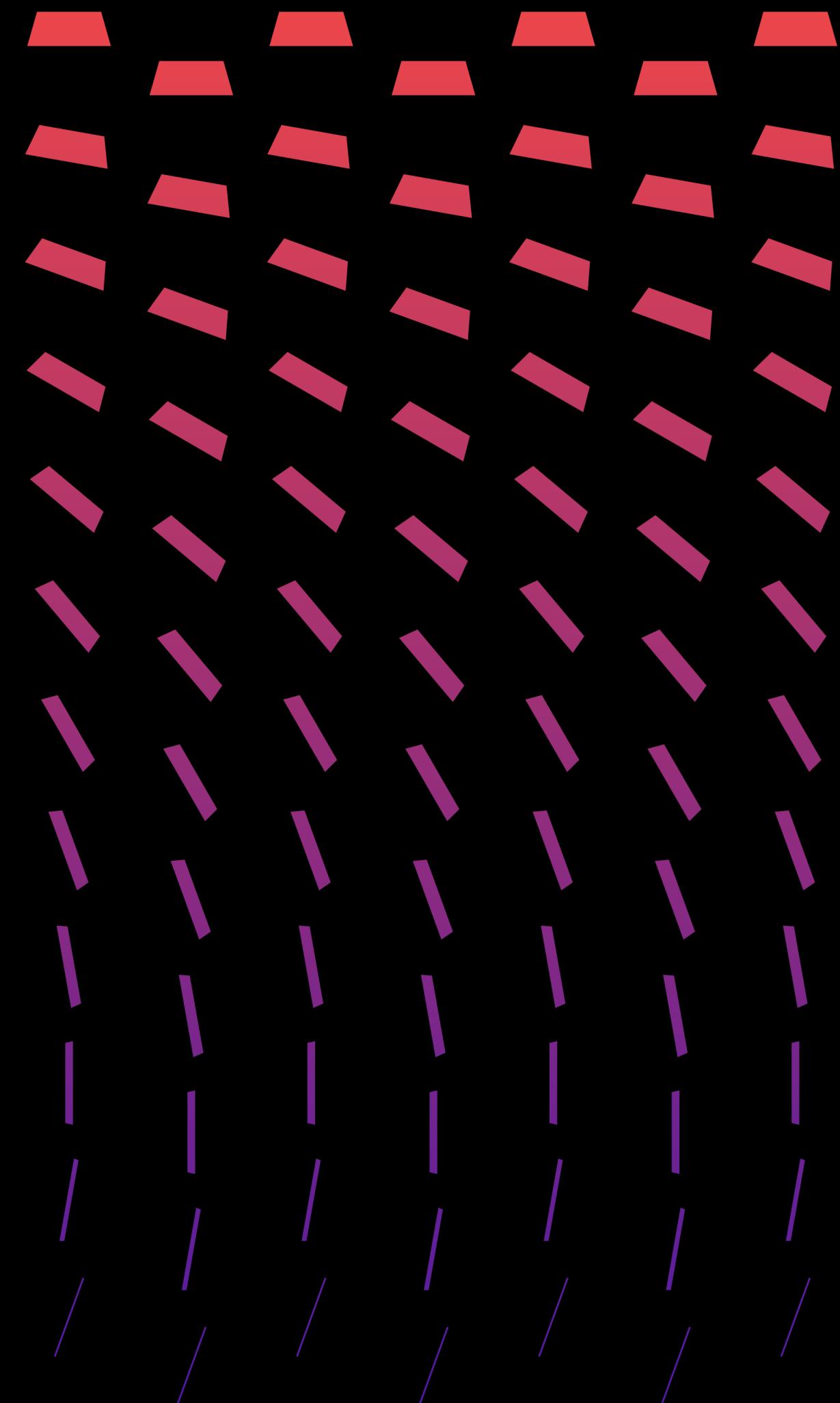


Machine Learning

Análisis del aporte del aprendizaje
de máquinas a la seguridad de la
información

Septiembre 2023

por Hamilton M.





Resumen



Todo dispositivo informático tiene sus propios registros de seguridad. Al juntar miles de dispositivos que intervienen en las comunicaciones de computadores personales, bases de datos, servidores web, dispositivos de red, firewalls, etc., se genera un gran volumen de registros con información interesante desde el punto de vista de seguridad, aunque imposible de revisar por un ser humano.

Ahí es donde hace sentido contar con herramientas automatizadas con cierta inteligencia capaces de realizar análisis y detectar patrones maliciosos que puedan afectar la confidencialidad, integridad y disponibilidad de la información

INTRODUCCIÓN



En un mundo donde la digitalización empresarial está en constante aumento, el riesgo de ataques informáticos se ha vuelto una preocupación creciente para las organizaciones. La información se ha convertido en un activo invaluable, y protegerla de manera eficaz se ha vuelto una prioridad.

En respuesta a esta amenaza, la industria ha avanzado significativamente, desarrollando herramientas de vanguardia basadas en Inteligencia Artificial y Aprendizaje Automático. Estos sistemas tienen la capacidad de analizar grandes volúmenes de datos, prever comportamientos y ofrecer resultados comparables a los procesos humanos.



LOS RIESGOS DE LA INFORMACIÓN ESTÁN PRESENTES DESDE QUE EXISTAN LAS AMENAZAS Y LAS VULNERABILIDADES

Tipos de amenazas:

Virus informáticos

Uso no autorizado

Robo de información

Ataques de fuerza bruta

Desastres naturales

Spywares

Troyanos o gusanos

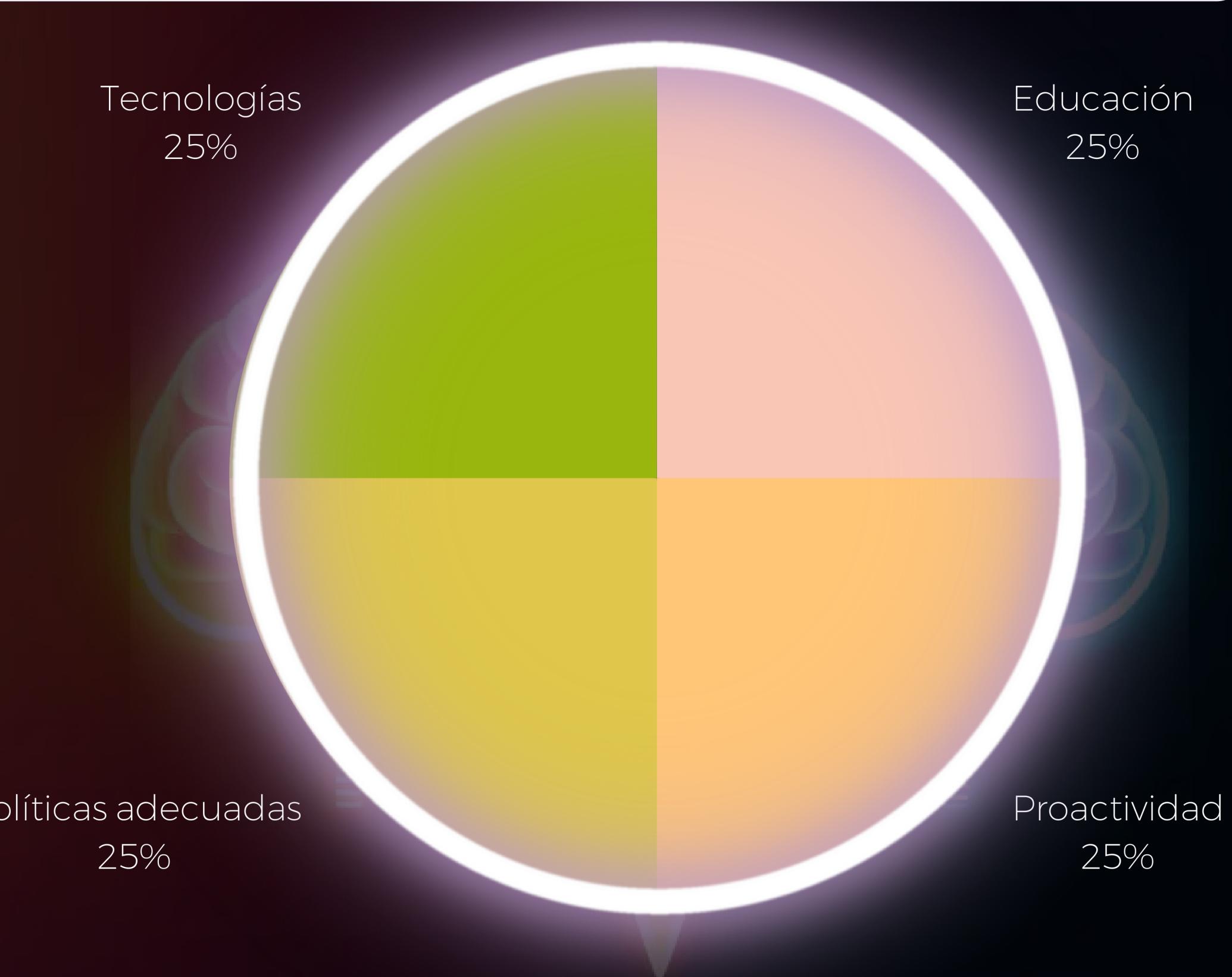
Phishing

Trashing

Ransomware

"Trazando el Camino hacia una Seguridad Informática Efectiva"

Dado que la organización está expuesta a tantas amenazas y vulnerabilidades, se puede afirmar que la fórmula para prevenir ser víctima de un ataque informático es combinar elementos como educación, proactividad, políticas adecuadas y tecnología que permita realizar análisis proactivo.



"OPTIMIZANDO LA SEGURIDAD: EXPLORANDO ALGORITMOS EN LA PREVENCIÓN DE ATAQUES INFORMÁTICOS"

A partir de las amenazas y vulnerabilidades descritas anteriormente. Las organizaciones ya están recurriendo al Machine-Learning, una de las ramas de la Inteligencia Artificial (IA), ésto como apoyo para el análisis y toma de decisiones de eventos de seguridad por medio de algoritmos.

Algoritmos que se utilizan para el Aprendizaje Automático

APRENDISAJE SUPERVISADO

En el aprendizaje supervisado del Machine Learning, los datos de entrada, llamados datos de entrenamiento, están etiquetados con resultados conocidos, como spam/no-spam o precios de acciones.

APRENDISAJE NO SUPERVISADO

En Algoritmos de aprendizaje no supervisados, los datos carecen de etiquetas y resultados predefinidos. Se construye un modelo identificando las estructuras inherentes en los datos, a menudo para derivar reglas generales.

APRENDISAJE SEMI-SUPERVISADO

Los algoritmos de aprendizaje semisupervisados, los datos de entrada son una combinación de ejemplos etiquetados y no etiquetados. A pesar de tener un problema de predicción definido, el modelo debe aprender las estructuras subyacentes de los datos para realizar predicciones precisas,

Tipos de Algoritmos del ML Agrupado

por Similitud

Aprendizaje Supervisado

Algoritmos de regresión

Predicen valores numéricos basados en datos anteriores.

Algoritmos de regulación

Utiliza técnicas del ML para prevenir SobreAjustes, controlando la complejidad del modelo

Aprendizaje No Supervizado

Algoritmos de agrupamiento

Agrupan datos similares en clústeres, facilitando el análisis de datos no etiquetados.

Aprendizaje Profundo

Algoritmos aprendizaje profundo

Modelos del ML compuestos por múltiples Capas de procesamiento.

Tipos de Algoritmos del ML Agrupado por Similitud

Otros tipos de Algoritmos de Aprendizaje

Algoritmos Basado en Instancias

Realizan predicciones basadas en similitudes con las instancias previas.

Algoritmos de árbol de decisión

Toman decisiones basadas en condiciones y estructuras del árbol.,

Algoritmos de Redes Neuronales

Son modelos del ML inspirado en la estructura del cerebro humano.

Algoritmos aprendizaje de reglas de asociación

Descubren patrones y relaciones en grandes conjuntos de datos.

Algoritmos Bayesianos

Son modelos basados en el teorema de Bayes que calcula la probabilidad basándose en conocimientos previos.

Dado el panorama complejo y en constante evolución de las amenazas ciberneticas, es esencial que las organizaciones adopten tecnologías avanzadas como el Aprendizaje Automático (ML) para fortalecer sus estrategias de seguridad. En lugar de centrarse únicamente en la protección de activos específicos, se debe considerar el contexto en el que se accede a estos activos y cómo se utilizan. Las herramientas de ML tienen la capacidad única de analizar grandes volúmenes de datos y proporcionar un contexto detallado sobre las actividades de los usuarios y las amenazas potenciales.

CONCLUSIÓN

Al invertir en sistemas de ML, las organizaciones pueden obtener una visión profunda de las actividades que rodean sus activos, permitiendo a los analistas discernir eventos a lo largo del tiempo y entre diferentes dispositivos y redes. Esta comprensión contextual no solo reduce los riesgos de violaciones de seguridad, sino que también aumenta significativamente el "costo del ataque" para los perpetradores, minimizando así posibles amenazas.

iGracias!

29-09-2023