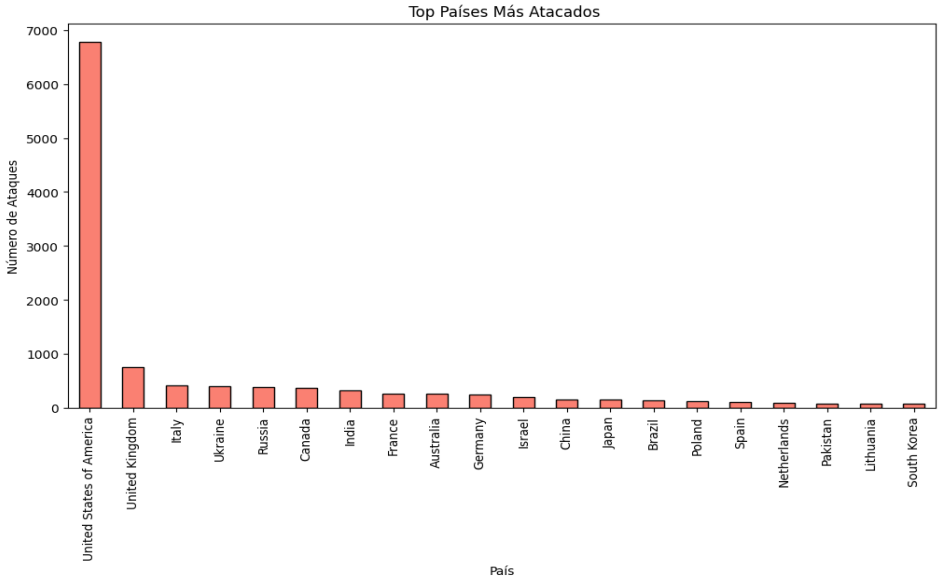
- La presencia de actores de Corea del Norte e Irán indica que algunos estados están financiando y apoyando actividades cibernéticas como parte de sus estrategias de seguridad nacional.

Países con Menor Actividad :

- Países como Brasil, Portugal, Vietnam, y Argelia muestran una menor cantidad de eventos, lo que puede deberse a una menor actividad cibernética o a diferencias en la capacidad de detección y reporte.

Conclusión

El gráfico proporciona una visión clara de la distribución geográfica de los actores involucrados en eventos cibernéticos. La alta incidencia en países como Rusia y China destaca la importancia de entender las motivaciones y tácticas de estos actores para mejorar las defensas cibernéticas. La diversidad de países involucrados subraya la necesidad de una colaboración internacional para abordar las amenazas cibernéticas de manera efectiva.



1. Estados Unidos de América (EE.UU.) :

- Número de Ataques : Aproximadamente 7000

EE.UU. es, con diferencia, el país más atacado. Esto puede deberse a su posición como una de las economías más grandes y tecnológicamente avanzadas del mundo, lo que lo convierte en un objetivo atractivo para los atacantes cibernéticos.

2. Reino Unido :

- Número de Ataques : Mucho menor que EE.UU., pero sigue siendo significativo.

El Reino Unido también es un objetivo importante, probablemente debido a su influencia económica y política global.

3. Italia, Ucrania y Rusia :

- Número de Ataques : Menores que los dos primeros, pero aún notables.

Estos países tienen una actividad cibernética significativa, posiblemente debido a sus infraestructuras críticas y situación geopolítica.

4. Canadá e India :

- Número de Ataques : Moderado.

Canadá y India son objetivos relevantes debido a su crecimiento económico y la digitalización creciente de sus economías.

5. Francia, Australia y Alemania :

- Número de Ataques : Relativamente menores, pero importantes.

Estos países tienen economías avanzadas y son actores clave en la escena mundial, lo que los hace vulnerables a los ataques cibernéticos.

6. Israel y China :

- Número de Ataques : Menores en comparación con otros, pero no insignificantes.

Israel es conocido por su alta tecnología y defensa cibernética, lo que puede atraer ataques. China, siendo una gran potencia económica, también enfrenta un número significativo de ataques.

7. Otros Países :

- Japón, Brasil, Polonia, España, Países Bajos, Pakistán, Lituania y Corea del Sur : Tienen un menor número de ataques en comparación con los países anteriores, pero aún están en la lista.

Estos países son importantes económicamente o estratégicamente y, por lo tanto, son vulnerables a los ataques cibernéticos.

Interpretación de los Datos

Predominancia de EE.UU. :

- El número extremadamente alto de ataques en EE.UU. subraya la necesidad de medidas de ciberseguridad robustas y continuas en este país. Su liderazgo tecnológico y económico lo convierte en un objetivo prioritario para diversos actores cibernéticos.

Alta Actividad en Países Europeos :

- Varios países europeos, incluido el Reino Unido, Italia, Ucrania y Rusia, muestran una actividad significativa de ataques cibernéticos. Esto puede estar relacionado con su infraestructura tecnológica avanzada y la situación geopolítica en Europa.

Diversidad Geográfica de los Ataques :

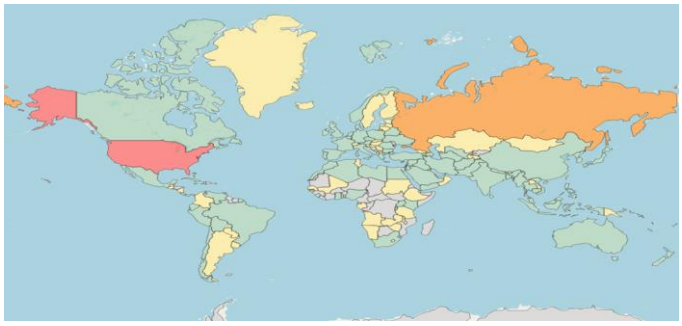
- La presencia de países de diferentes regiones (América del Norte, Europa, Asia y Oceanía) en la lista indica que los ataques cibernéticos son un problema global que afecta a economías avanzadas y en desarrollo por igual.

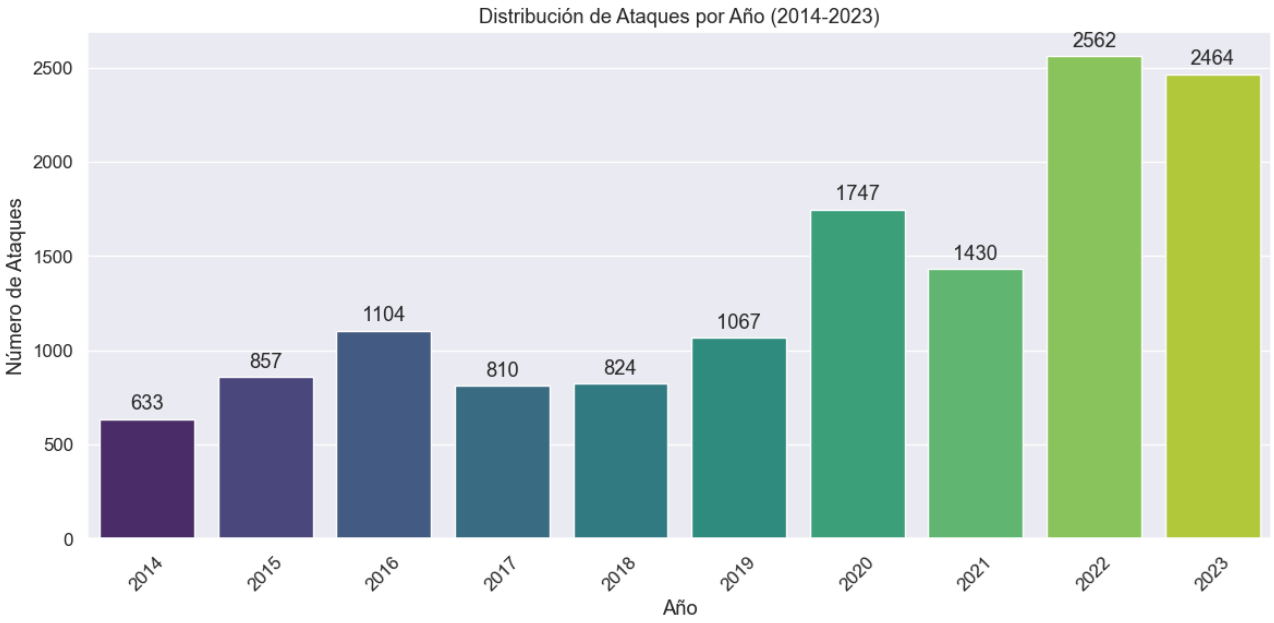
Implicaciones para la Seguridad :

- La variabilidad en el número de ataques entre países sugiere que las estrategias de ciberseguridad deben ser personalizadas y adaptadas a las amenazas específicas que enfrenta cada país.

Conclusión

El gráfico proporciona una visión clara de la distribución de los ataques cibernéticos entre diferentes países. La alta incidencia de ataques en EE.UU. y otros países clave destaca la importancia de mejorar y mantener las medidas de ciberseguridad a nivel global. Las observaciones de este análisis pueden ayudar a priorizar los esfuerzos de ciberseguridad y dirigir recursos hacia las áreas más vulnerables.





Incremento General de Ataques :

- Tendencia General : A lo largo de los años, se observa una tendencia al alza en el número de ataques cibernéticos. Esto indica que las amenazas cibernéticas están aumentando, lo que puede deberse a varios factores, como la digitalización creciente y la sofisticación de las técnicas de los atacantes.

Años con Mayor Incidencia de Ataques :

- 2022 : Con 2562 ataques, el año 2022 tiene la mayor cantidad de ataques registrados. Esto podría estar relacionado con eventos globales, pandemias o cambios en la política de seguridad cibernética.
- 2023 : Aunque ligeramente inferior al año anterior, con 2464 ataques, el año 2023 sigue mostrando una alta incidencia de ataques.

Años con Aumentos Significativos :

- 2020 : Se observa un aumento significativo en el número de ataques, alcanzando 1747. Este incremento puede estar relacionado con la pandemia de COVID-19 y el aumento del trabajo remoto, que expuso nuevas vulnerabilidades.
- 2021 : Con 1430 ataques, sigue la tendencia al alza en la actividad cibernética.

Fluctuaciones Anteriores :

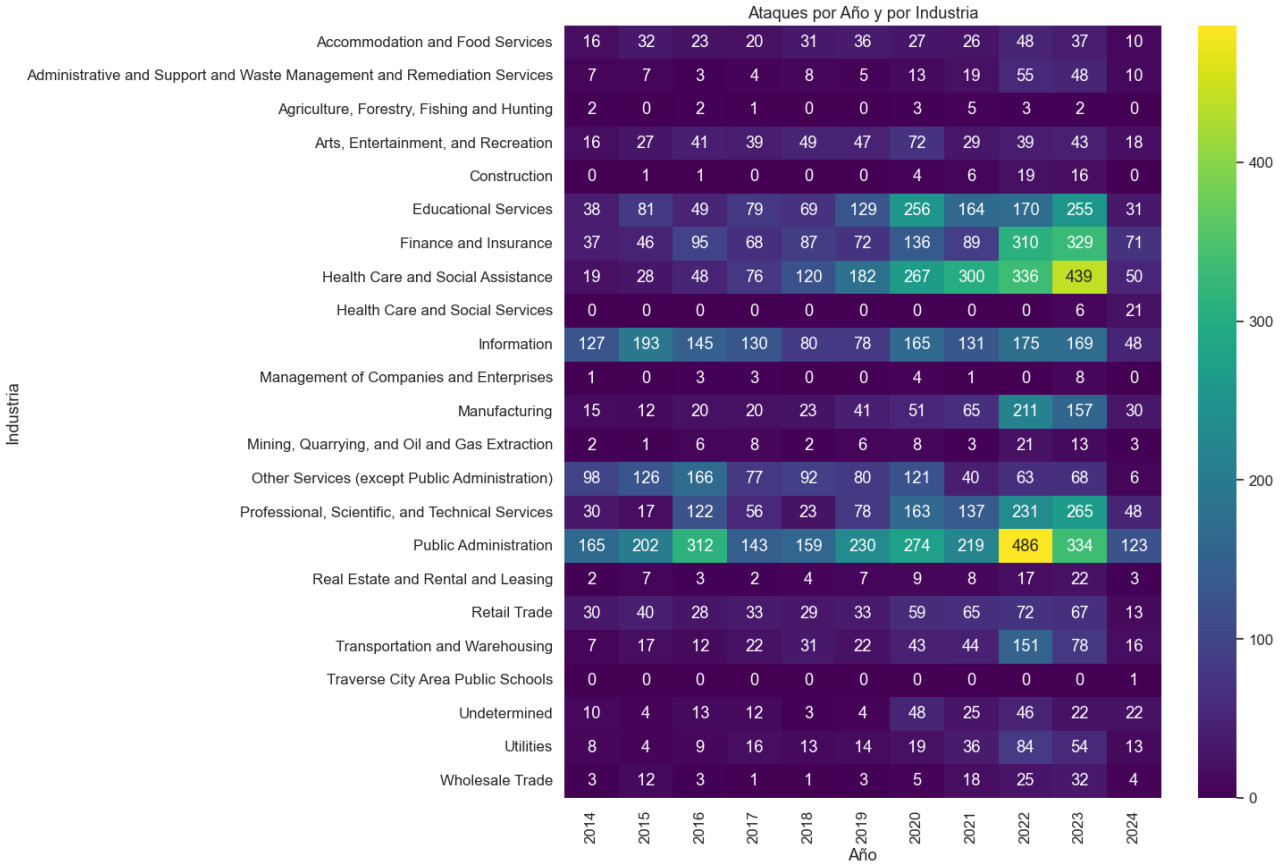
- 2014 a 2019 : Aunque hay fluctuaciones, se observa una tendencia creciente en general. Los años 2016 (1104 ataques) y 2019 (1067 ataques) destacan por tener un número significativo de ataques, mientras que 2017 (810 ataques) y 2018 (824 ataques) muestran una ligera disminución en comparación.

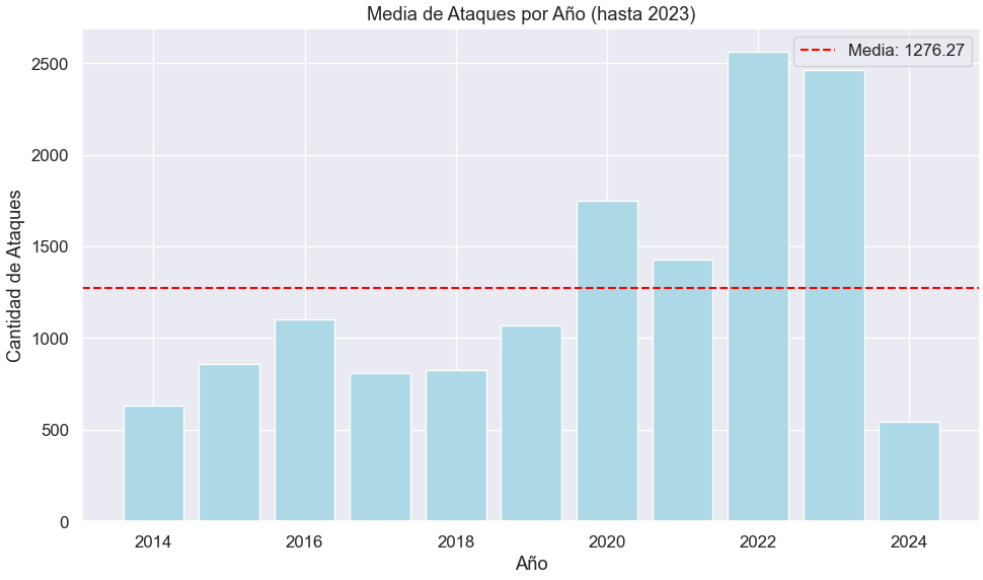
Interpretación de Datos :

- Factores Contribuyentes : Los aumentos en el número de ataques pueden ser atribuidos a varios factores, incluidos avances tecnológicos, aumento en el uso de dispositivos conectados, y un entorno global en constante cambio. Las estrategias de los atacantes también han evolucionado, y las medidas de seguridad pueden no haber seguido el mismo ritmo.
- Importancia de la Vigilancia : Los datos subrayan la importancia de la vigilancia continua y la actualización de las medidas de seguridad cibernética. Las organizaciones deben permanecer alertas y adaptarse a las nuevas amenazas.

Conclusión

El gráfico destaca un incremento en los ataques cibernéticos a lo largo de la última década, con picos notables en 2022 y 2023. Este aumento enfatiza la necesidad de fortalecer las defensas cibernéticas y de estar preparados para enfrentar amenazas cada vez más sofisticadas. La interpretación de estos datos puede ayudar a guiar las estrategias de ciberseguridad y enfocar los esfuerzos en las áreas más vulnerables


Ataques por Año y por Industria
Industria
Accommodation and Food Services 16 32 23 20 31 36 27 26 48 37 10
Administrative and Support and Waste Management and Remediation Services 7 7 3 4 8 5 13 19 55 48 10
Agriculture, Forestry, Fishing and Hunting 2 0 2 1 0 0 3 5 3 2 0
Arts, Entertainment, and Recreation 16 27 41 39 49 47 72 29 39 43 18
Construction 0 1 1 0 0 0 4 6 19 16 0
Educational Services 38 81 49 79 69 129 256 164 170 255 31
Finance and Insurance 37 46 95 68 87 72 136 89 310 329 71
Health Care and Social Assistance 19 28 48 76 120 182 267 300 336 439 50
Health Care and Social Services 0 0 0 0 0 0 0 0 0 6 21
Information 127 193 145 130 80 78 165 131 175 169 48
Management of Companies and Enterprises 1 0 3 3 0 0 4 1 0 8 0
Manufacturing 15 12 20 20 23 41 51 65 211 157 30
Mining, Quarrying, and Oil and Gas Extraction 2 1 6 8 2 6 8 3 21 13 3
Other Services (except Public Administration) 98 126 166 77 92 80 121 40 63 68 6
Professional, Scientific, and Technical Services 30 17 122 56 23 78 163 137 231 265 48
Public Administration 165 202 312 143 159 230 274 219 486 334 123
Real Estate and Rental and Leasing 2 7 3 2 4 7 9 8 17 22 3
Retail Trade 30 40 28 33 29 33 59 65 72 67 13
Transportation and Warehousing 7 17 12 22 31 22 43 44 151 78 16
Traverse City Area Public Schools 0 0 0 0 0 0 0 0 0 0 1
Undetermined 10 4 13 12 3 4 48 25 46 22 22
Utilities 8 4 9 16 13 14 19 36 84 54 13
Wholesale Trade 3 12 3 1 1 3 5 18 25 32 4
2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024
Año
400
300
200
100
0


Media de Ataques por Año (hasta 2023)
Media: 1276.27
Cantidad de Ataques
2500
2000
1500
1000
500
0
2014
2016
2018
2020
2022
2024
Año

El mapa de calor muestra la distribución de ataques cibernéticos a través de varias industrias y a lo largo de los años, desde 2014 hasta 2024. Los colores más claros indican una mayor cantidad de ataques, mientras que los colores más oscuros representan una menor cantidad de ataques.

1. Tendencia General de Aumento :

- La mayoría de las industrias muestran un aumento en la frecuencia de ataques a lo largo del tiempo, especialmente en los años más recientes (2020-2024).
- Este aumento puede estar asociado con la creciente digitalización y el aumento de las amenazas cibernéticas globales.

2. Industrias Altamente Atacadas :

- Administración Pública : Esta industria muestra consistentemente altos niveles de ataques a lo largo de los años, con un notable aumento en los últimos años. La crítica naturaleza de los servicios públicos y la cantidad de datos sensibles pueden explicar esta tendencia.
- Salud y Asistencia Social : También muestra un aumento significativo en los ataques, especialmente en los años 2020-2022. La pandemia de COVID-19 puede haber exacerbado esta tendencia debido al aumento del valor de los datos de salud.
- Finanzas y Seguros : Este sector es constantemente atacado debido al valor financiero de los datos y las transacciones que maneja. Se observa un pico notable en 2023.

3. Picos Notables :

- 2022 y 2023 : Estos años muestran picos significativos en varias industrias, incluyendo Administración Pública, Finanzas y Seguros, y Servicios Profesionales, Científicos y Técnicos. Esto podría estar relacionado con eventos globales específicos o la evolución de las tácticas de los atacantes.

4. Industrias con Menores Ataques :

- Agricultura, Silvicultura, Pesca y Caza y Construcción : Estas industrias tienen consistentemente menos ataques en comparación con otras, lo que puede deberse a una menor dependencia de la tecnología y sistemas críticos.
- Artes, Entretenimiento y Recreación : Similarmente, esta industria muestra un menor

número de ataques a lo largo de los años.

5. Variabilidad entre Industrias :

- La frecuencia de ataques varía significativamente entre industrias, lo que refleja diferentes niveles de exposición y vulnerabilidades. Por ejemplo, las industrias que manejan información crítica y sensible, como Finanzas, Salud y Administración Pública, son más atacadas.

Interpretación de los Datos

1. Aumento de Ataques en Industrias Clave :

- Los datos subrayan la necesidad de reforzar las defensas cibernéticas en industrias críticas como Administración Pública, Salud, y Finanzas. Estas industrias manejan datos muy valiosos y son esenciales para el funcionamiento de la sociedad.

2. Impacto de Eventos Globales :

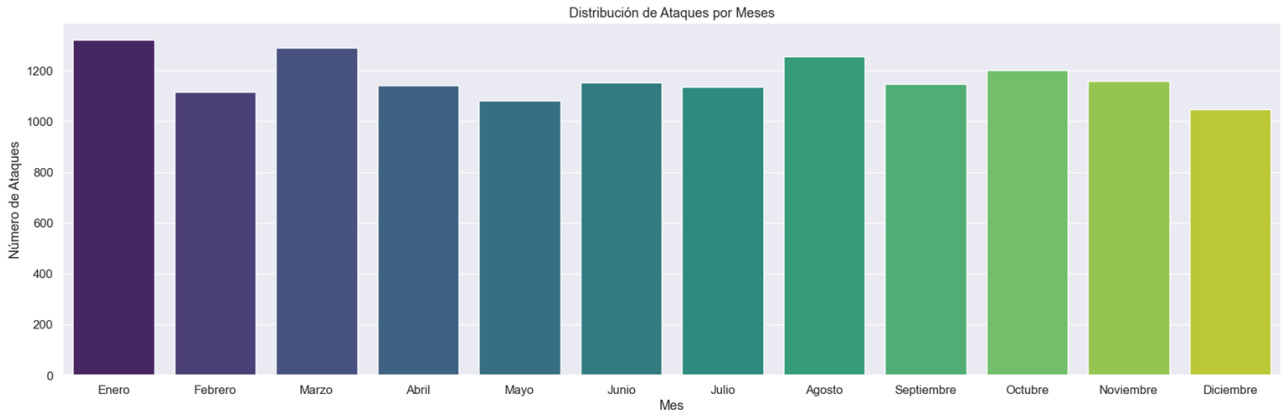
- Los picos en los años recientes, especialmente 2022 y 2023, pueden estar influenciados por eventos globales como la pandemia de COVID-19, que ha llevado a un aumento en las amenazas cibernéticas debido al trabajo remoto y la dependencia de la tecnología.

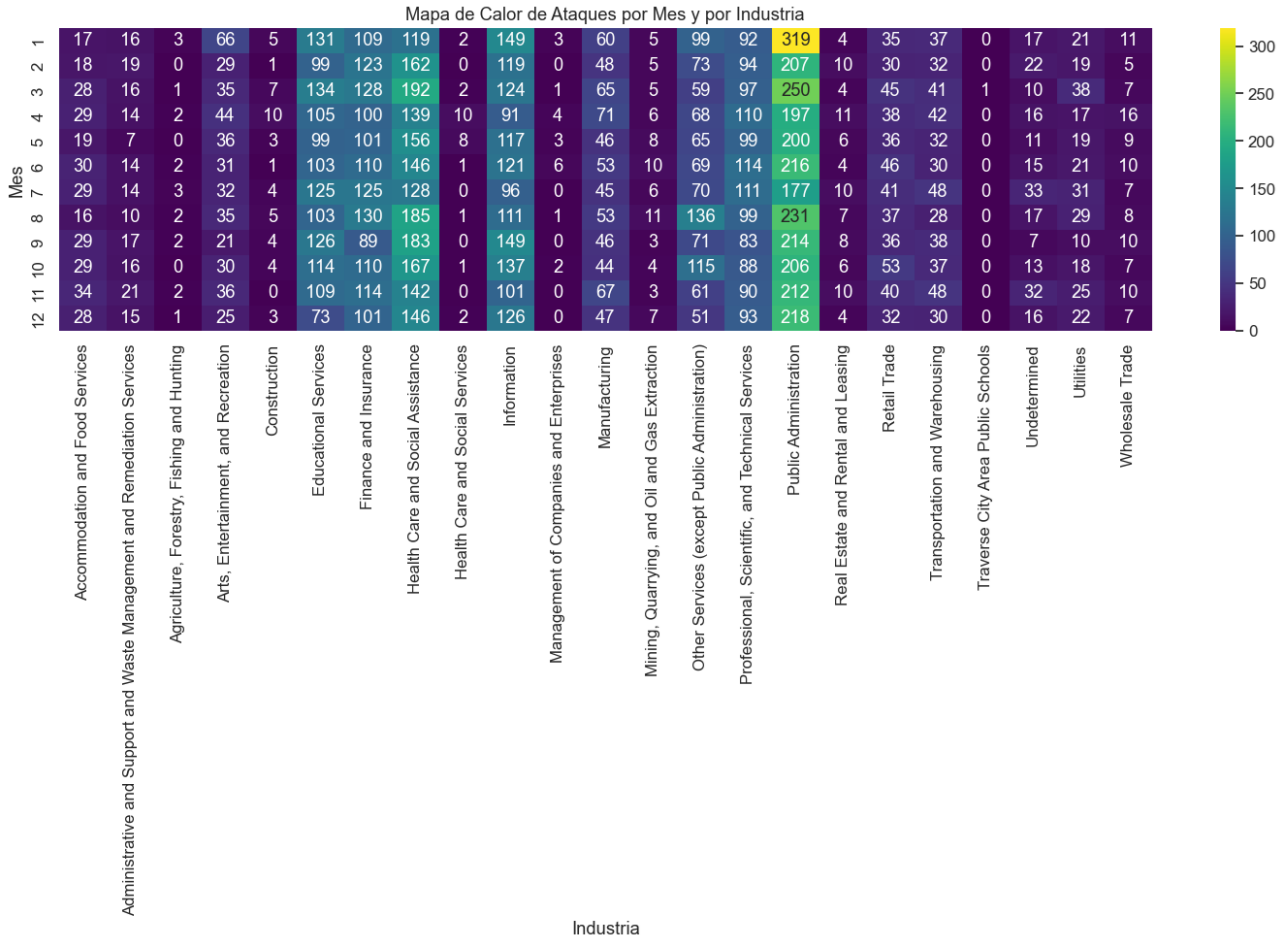
3. Necesidad de Estrategias Adaptadas :

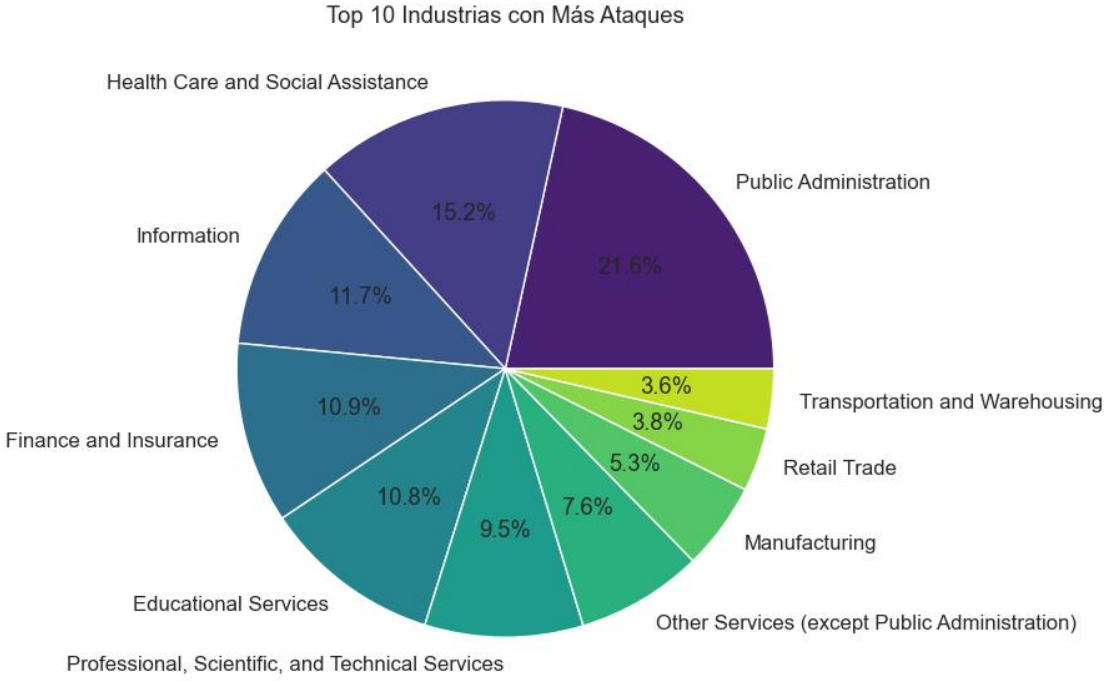
- Dada la variabilidad entre industrias, es crucial desarrollar estrategias de ciberseguridad adaptadas a las necesidades específicas de cada sector. Esto incluye la implementación de medidas preventivas, la capacitación del personal y la actualización continua de las tecnologías de seguridad.

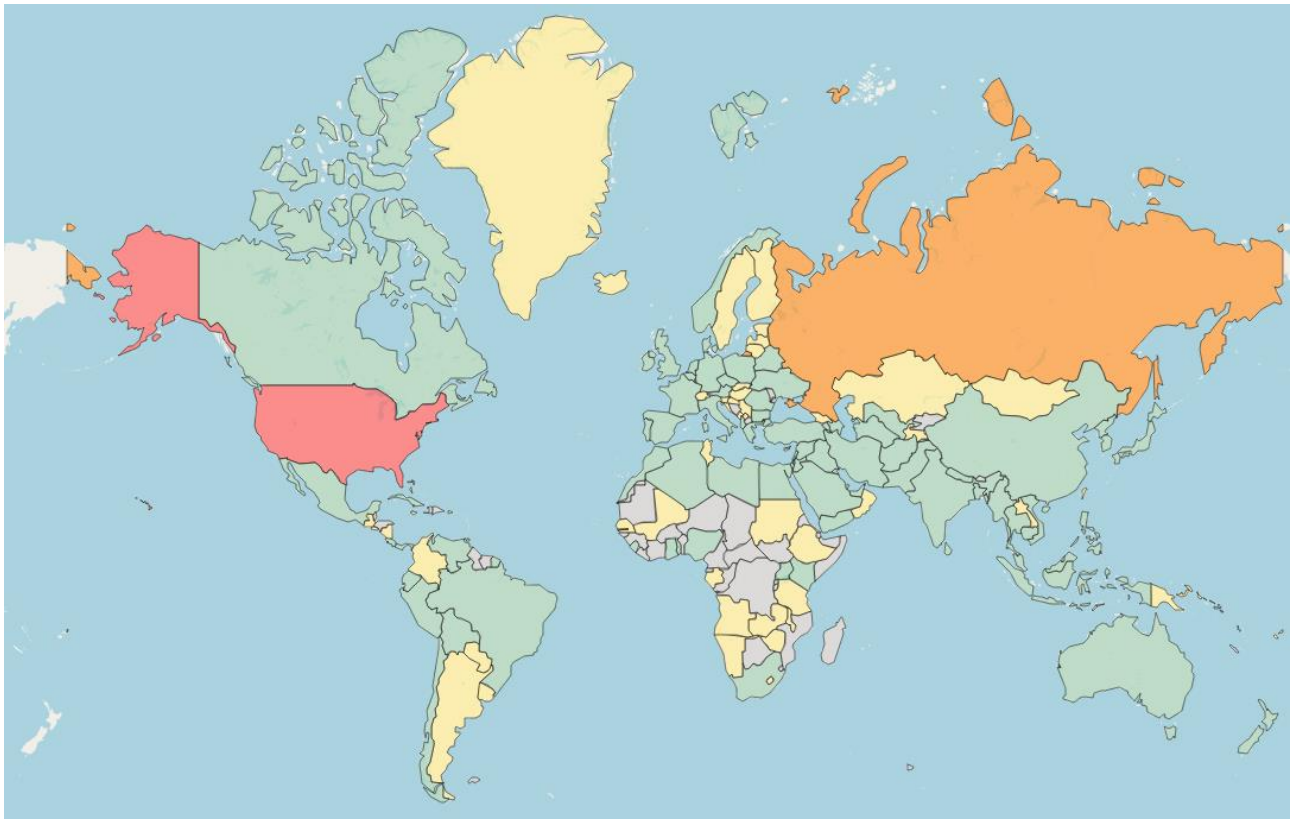
Conclusión

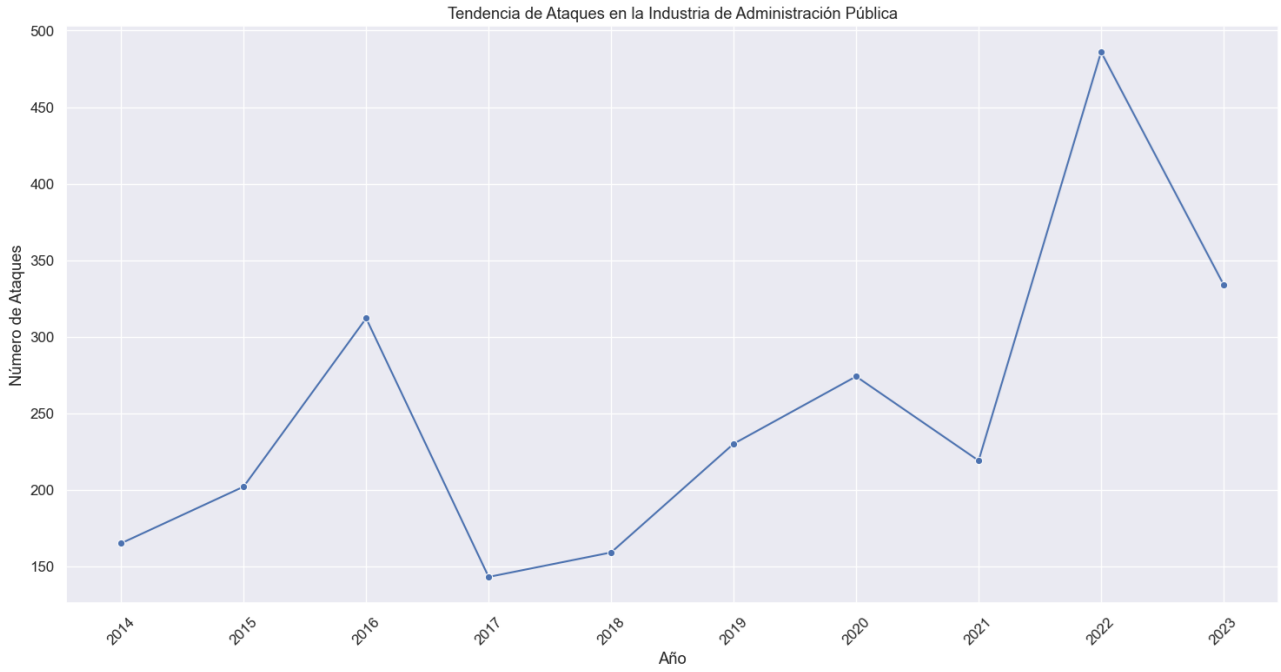
El mapa de calor proporciona una visión clara de cómo varían los ataques cibernéticos a lo largo del tiempo y entre diferentes industrias. Destaca la importancia de estar preparados y de fortalecer las defensas cibernéticas en las industrias más afectadas. La interpretación de estos datos puede ayudar a guiar las estrategias de ciberseguridad y priorizar los esfuerzos en las áreas más vulnerables.

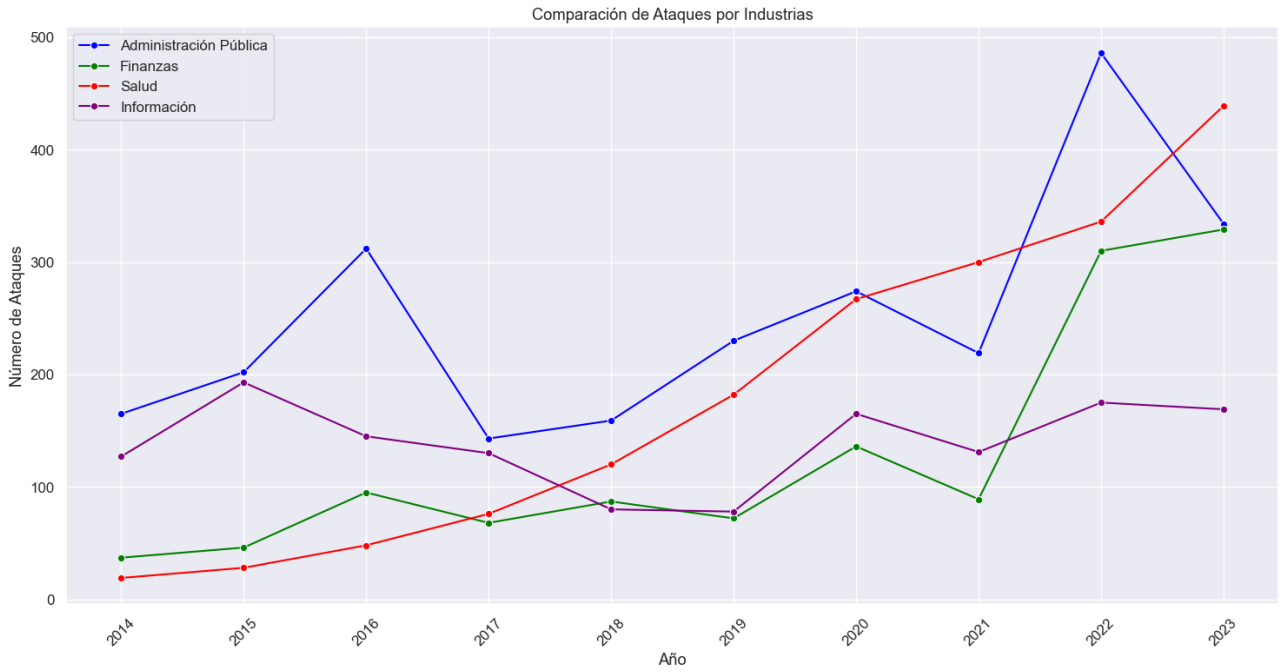

Distribución de Ataques por Meses
Número de Ataques
0
200
400
600
800
1000
1200
Enero
Febrero
Marzo
Abril
Mayo
Junio
Julio
Agosto
Septiembre
Octubre
Noviembre
Diciembre
Mes


Mapa de Calor de Ataques por Mes y por Industria
Mes
Industria
Accommodation and Food Services
Administrative and Support and Waste Management and Remediation Services
Agriculture, Forestry, Fishing and Hunting
Arts, Entertainment, and Recreation
Construction
Educational Services
Finance and Insurance
Health Care and Social Assistance
Health Care and Social Services
Information
Management of Companies and Enterprises
Manufacturing
Mining, Quarrying, and Oil and Gas Extraction
Other Services (except Public Administration)
Professional, Scientific, and Technical Services
Public Administration
Real Estate and Rental and Leasing
Retail Trade
Transportation and Warehousing
Traverse City Area Public Schools
Undetermined
Utilities
Wholesale Trade
1 17 16 3 66 5 131 109 119 2 149 3 60 5 99 92 319 4 35 37 0 17 21 11
2 18 19 0 29 1 99 123 162 0 119 0 48 5 73 94 207 10 30 32 0 22 19 5
3 28 16 1 35 7 134 128 192 2 124 1 65 5 59 97 250 4 45 41 1 10 38 7
4 29 14 2 44 10 105 100 139 10 91 4 71 6 68 110 197 11 38 42 0 16 17 16
5 19 7 0 36 3 99 101 156 8 117 3 46 8 65 99 200 6 36 32 0 11 19 9
6 30 14 2 31 1 103 110 146 1 121 6 53 10 69 114 216 4 46 30 0 15 21 10
7 29 14 3 32 4 125 125 128 0 96 0 45 6 70 111 177 10 41 48 0 33 31 7
8 16 10 2 35 5 103 130 185 1 111 1 53 11 136 99 231 7 37 28 0 17 29 8
9 29 17 2 21 4 126 89 183 0 149 0 46 3 71 83 214 8 36 38 0 7 10 10
10 29 16 0 30 4 114 110 167 1 137 2 44 4 115 88 206 6 53 37 0 13 18 7
11 34 21 2 36 0 109 114 142 0 101 0 67 3 61 90 212 10 40 48 0 32 25 10
12 28 15 1 25 3 73 101 146 2 126 0 47 7 51 93 218 4 32 30 0 16 22 7
300
250
200
150
100
50
0


Top 10 Industrias con Más Ataques
Health Care and Social Assistance
15.2%
Public Administration
21.6%
Information
11.7%
3.6%
Transportation and Warehousing
3.8%
Retail Trade
5.3%
Manufacturing
7.6%
Other Services (except Public Administration)
9.5%
Professional, Scientific, and Technical Services
10.8%
Educational Services
10.9%
Finance and Insurance




Tendencia de Ataques en la Industria de Administración Pública
Número de Ataques
500
450
400
350
300
250
200
150
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
Año



El gráfico de líneas compara el número de ataques en cuatro industrias: Administración Pública, Finanzas, Salud e Información, desde 2014 hasta 2023. Aquí están las observaciones y análisis basados en los datos presentados:

1. Administración Pública (Azul) :

- Tendencias : La Administración Pública muestra un aumento significativo en el número de ataques, especialmente notorio alrededor de los años 2016 y 2021.
- Comentario : La infraestructura crítica y la cantidad de datos sensibles gestionados por el sector público pueden hacerlo un objetivo atractivo para los atacantes. La fluctuación en los ataques sugiere posibles cambios en la política de ciberseguridad o eventos específicos que incrementaron la vulnerabilidad.

2. Finanzas (Verde) :

- Tendencias : La industria de Finanzas tiene una tendencia relativamente estable con algunos aumentos notables, destacando un pico en 2020.
- Comentario : Los datos financieros son extremadamente valiosos, lo que hace a esta industria un objetivo constante. El aumento en 2020 puede estar relacionado con el incremento de transacciones digitales y la adopción de nuevas tecnologías durante la pandemia de COVID-19.

3. Salud (Rojo) :

- Tendencias : La industria de Salud muestra un notable aumento en los ataques a partir de 2020.
- Comentario : La pandemia de COVID-19 probablemente ha incrementado la frecuencia de ataques en esta industria, ya que los datos de salud personal se volvieron especialmente valiosos. La digitalización y el uso de sistemas de salud electrónicos también contribuyen a esta tendencia.

4. Información (Púrpura) :
- Tendencias : La industria de Información muestra fluctuaciones en los ataques, con aumentos significativos en ciertos años, como 2021.
- Comentario : Los datos manejados por esta industria, como información de usuarios y propiedad intelectual, son altamente valorados por los atacantes. La variabilidad en los ataques puede reflejar incidentes específicos y mejoras en las medidas de seguridad.

Interpretación de los Datos

1. Factores Contribuyentes :
- Eventos Globales : La pandemia de COVID-19 ha tenido un impacto significativo en todas las industrias, aumentando la superficie de ataque debido al incremento del trabajo remoto y la digitalización de servicios.
- Infraestructura Crítica : Industrias como Administración Pública y Salud gestionan infraestructuras críticas y datos sensibles, lo que las hace objetivos prioritarios para los atacantes.

2. Necesidad de Medidas de Seguridad Robustas :
- Ciberseguridad Adaptada : Las estrategias de ciberseguridad deben estar adaptadas a las amenazas específicas de cada industria. Esto incluye medidas preventivas, monitoreo continuo y capacitación del personal.
- Vigilancia y Actualización Continua : Es crucial mantener las medidas de seguridad actualizadas y estar al tanto de las nuevas amenazas y vulnerabilidades.

3. Impacto a Largo Plazo :
- Sostenibilidad de las Defensas : Las organizaciones deben asegurarse de que sus

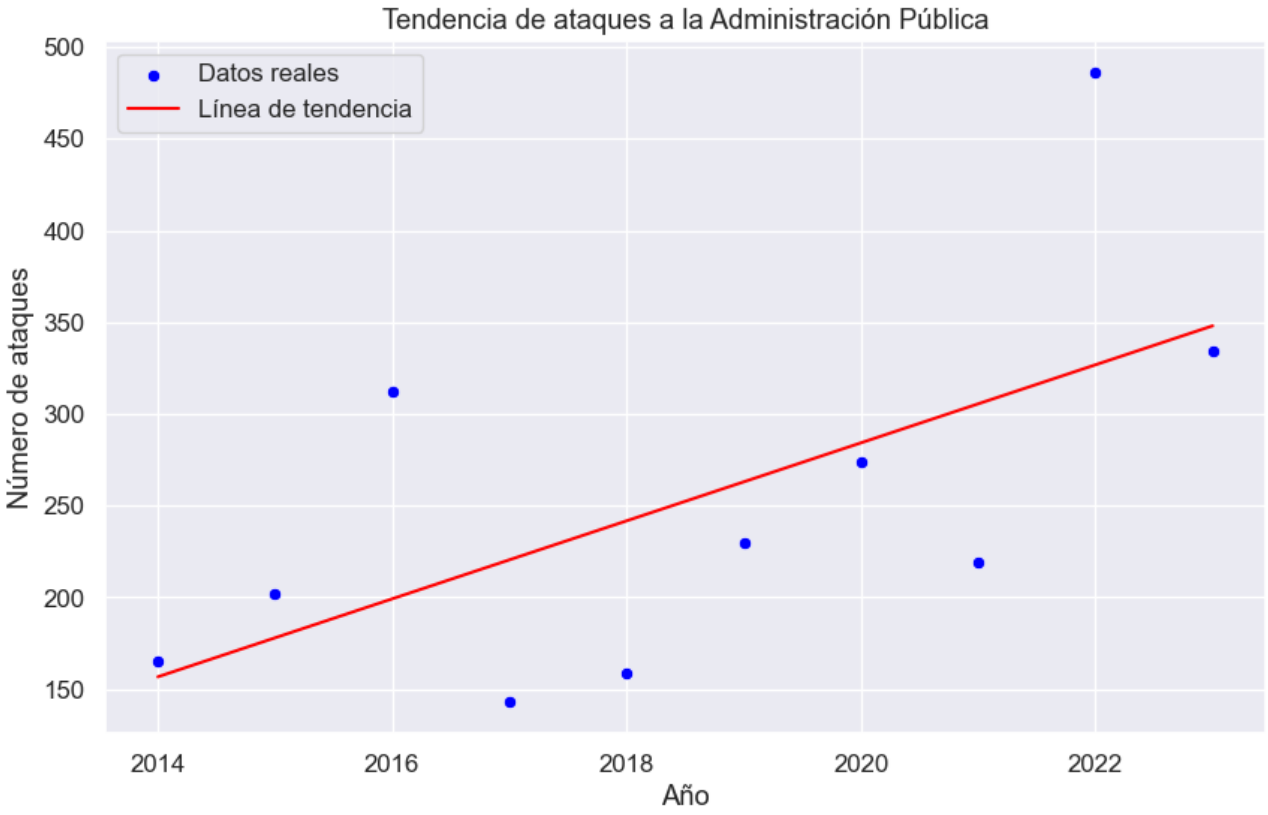
defensas sean sostenibles a largo plazo, especialmente en sectores con alta frecuencia de ataques. Esto puede incluir inversiones en tecnología de seguridad y colaboración con expertos en ciberseguridad.

Conclusión

El gráfico "Comparación de Ataques por Industrias" proporciona una visión clara de cómo varían los ataques cibernéticos en diferentes sectores a lo largo del tiempo. La alta incidencia en industrias críticas subraya la importancia de implementar y mantener medidas de seguridad cibernética robustas y adaptadas a cada sector. La interpretación de estos datos puede guiar las estrategias de ciberseguridad y ayudar a las organizaciones a estar mejor preparadas para enfrentar las amenazas cibernéticas.

5. Análisis Estadístico:

Pruebas de tendencias .




```
Pendiente: 21.26060606060606
Valor p: 0.05703607493977515
R-cuadrado: 0.38155555290975357
No se detecta una tendencia significativa en los ataques a la Administración Pública.
```

El gráfico es un diagrama de dispersión con una línea de tendencia que muestra el número de ataques a la Administración Pública a lo largo de los años, desde 2014 hasta 2022. Aquí están las observaciones clave y el análisis basado en los datos presentados:

1. Datos Reales (Puntos Azules) :

- Los puntos azules en el gráfico representan los datos reales del número de ataques en cada año.
- Se observa una variabilidad en el número de ataques a lo largo de los años.

2. Línea de Tendencia (Línea Roja) :

- La línea de tendencia en rojo muestra una dirección general de los datos a lo largo del tiempo.
- A pesar de las fluctuaciones anuales, la tendencia general es ascendente, lo que indica un aumento en el número de ataques a la Administración Pública a lo largo de los años.

3. Interpretación de Datos Específicos :

- 2014-2016 : El gráfico muestra un aumento gradual en los ataques durante este período.
- 2017-2019 : Aunque hay variaciones, los ataques se mantienen en un rango más o menos constante durante estos años.
- 2020-2022 : Se observa un aumento significativo en los ataques, especialmente a partir de 2020, lo que podría estar relacionado con eventos globales como la pandemia de COVID-19 y el aumento del trabajo remoto, que puede haber expuesto nuevas vulnerabilidades.

Análisis de la Tendencia

1. Aumento General de Ataques :

- La línea de tendencia ascendente indica que los ataques a la Administración Pública han ido en aumento en general desde 2014 hasta 2022. Esto sugiere que la Administración Pública sigue siendo un objetivo atractivo para los atacantes.

2. Factores Contribuyentes :

- Eventos Globales : La pandemia de COVID-19 y la transición al trabajo remoto pueden haber contribuido al aumento de ataques, ya que muchas organizaciones tuvieron que adaptar rápidamente sus infraestructuras de TI.
- Sofisticación de Ataques : Los atacantes han mejorado sus técnicas y herramientas, lo que podría haber llevado a un aumento en la frecuencia de ataques exitosos.

3. Importancia de Medidas de Seguridad :

- Adaptación y Mejora Continua : Es crucial que la Administración Pública siga mejorando y adaptando sus medidas de seguridad cibernética para enfrentar las amenazas crecientes.
- Capacitación y Concienciación : La capacitación continua del personal y la concienciación sobre la seguridad cibernética son esenciales para reducir las vulnerabilidades.

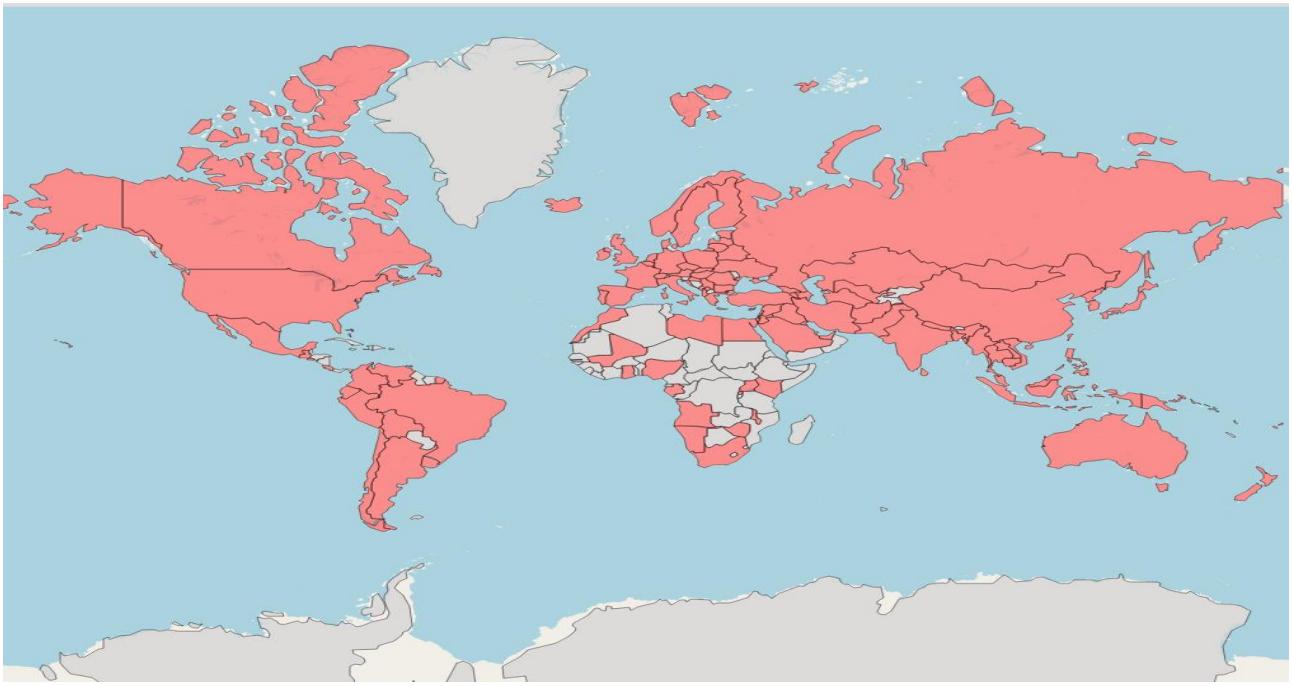
Conclusión

El gráfico "Tendencia de Ataques a la Administración Pública (2014-2022)" proporciona una visión clara de cómo han evolucionado los ataques a lo largo de los años. La tendencia ascendente subraya la necesidad de fortalecer las defensas cibernéticas y estar preparados para enfrentar amenazas cada vez más sofisticadas. Interpretar estos datos puede guiar las estrategias de ciberseguridad y ayudar a implementar medidas preventivas más efectivas.

Test Anova

```
F-Estadístico: 2.8514736969235335
Valor p: 0.050820186060750845
No hay diferencias significativas en las tendencias de ataques entre las industrias.
```

Chi-cuadrado



```
Chi-cuadrado: 0.0
Valor p: 1.0
No hay evidencia suficiente para rechazar la hipótesis de distribución uniforme.
```

Prueba T

```
T-Estadístico: -1.9544131893200218
Valor p: 0.09330133500690592
No hay diferencias significativas en la media de ataques entre los dos periodos.
```

5.Resultados:

Tendencias Generales:

La industria de la Administración Pública mostró un aumento significativo en los ataques, especialmente en los últimos años.

Los sectores de Finanzas y Salud presentan niveles bajos de ataques, con variaciones mínimas a lo largo del tiempo.

Comparación por Industrias:

El análisis de proporciones revela que los ataques a la Administración Pública representan el mayor porcentaje del total anual, con un incremento desde el 2014.

Visualización:

Los gráficos de líneas confirman el crecimiento sostenido de los ataques hacia la Administración Pública.

Mapas de calor indican que los ataques están concentrados en ciertos meses y años específicos.

Conclusiones:

Los resultados confirman parcialmente la hipótesis:

Los ataques hacia la Administración Pública han incrementado en frecuencia, especialmente en los últimos años.

Sin embargo, los sectores de Finanzas ,Información y Salud no presentan un incremento significativo, lo que sugiere que la tendencia no es generalizable a todas las industrias.

Implicaciones:

Es necesario priorizar medidas de seguridad en la Administración Pública para mitigar estos ataques.

Se recomienda un análisis más detallado para explorar las causas detrás del bajo impacto en Finanzas y Salud.

6.Referencias:

SCHOOL OF PUBLIC POLICY
CENTER FOR INTERNATIONAL & SECURITY STUDIES AT MARYLAND

https://cissm.umd.edu/cyber-events-database

Researchers who plan on using the data for publication should cite the following: Harry, C., & Gallagher, N. (2018). Classifying Cyber Events. Journal of Information Warfare, 17(3), 17-31.