Módulo 2. Introducción a la IA aplicada sin código. Ciberataque DoS

El panorama actual de las ciberamenazas es complejo. El cambio a entornos de nube y nube híbrida ha provocado la proliferación de datos y la ampliación de las superficies de ataque, mientras que los actores de amenazas siguen encontrando nuevas formas de explotar las vulnerabilidades.

La seguridad usando IA puede ofrecer una solución al automatizar la detección y respuesta a amenazas; la IA facilita la prevención de ataques y la detección de actores de amenazas en tiempo real. Las herramientas de IA pueden ayudar con todo, desde prevenir ataques de *malware* identificando y aislando *software* malicioso hasta detectar ataques de fuerza bruta reconociendo y bloqueando intentos repetidos de inicio de sesión.

No invertir en seguridad de IA sale caro; hay estudios que hablan sobre las organizaciones sin seguridad de IA, como por ejemplo las publicaciones de la empresa de tecnología IBM (s. f., https://shorturl.at/v6S0c) que mencionan que estas organizaciones se enfrentan a un coste medio de

vulneración de datos de 5,36 millones de dólares, un 18,6 % más que el coste medio de todas las organizaciones.

Los modelos de IA son tan fiables como sus datos de entrenamiento. Los datos manipulados o sesgados pueden dar lugar a falsos positivos o respuestas inexactas. Por ejemplo, los datos de entrenamiento sesgados utilizados para las decisiones de contratación pueden reforzar los sesgos de género o raciales con modelos de IA que favorecen a ciertos grupos demográficos y discriminan a otros.

Según Silva (2023, https://shorturl.at/f0WGj), la Oficina Federal de Investigación (FBI) ha observado un aumento de las intrusiones cibernéticas debido a la IA.

1. Beneficios de la seguridad de la IA

Beneficios de la seguridad de la IA

Las capacidades de la IA pueden proporcionar muchas ventajas para mejorar las defensas de ciberseguridad. Algunos de los beneficios más significativos de la seguridad de la IA incluyen los siguientes.

Detección mejorada de amenazas:

los algoritmos de IA pueden analizar grandes cantidades de datos en tiempo real para mejorar la velocidad y la precisión de la detección de posibles ciberamenazas. Las herramientas de IA también pueden identificar vectores de ataque sofisticados que las medidas de seguridad tradicionales podrían pasar por alto.

Respuesta más rápida a los incidentes:

la IA puede acortar el tiempo necesario para detectar, investigar y responder a los incidentes de seguridad, lo que permite a las organizaciones hacer frente a las amenazas con mayor rapidez y reducir los daños potenciales.

Mayor eficiencia operativa:

las tecnologías de IA pueden automatizar las tareas rutinarias, agilizar las operaciones de seguridad y reducir los costes. La optimización de las operaciones de ciberseguridad también puede reducir los errores humanos y liberar a los equipos de seguridad para proyectos más estratégicos.

Un enfoque proactivo de la ciberseguridad:

la seguridad de la IA permite a las organizaciones adoptar un enfoque más proactivo de la ciberseguridad mediante el uso de datos históricos para predecir futuras ciberamenazas e identificar vulnerabilidades.

Comprender las amenazas emergentes:

la seguridad de la IA ayuda a las organizaciones a adelantarse a los actores de amenazas. Al aprender continuamente de nuevos datos, los sistemas de IA pueden adaptarse a las amenazas emergentes y

garantizar que las defensas de ciberseguridad se mantengan actualizadas contra los nuevos métodos de ataque.

Experiencia de usuario mejorada:

la IA puede mejorar las medidas de seguridad sin comprometer la experiencia del usuario. Por ejemplo, los métodos de autenticación con IA, como el reconocimiento biométrico y el análisis del comportamiento, pueden hacer que la autenticación de los usuarios resulte más fluida y segura.

Cumplimiento normativo automatizado:

la IA puede ayudar a automatizar la monitorización del cumplimiento, la protección de datos y la elaboración de informes, garantizando que las organizaciones cumplan sistemáticamente los requisitos normativos.

Capacidad de escalar:

las soluciones de ciberseguridad de IA pueden escalar para proteger entornos de TI grandes y complejos. También pueden integrarse con herramientas e infraestructura de ciberseguridad existentes, como plataformas de gestión de eventos e información de seguridad (SIEM) para mejorar la inteligencia de amenazas en tiempo real de la red y las capacidades de respuesta automatizada.

Posibles vulnerabilidades y riesgos de seguridad de la IA

A pesar de las numerosas ventajas, la adopción de nuevas herramientas de IA puede ampliar la superficie de ataque de una organización y presentar varias amenazas a la seguridad.

Algunos de los riesgos de seguridad más comunes que plantea la IA incluyen los siguientes.

Riesgos para la seguridad de los datos

Los sistemas de IA se basan en conjuntos de datos que pueden ser vulnerables a manipulaciones, vulneraciones y otros ataques. Las organizaciones pueden mitigar estos riesgos protegiendo la confidencialidad, disponibilidad e integridad de los datos a lo largo de todo el ciclo de vida de la IA, desde el desarrollo hasta el entrenamiento y la implementación.

Riesgos de seguridad del modelo de IA

Los actores de amenazas pueden apuntar a los modelos de IA para robarlos, realizar ingeniería inversa o manipularlos sin autorización. Los atacantes pueden comprometer la integridad de un modelo manipulando su arquitectura,

pesos o parámetros, los componentes principales que determinan el comportamiento y el rendimiento de un modelo de IA.

Ataques adversarios

Los ataques adversarios implican la manipulación de datos de entrada para engañar a los sistemas de IA, lo que lleva a predicciones o clasificaciones incorrectas. Por ejemplo, **los atacantes pueden generar ejemplos adversarios que exploten las vulnerabilidades de los algoritmos de IA para interferir en la toma de decisiones de los modelos de IA o producir sesgos.**

Del mismo modo, las inyecciones de instrucciones utilizan instrucciones maliciosas para engañar a las herramientas de IA para que realicen acciones dañinas, como filtrar datos o eliminar documentos importantes.

Implementación ética y segura

Si los equipos de seguridad no priorizan la seguridad y la ética a la hora de implementar los sistemas de IA, corren el riesgo de cometer violaciones de la privacidad y de exacerbar los sesgos y los falsos positivos. Solo con una implementación ética pueden las organizaciones garantizar

la equidad, la transparencia y la responsabilidad en la toma de decisiones de la IA.

Conformidad con la normativa

Cumplir con los requisitos legales y reglamentarios es esencial para garantizar el uso legal y ético de los sistemas de IA. Las organizaciones deben cumplir, según la jurisdicción pertinente, normativas como el Reglamento General de Protección de Datos (RGPD),[1] la California Consumer Privacy Act (CCPA)[2] y la Ley de IA de la UE (Unión Europea),[3] de lo contrario se arriesgan a exponer datos sensibles y a enfrentarse a duras sanciones legales

[1] Reglamento 2016/679 [Parlamento Europeo; Consejo de la Unión Europea]. Reglamento General de Protección de Datos. 14 de abril de 2016.

[2] Ley de Privacidad del Consumidor de California de 2018 [Legislatura Estatal de California]. 3 de enero de 2018.

[3] Reglamento 2024/1689 [Comisión Europea]. Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. 13 de marzo de 2024.

Ataques de manipulación de entrada

Los ataques de manipulación de entrada implican alterar los datos de entrada para influir en el comportamiento o los resultados de los sistemas de IA. Los atacantes pueden manipular los datos de entrada para evadir la detección, eludir las medidas de seguridad o influir en los procesos de toma de decisiones, lo que puede dar lugar a resultados sesgados o inexactos.

Por ejemplo, los actores de amenazas pueden comprometer los *outputs* de un sistema de IA en ataques de envenenamiento de datos al alimentar intencionalmente al modelo con datos de entrenamiento incorrectos.

Ataques a la cadena de suministro

Los ataques a la cadena de suministro se producen cuando los actores de amenazas se dirigen a los sistemas de IA con respecto a la cadena de suministro, incluidas sus etapas de desarrollo, implementación o mantenimiento. Por ejemplo, los atacantes pueden explotar vulnerabilidades en componentes, bibliotecas de *software* o módulos de terceros utilizados en el desarrollo de IA, lo que provoca vulneraciones de datos o accesos no autorizados.

Los modelos de IA se desvían y decaen

Los modelos de IA pueden experimentar un decaimiento con el tiempo, lo que provoca una degradación del rendimiento o la eficacia. Los adversarios pueden explotar los puntos débiles de un modelo de IA en decadencia o a la deriva para manipular los *outputs*. Las organizaciones pueden monitorizar los modelos de IA en busca de cambios en el rendimiento, el comportamiento o la precisión para mantener su fiabilidad y relevancia

Casos de uso de seguridad de IA

Las aplicaciones de la IA en ciberseguridad son diversas y evolucionan continuamente a medida que las herramientas de IA se vuelven más avanzadas y accesibles.

Algunos de los casos de uso más comunes de la seguridad de la IA en la actualidad incluyen los siguientes.

Protección de datos

La protección de datos implica salvaguardar la información sensible contra la pérdida y la corrupción de datos para protegerlos y garantizar su disponibilidad y el cumplimiento de los requisitos normativos.

Las herramientas de inteligencia artificial pueden ayudar a las organizaciones a mejorar la protección de datos al clasificar los datos confidenciales, supervisar el movimiento de los datos e impedir el acceso o la filtración no autorizados. La IA también puede optimizar los procesos de cifrado y tokenización para proteger los datos en reposo y en tránsito.

Además, la IA puede adaptarse automáticamente al panorama de las amenazas y monitorizarlas las 24 horas del día, lo que permite a las organizaciones adelantarse a las ciberamenazas emergentes.

Seguridad de punto final

La seguridad de *endpoints* implica proteger los *endpoints*, como computadoras, servidores y dispositivos móviles, de las amenazas a la ciberseguridad.

La IA puede mejorar las soluciones existentes de detección y respuesta de *endpoints* (EDR) mediante la monitorización continua de los *endpoints* en busca de comportamientos sospechosos y anomalías para detectar amenazas de seguridad en tiempo real.

Los algoritmos de *machine learning* también pueden ayudar a identificar y mitigar las amenazas avanzadas para

endpoints, como el *malware* sin archivos y los ataques de día cero, antes de que causen daños.

Seguridad en la nube

La IA puede ayudar a proteger los datos confidenciales en entornos de *cloud* híbrido identificando automáticamente los datos invisibles, monitorizando las anomalías en el acceso a los datos y alertando a los profesionales de la ciberseguridad sobre las amenazas a medida que se producen.

Búsqueda avanzada de amenazas

Las plataformas de búsqueda de amenazas buscan de forma proactiva signos de actividad maliciosa dentro de la red de una organización.

Con las integraciones de IA, estas herramientas pueden ser aún más avanzadas y eficientes al analizar grandes conjuntos de datos, identificar signos de intrusión y permitiruna detección y respuesta más rápidas a las amenazas avanzadas.

Detección del fraude

A medida que los ciberataques y el robo de identidad se vuelven más comunes, las instituciones financieras necesitan formas de proteger a sus clientes y activos.

La IA ayuda a estas instituciones al analizar automáticamente los datos de las transacciones para detectar patrones que indiquen fraude. Además, los algoritmos de *machine learning* pueden adaptarse a amenazas nuevas y evolucionar en tiempo real, lo que permite a los proveedores financieros mejorar continuamente su detección del fraude y sus capacidades y adelantarse a los actores de amenazas.

Automatización de la ciberseguridad

Las herramientas de seguridad de la IA suelen ser más eficaces cuando se integran con la infraestructura de seguridad existente de la organización.

> Por ejemplo, la orquestación, automatización y respuesta de seguridad (SOAR) es una solución de *software* que muchas organizaciones utilizan para agilizar las operaciones de seguridad. La IA puede integrarse con las plataformas SOAR para automatizar las tareas rutinarias y los flujos de trabajo. Esta integración puede permitir una respuesta más rápida a los incidentes y liberar a los

analistas de seguridad para que se centren en problemas más complejos.

Gestión de identidad y acceso (IAM)

Las herramientas de gestión de identidades y accesos (IAM) gestionan cómo los usuarios acceden a los recursos digitales y qué pueden hacer con ellos. Su objetivo es mantener alejados a los *hackers* y, al mismo tiempo, garantizar que cada usuario tenga los permisos exactos que necesita y nada más.

Las soluciones de IAM impulsadas por IA pueden mejorar este proceso proporcionando controles de acceso granulares basados en roles, responsabilidades y comportamiento, garantizando aún más que solo los usuarios autorizados puedan acceder a datos confidenciales.

La IA también puede mejorar los procesos de autenticación mediante el uso del *machine learning* para analizar los patrones de comportamiento de los usuarios y habilitar medidas de autenticación adaptativas que cambian en función de los niveles de riesgo de los usuarios individuales.

Detección de *phishing*

Los LLM (Modelos de Lenguaje Grande) como ChatGPT han hecho que los ataques de suplantación de identidad sean más fáciles de llevar a cabo y más difíciles de reconocer. Sin embargo, la IA también se ha convertido en una herramienta fundamental para combatir la suplantación de identidad.

Los modelos de *machine learning* pueden ayudar a las organizaciones a analizar correos electrónicos y otras comunicaciones en busca de signos de *phishing*, mejorando la precisión de la detección y reduciendo los intentos de *phishing* exitosos. Las soluciones de seguridad del correo electrónico con IA también pueden proporcionar inteligencia sobre amenazas en tiempo real y respuestas automatizadas para detectar ataques de *phishing* en cuanto se produzcan.

Gestión de vulnerabilidades

La gestión de vulnerabilidades es el descubrimiento, la priorización, la mitigación y la resolución continuos de vulnerabilidades de seguridad en la infraestructura y el *software* de TI (Tecnología de la Información) de una organización.

La IA puede mejorar los escáneres de vulnerabilidades tradicionales priorizando automáticamente las vulnerabilidades en función del impacto potencial y la

probabilidad de explotación. Esto ayuda a las organizaciones a abordar primero los riesgos de seguridad más críticos.

La IA también puede automatizar la gestión de parches para reducir rápidamente la exposición a las ciberamenazas.

Detección de ataques DDoS

Gestado en la tesis doctoral del magíster Walter Agüero (2025), se ha desarrollado lo que se considera el primer antivirus argentino que detecta los ataques de denegación de servicios distribuidos en redes definidas por *software* en forma muy eficiente. Este conocimiento permite que se explique más adelante cómo detectar DoS (denegación de servicio distribuido), tarea que realizarán los alumnos, es decir, realizarán su primer antivirus también. Este proyecto forma parte de dos proyectos de investigación en la Universidad Siglo 21 y la Universidad Nacional de Villa Mercedes, San Luis.

Sistema de Reconocimiento

El Sistema de Reconocimiento Facial Multimodal para Aplicaciones *Online/Offline* con Capacidad Transetaria (**DeepAgeFace**) (2025) es el otro desarrollo del Mgter. Walter Agüero. Este trabajo presenta DeepAgeFace, un sistema de

reconocimiento facial basado en redes neuronales convolucionales (CNN) que integra tres modalidades clave:

1. reconocimiento *online* en tiempo real mediante cámaras convencionales o drones,
2. análisis *offline* en videos (cámaras de seguridad, drones), y
3. reconocimiento transetario en fotografías, capaz de identificar personas con diferencias de edad extremas (ej.: 7 vs. 35 años).

El modelo utiliza una arquitectura Siamese Network con mecanismos de atención espacial y un *loss function* híbrido (ArcFace + regularización temporal). Con esto, logra un 98.7 % de precisión en LFW (Labeled Faces in the Wild [Rostros Etiquetados en la Naturaleza]) y un 92.4 % en el desafío transetario CACD-VS. Esta investigación contribuye a las capacidades nacionales de ciberseguridad y ciberdefensa, cuyas funciones prácticas pueden ser utilizadas en la seguridad pública, búsqueda de personas desaparecidas, vigilancia con drones, neutralizar objetivos específicos, entre algunas de las funciones.

Figura 1. DeepAgeFace

Fuente: elaboración propia.

IA aplicada sin escribir código de programación

La IA aplicada sin código se logra mediante plataformas «no-code» [sin código] que usan interfaces visuales de arrastrar y soltar y descripciones en lenguaje natural para crear aplicaciones, automatizaciones y análisis, lo que democratizala creación de *software* para usuarios no técnicos, permitiendo desarrollar desde asistentes virtuales

hasta *apps* móviles funcionales con herramientas como Bubble, Adalo, Glide o integrando IA generativa para crear *apps* a partir de descripciones como con Google Firebase Studio o Lovable, lo que acelera la innovación sin depender de programadores.

¿Cómo funciona la IA sin código?

- **Interfaces visuales:** construyes *apps* arrastrando y soltando componentes predefinidos (como bloques de LEGO) en lugar de escribir código.
- **Lenguaje natural:** describes lo que quieres que haga la IA (ej. «una app de recetas con buscador») y la IA genera la estructura y el código base.
- **Automatización**: conectas diferentes herramientas (como Zapier) para automatizar flujos de trabajo que incorporan IA sin programa.

Qué puedes crear

Si bien la creatividad es el techo de lo que se puede desarrollar, la base es el conocimiento que se transmite. Algunos desarrollos que pueden realizarse son los siguientes.

- **Asistentes virtuales y chatbots**: para atención al cliente o automatización interna.
- **Aplicaciones móviles**: desde hojas de cálculo hasta apps más complejas con Adalo o Glide.
- **Herramientas internas**: paneles de control, sistemas de análisis predictivo o motores de recomendación.
- **Automatización de *marketing***: formularios inteligentes con Typeform o flujos de datos con Parabola.

Herramientas populares.

- **Bubble, Adalo, Glide:** para crear apps web y móviles visualmente.
- **Zapier**: para automatizar tareas entre aplicaciones.

- **Firebase Studio (Google):** integra IA Gemini para generar *apps* a partir de descripciones o bocetos.

- **Lovable**: convierte lenguaje natural en *apps* web funcionales.

Beneficios

- Democratización: acceso a la IA para no técnicos (*marketing*, RRHH, ventas).

- Rapidez: desarrollo y despliegue más rápidos.

- Enfoque en el usuario: priorizas la experiencia y funcionalidad sobre la complejidad técnica.

Sin bien en otro de los cursos se describió conceptos de *no-code*, repasaremos aquí algunos conceptos de Google.

Definición de «sin código»

El desarrollo sin código es un método para crear *software* que utiliza una herramienta visual de arrastrar y soltar. En

lugar de escribir líneas de código en un lenguaje de programación especial, usas el *mouse* para mover **piezas prefabricadas** y para configurar su funcionamiento.

La plataforma sin código se encarga de todo el código, los servidores y los detalles técnicos complicados en segundo plano. Convierte nuestro diseño visual en una aplicación real y funcional. Este enfoque ayuda a las personas que entienden un problema empresarial pero no tienen conocimientos de programación (a menudo denominados «desarrolladores ciudadanos») a crear sus propias soluciones.

¿Cómo funciona una plataforma sin código?

Las plataformas sin código se encargan de las tareas más complejas. El usuario decide lo que quiere que haga la aplicación y la plataforma se encarga de que funcione. Utilizas piezas prediseñadas y listas para usar que representan partes comunes de una aplicación.

¿Cuáles son los componentes de una plataforma sin código?

- **Creador de interfaz de usuario visual:** una herramienta de arrastrar y soltar para diseñar

el aspecto de la aplicación a construir, incluidas sus pantallas, formularios y botones.

- **Modelización de datos:** herramientas que ayudan a configurar los datos de la aplicación, normalmente conectándose a una hoja de cálculo o base de datos que ya tenga.

- **Motor de lógica y flujo de trabajo:** un sistema visual para definir reglas y automatizar tareas. Por ejemplo, puede definir una regla como «si el estado es 'aprobado', envía un correo».

- **Conectores:** conexiones listas para usar que vinculan tu aplicación con otros servicios y herramientas populares.

- **Implementación con un clic:** una forma sencilla de publicar su aplicación para que los usuarios la utilicen en la Web o en sus teléfonos, sin necesidad de configurar ningún servidor.

Sin código, con poco código o mediante programación intuitiva

Para crear aplicaciones hoy en día, hay varias opciones. Comprender las diferencias entre los enfoques de programación sin código, con poco código, intuitiva y tradicional te ayudará a seleccionar la herramienta más adecuada para tus necesidades, independientemente de tu experiencia en programación.

Tabla 1. Creación de aplicaciones

Proporción	Sin código	Poco código	Programación intuitiva o generación de código con IA
Usuario principal	Usuarios empresariales, desarrolladores ciudadanos y cualquier personal no técnico.	Desarrolladores profesionales y expertos en TI.	Cualquier persona con una idea clara, incluidos desarrolladores, diseñadores y pensadores.
Método	Usando herramientas puramente visuales como	Herramientas visuales con la opción de añadir código	Usar texto sin formato para indicar a un asistente de IA

	arrastrar y soltar, formularios y menús.	para las partes más complejas o personalizadas.	lo que quieres que haga la aplicación.
Enfoca	Solucionar problemas empresariales específicos con componentes predefinidos.	Agiliza el proceso de desarrollo de aplicaciones más grandes y personalizadas.	Crear rápidamente código inicial, aplicaciones sencillas o funciones específicas a partir de una descripción de texto.
Productos de ejemplo	AppSheet Google AI Studio	Gemini Code Assist	Firebase Studio Gemini Code Assist Google AI Studio

Fuente: elaboración propia.

CONTINUAR

2. Ciberataque

Un ciberataque es un intento malicioso de acceder, dañar, robar, modificar o destruir datos, sistemas informáticos o redes, a menudo para obtener ganancias financieras, políticas o personales, utilizando técnicas como *malware*, *phishing* o *ransomware* y buscando vulnerabilidades para interrumpir operaciones o robar información sensible, lo que afecta tanto a individuos como a grandes organizaciones conectadas a internet.

¿Qué implica un ciberataque?

- **Acceso no autorizado:** el objetivo principal es entrar en sistemas sin permiso para robar información, alterarla o inhabilitarla.
- **Diversidad de objetivos:** pueden dirigirse a una red personal, una gran empresa, aplicaciones, servidores o dispositivos.

- **Motivaciones variadas:** detrás de un ataque puede haber intereses criminales, políticos, espionaje o incluso actos de vandalismo digital.

Tipos comunes de ciberataques

- ***Malware***: *software* malicioso (virus, troyanos, gusanos, *spyware*) que se infiltra para obtener acceso o dañar el sistema.
- ***Phishing*:** correos o mensajes fraudulentos que se hacen pasar por entidades legítimas para engañar y robar datos.
- **Ransomware:** bloquea el acceso a archivos o sistemas y exige un rescate para liberarlos.
- **Ataques DDoS**:sobrecargan un servidor o red para que deje de funcionar.
- **Inyección SQL y XSS:** aprovechan vulnerabilidades en aplicaciones web para robar o manipular datos.

- **Ataques de fuerza bruta:** intentan descifrar contraseñas probando miles de combinaciones.

¿Quién los realiza?

Hackers solitarios.

Grupos de cibercrimen organizados.

Actores patrocinados por estados (ciberguerra).

¿Cómo protegerse?

Usar *software* de seguridad confiable y mantenerlo actualizado.

Implementar una buena estrategia de ciberseguridad con contraseñas fuertes y autenticación de dos factores.

Tener un plan de respuesta a incidentes para recuperarse.

Ciberataque DoS

Un ciberataque DoS busca dejar un sistema, red o servicio inaccesible para usuarios legítimos, inundándolo con tráfico o solicitudes hasta agotar sus recursos (ancho de banda, procesamiento) y colapsarlo. Suelen tener como motivación lo económico, político o el sabotaje, y se manifiestan como lentitud extrema o caídas de sitios web.

¿Cómo funciona un ataque DoS?

El objetivo principal de un ataque DoS es sobrecargar la capacidad de una máquina objetivo, lo que da lugar a una denegación de servicio a solicitudes adicionales. Los múltiples **vectores de ataque** de los ataques DoS pueden agruparse por sus similitudes.

Los ataques DoS suelen ser de dos categorías.

ATAQUES DE DESBORDAMIENTO DE BÚFER	ATAQUES DE INUNDACIÓN
Un tipo de ataque en el que se produce un desbordamiento del búfer de la memoria puede hacer que una máquina consuma todo el espacio disponible en el disco duro, la memoria o el tiempo de la CPU. Esto suele provocar un rendimiento lento, caídas del sistema u	

otros comportamientos perjudiciales para el servidor, lo que acaba desembocando en una denegación de servicio.

ATAQUES DE DESBORDAMIENTO DE BÚFER

ATAQUES DE INUNDACIÓN

Al saturar un servidor objetivo con una cantidad abrumadora de paquetes, un actor malicioso es capaz de sobrecargar la capacidad del servidor, lo que provoca una denegación de servicio. Para que la mayoría de los ataques de inundación DoS tengan éxito, el actor malicioso debe tener más ancho de banda disponible que el objetivo.

Ataques DoS habituales

- **Ataque Smurf:** un ataque DoS que se ha aprovechado previamente en el que un actor malicioso utiliza la dirección de difusión de una red vulnerable mediante el envío de paquetes falsos, lo que resulta en la inundación de una dirección IP objetivo.
- **Inundación de *ping***: este sencillo ataque de denegación de servicio se basa en sobrecargar a un objetivo con paquetes ICMP (*ping*). Al inundar un objetivo con más *pings* de los que es capaz de responder con eficacia, se

puede producir una denegación de servicio. Este ataque también se puede utilizar como un ataque DDoS.

- ***Ping* de la muerte:** se suele confundir con un ataque de inundación de *ping*, pero un ataque de *ping* de la muerte implica el envío de un paquete malformado a una máquina objetivo, lo que provoca un comportamiento dañino, como la caída del sistema.

¿Cómo saber si hay un ataque DoS?

Aunque pueda ser difícil separar un ataque de otros errores de conectividad de red o de gran consumo de ancho de banda, hay algunas características que pueden indicar que se está produciendo un ataque.

Los indicadores de un ataque DoS incluyen lo siguiente.

- Rendimiento atípico de la red, manifestado en tiempos de carga de archivos o sitios web demasiado largos.

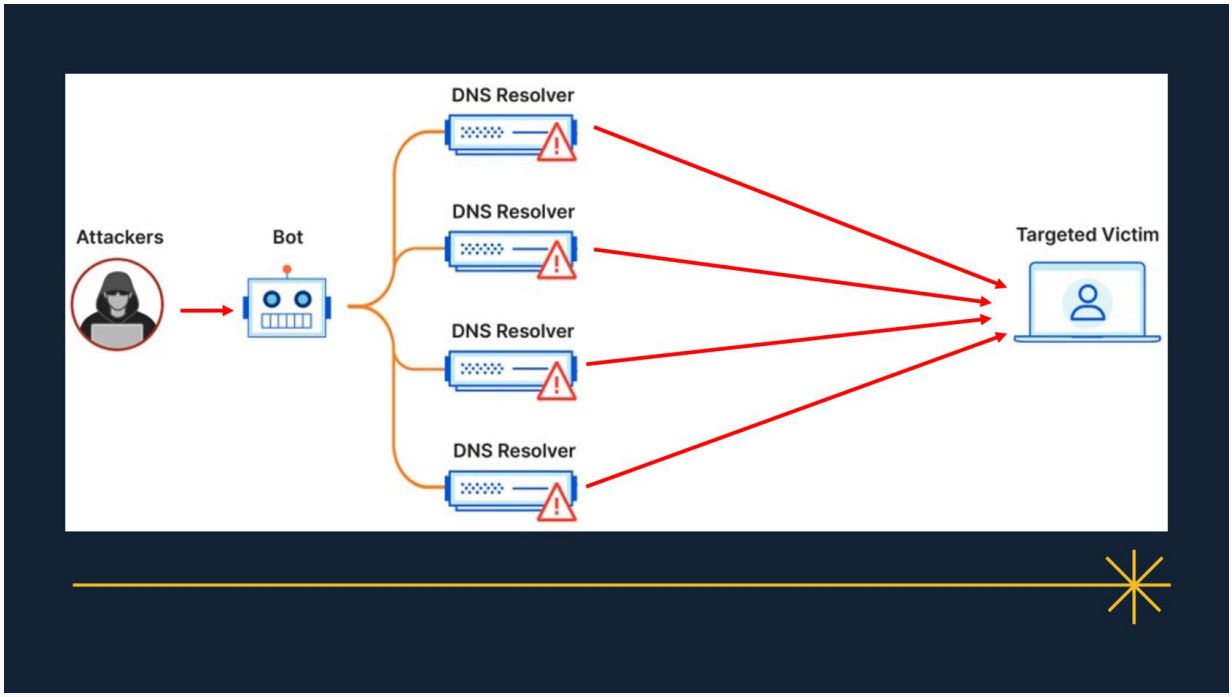
- La imposibilidad de cargar un sitio web concreto, como tu propiedad web.

- Pérdida repentina de conectividad en los dispositivos de la misma red.

Cómo detectar DoS

La siguiente imagen demuestra claramente que habría una comunicación hacia un destino que podría calificarse como potencial víctima (*targeted victim*).

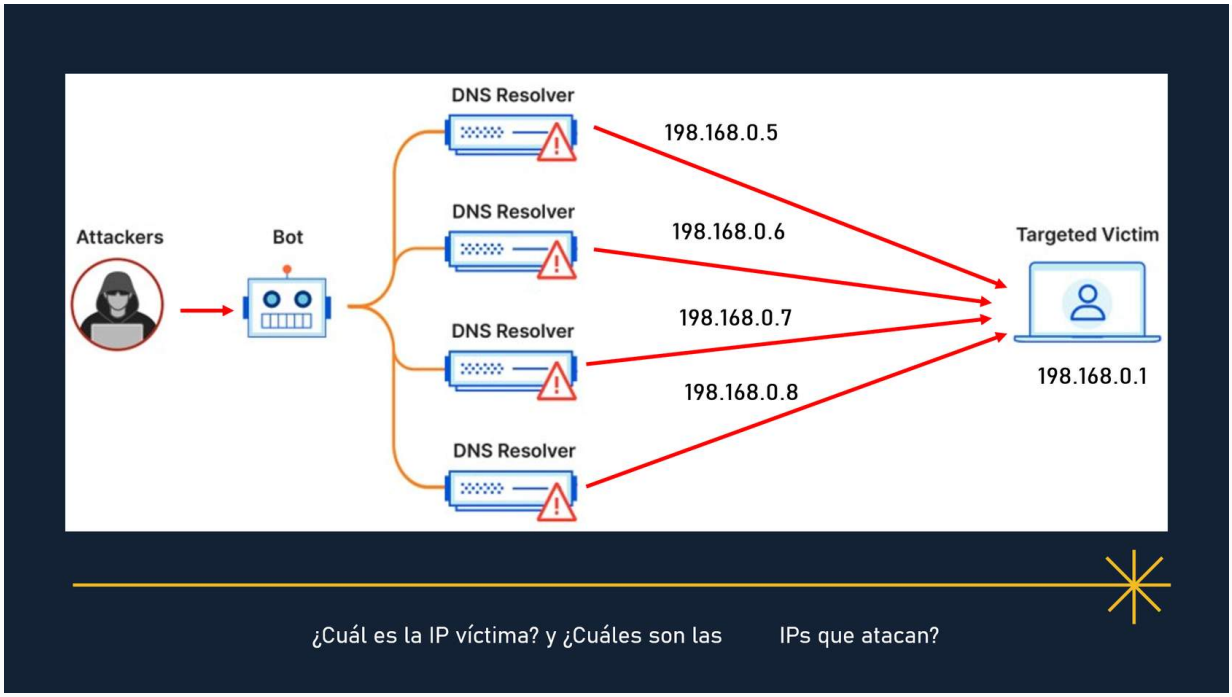
Figura 2. Víctima



Fuente: elaboración propia con base en [imagen sin título sobre víctima]. (2023). https://shorturl.at/GzP0I

Es necesario analizar las IP origen e IP destino.

Figura 3. IP



Fuente: elaboración propia con base en [imagen sin título sobre víctima]. (2023). https://shorturl.at/GzP0I

Si agrupamos las IP origen y destino, vemos lo siguiente.

Tabla 2. IP de origen y destino

IP ORIGEN	IP DESTINO
192.168.0.5	192.168.0.1
192.168.0.5	192.168.0.1

192.168.0.5	192.168.0.1
192.168.0.5	192.168.0.1
192.168.0.5	192.168.0.1

Fuente: elaboración propia.

Luego, si sumamos la cantidad de la misma IP origen que le llegan a la IP destino, podríamos tener algo así como lo siguiente.

Tabla 3. Suma de IP

IP ORIGEN	IP DESTINO	CANTIDAD
192.168.0.5	192.168.0.1	10.482.447

Fuente: elaboración propia.

El número 10.482.447 indicaría que estamos en presencia de un ataque DoS.

Si tuviéramos un contador ajustable que sume la cantidad de IP como lo de la tabla anterior y si esa cuenta superase el valor fijado, podría sonar una alarma que obligue a un

humano a prestar atención y certificar si es un ataque de DoS.

CONTINUAR

Referencias

Agüero, W. (8 y 9 de octubre de 2025). *DeepAgeFace: sistema de reconocimiento facial multimodal para aplicaciones online/offline con capacidad transetaria*. 2° Congreso Ciencia, Tecnología e Innovación para la Defensa y 1° Exposición de Empresas de la Defensa.

Agüero, W., Uzal, R., Gonzales, M., Britos, P. y Vallejo, M. (2025). *Distributed Denial of Service Detection Using Neural Networks in Software-Defined Networks*. World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering, 19(10), 488-493. https://publications.waset.org/10014284.pdf

[Imagen sin título sobre víctima]. (2023). https://achirou.com/wp-content/uploads/2023/11/amplification_ddos_example-980x490.png

International Business Machines Corporation. (s. f.). *Informe "Cost of a Data Breach" de 2025*. International Business Machines Corporation. https://www.ibm.com/es-es/reports/data-breach

Ley de Privacidad del Consumidor de California de 2018 [Legislatura Estatal de California]. 3 de enero de 2018.

Reglamento 2016/679 [Parlamento Europeo; Consejo de la Unión Europea]. Reglamento General de Protección de Datos. 14 de abril de 2016.

Reglamento 2024/1689 [Comisión Europea]. Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. 13 de marzo de 2024.

Silva, R. (31 de julio de 2023). *FBI revela que cibercriminales están usando inteligencia artificial para crear malware*. Infobae. https://www.infobae.com/tecno/2023/07/31/fbi-revela-que-cibercriminales-estan-usando-inteligencia-artificial-para-crear-malware/

CONTINUAR