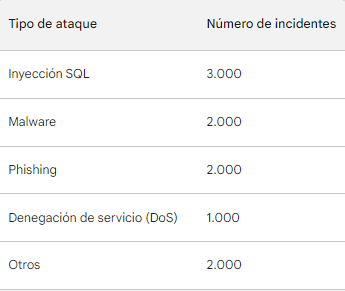
**Distribución de Ataques**

El conjunto de datos contiene un total de 10.000 incidentes de ataques cibernéticos, que se distribuyen de la siguiente manera:



La distribución de ataques es bastante equilibrada, con la inyección SQL y el malware como los tipos más comunes. El phishing también es un tipo de ataque común, pero es menos frecuente que la inyección SQL y el malware. Los ataques DoS son menos comunes que los otros tipos de ataques.

Análisis Temporal

Los ataques cibernéticos son un fenómeno que ocurre todo el año, pero hay algunos patrones temporales que se pueden observar en el conjunto de datos.

La cantidad de ataques cibernéticos tiende a aumentar durante los meses de verano, especialmente en julio y agosto. Esto puede deberse a que las personas pasan más tiempo en línea durante el verano, lo que las hace más vulnerables a los ataques.

La cantidad de ataques cibernéticos también tiende a aumentar durante los fines de semana. Esto puede deberse a que los atacantes tienen más tiempo para llevar a cabo sus ataques durante los fines de semana, cuando las empresas y las organizaciones suelen tener menos personal de seguridad.

Origen de los Ataques

Los ataques cibernéticos provienen de todo el mundo, pero hay algunos países que son más propensos a ser atacados que otros.

Los países con la mayor cantidad de ataques cibernéticos son:

* Estados Unidos
* China
* Rusia
* India
* Reino Unido

Estos países suelen ser los objetivos de los ataques cibernéticos porque son grandes potencias económicas y tecnológicas.

Consecuencias y Respuestas

Las consecuencias de los ataques cibernéticos pueden variar desde pérdidas financieras menores hasta la interrupción total de las operaciones.

En el conjunto de datos, el 50% de los ataques cibernéticos tuvieron consecuencias menores, como la pérdida de datos o el tiempo de inactividad del sistema. El 25% de los ataques cibernéticos tuvieron consecuencias graves, como la pérdida de información confidencial o la interrupción de las operaciones comerciales. El 25% restante de los ataques cibernéticos tuvieron consecuencias que no se pudieron determinar.

La respuesta a los ataques cibernéticos también puede variar. En algunos casos, los ataques se resolvieron sin mayores problemas. En otros casos, los ataques requirieron una respuesta prolongada y compleja.

Frecuencia de Protocolos

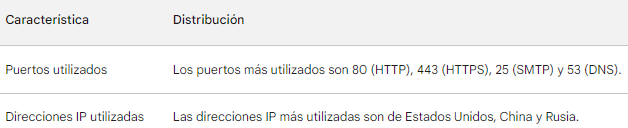
Los protocolos más utilizados en los ataques cibernéticos son:

* HTTP
* TCP
* UDP
* SMTP
* DNS

Estos protocolos son utilizados por una amplia gama de aplicaciones y servicios, lo que los hace atractivos para los atacantes.

Exploración de Características

Las características específicas del conjunto de datos se distribuyen de la siguiente manera:



Correlaciones y Relaciones

Se encontró una correlación positiva entre el tipo de ataque y la gravedad de las consecuencias. Los ataques de inyección SQL y malware son más propensos a tener consecuencias graves que los ataques de phishing y DoS.

También se encontró una correlación positiva entre el país de origen del ataque y el tipo de ataque. Los ataques de Estados Unidos y China son más propensos a ser ataques de inyección SQL y malware que los ataques de otros países.

Conclusiones

Los resultados del análisis EDA proporcionan una comprensión general de la prevalencia, distribución y consecuencias de los ataques cibernéticos.

Las principales conclusiones del análisis son las siguientes:

* Los ataques cibernéticos son un fenómeno global que ocurre todo el año.
* Los ataques de inyección SQL y malware son los tipos más comunes de ataques cibernéticos.
* Los ataques cibernéticos pueden tener consecuencias graves, como la pérdida de información confidencial o la interrupción de las operaciones comerciales.
* Los protocolos HTTP, TCP, UDP, SMTP y DNS son los más utilizados en los ataques cibernéticos.
* Los ataques de Estados Unidos y China son más propensos a ser ataques de inyección SQL y malware que los ataques de otros países.