UNIVERSIDAD TECNOLÓGICA DE PANAMÁ
FACULTAD DE INGENIERÍA DE SISTEMAS COMPUTACIONALES
DEPARTAMENTO DE PROGRAMACIÓN DE COMPUTADORAS
GUÍA DE LABORATORIO N° 1

Facilitador: Ing. José Javier Chirú F. Asignatura: Desarrollo WEB

Estudiante: _____ Fecha: _____ Grupo: _____

A. TÍTULO DE LA EXPERIENCIA: *HTML*

B. TEMAS: *Etiquetas sobre títulos, párrafos*

C. OBJETIVO(S):

- Identificar la estructura básica de una página HTML
- Emplear las etiquetas a la hora de crear paginas HTML

D. METODOLOGÍA:

1. Trabaje de manera grupal
2. Debe desarrollar su página HTML
3. Discutir los resultados en el salón de clase

E. ENUNCIADOS:

Debe construir una página HTML que trate sobre, Texto del artículo:

¿Cómo afecta la inteligencia artificial a la ciberseguridad?

La IA es una novedad que últimamente está en boca de todos. Se refiere a un campo de la informática que se enfoca en crear sistemas o programas capaces de realizar tareas que normalmente requerirían de la inteligencia humana. La IA busca imitar ciertas capacidades cognitivas de los seres humanos, como el razonamiento, la percepción o el procesamiento del lenguaje y el aprendizaje.

Existen diferentes enfoques dentro del campo de la IA, como el Machine Learning, donde los sistemas son capaces de aprender de forma autónoma a partir de los datos; el Procesamiento del lenguaje natural, que permite a la tecnología entender y comunicarse en lenguaje humano; y la Visión artificial (Computer vision), que facilita a las máquinas interpretar y analizar imágenes y videos.

“Este avance no deja de sorprender, revolucionando el paradigma social y tecnológico, garantizando una nueva realidad que debemos entender, pero, sobre todo, saber manipular. Gartner estima que para el 2025 al menos un 50% de las empresas habrá diseñado plataformas

de orquestación para operacionalizar la IA, en comparación con menos del 10% en 2020", afirma Carlos Oviedo Risi, Country Manager para Argentina y Chile de IFX Networks.

Protección de la información

En el campo de la ciberseguridad, la IA puede ser utilizada como una herramienta poderosa para mejorar la protección de la información. Algunas de las opciones a considerar son:

Detección de amenazas: los sistemas de IA están en capacidad de analizar grandes volúmenes de datos en tiempo real. Esto permite detectar comportamientos anómalos que pueden indicar un ciberataque, como intentos de intrusión o malware. Con un correcto diagnóstico, pueden alertar de manera temprana a los profesionales de seguridad para tomar medidas inmediatas.

Análisis de vulnerabilidades: la IA puede estudiar y evaluar la seguridad de los sistemas de las organizaciones en busca de posibles vulnerabilidades. De esta manera es posible prevenir las amenazas de ciberdelincuentes, tomando las medidas preventivas necesarias.

Autenticación y acceso seguro: el uso de técnicas de reconocimiento de voz, reconocimiento facial o análisis de comportamiento del usuario contribuye a fortalecer la autenticación y el acceso seguro a las cuentas o plataformas.

Peligros a tener en cuenta

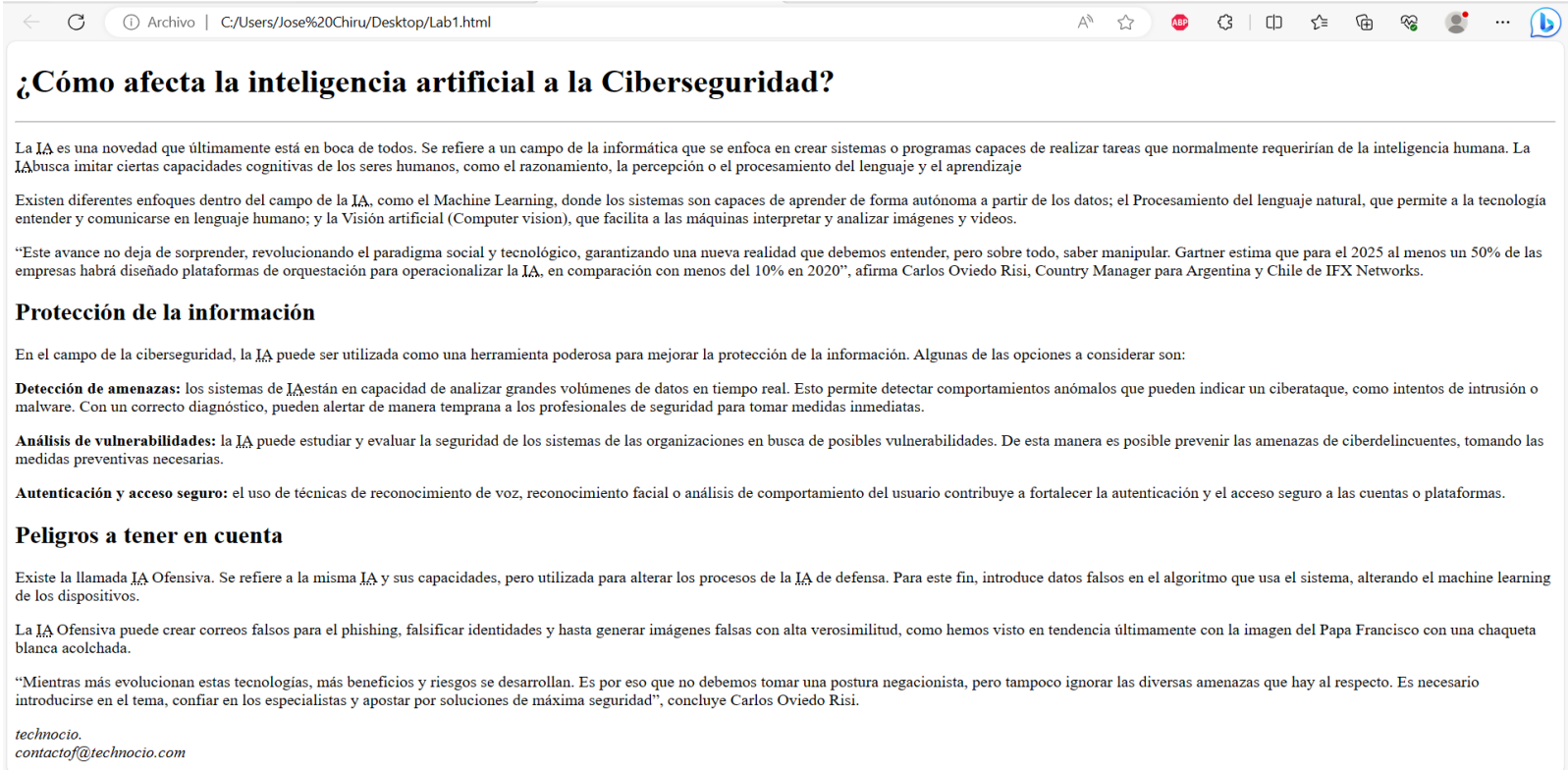
Existe la llamada IA Ofensiva. Se refiere a la misma IA y sus capacidades, pero utilizada para alterar los procesos de la IA de defensa. Para este fin, introduce datos falsos en el algoritmo que usa el sistema, alterando el machine learning de los dispositivos.

La IA Ofensiva puede crear correos falsos para el phishing, falsificar identidades y hasta generar imágenes falsas con alta verosimilitud, como hemos visto en tendencia últimamente con la imagen del Papa Francisco con una chaqueta blanca acolchada.

"Mientras más evolucionan estas tecnologías, más beneficios y riesgos se desarrollan. Es por eso que no debemos tomar una postura negacionista, pero tampoco ignorar las diversas amenazas que hay al respecto. Es necesario introducirse en el tema, confiar en los especialistas y apostar por soluciones de máxima seguridad", concluye Carlos Oviedo Risi.

technocio

UNIVERSIDAD TECNOLÓGICA DE PANAMÁ
FACULTAD DE INGENIERÍA DE SISTEMAS COMPUTACIONALES
DEPARTAMENTO DE PROGRAMACIÓN DE COMPUTADORAS
GUÍA DE LABORATORIO N° 1



¿Cómo afecta la inteligencia artificial a la Ciberseguridad?

La IA es una novedad que últimamente está en boca de todos. Se refiere a un campo de la informática que se enfoca en crear sistemas o programas capaces de realizar tareas que normalmente requerirían de la inteligencia humana. La IAbusca imitar ciertas capacidades cognitivas de los seres humanos, como el razonamiento, la percepción o el procesamiento del lenguaje y el aprendizaje

Existen diferentes enfoques dentro del campo de la IA, como el Machine Learning, donde los sistemas son capaces de aprender de forma autónoma a partir de los datos; el Procesamiento del lenguaje natural, que permite a la tecnología entender y comunicarse en lenguaje humano; y la Visión artificial (Computer vision), que facilita a las máquinas interpretar y analizar imágenes y videos.

"Este avance no deja de sorprender, revolucionando el paradigma social y tecnológico, garantizando una nueva realidad que debemos entender, pero sobre todo, saber manipular. Gartner estima que para el 2025 al menos un 50% de las empresas habrá diseñado plataformas de orquestación para operacionalizar la IA, en comparación con menos del 10% en 2020", afirma Carlos Oviedo Risi, Country Manager para Argentina y Chile de IFX Networks.

Protección de la información

En el campo de la ciberseguridad, la IA puede ser utilizada como una herramienta poderosa para mejorar la protección de la información. Algunas de las opciones a considerar son:

Detección de amenazas: los sistemas de IAestán en capacidad de analizar grandes volúmenes de datos en tiempo real. Esto permite detectar comportamientos anómalos que pueden indicar un ciberataque, como intentos de intrusión o malware. Con un correcto diagnóstico, pueden alertar de manera temprana a los profesionales de seguridad para tomar medidas inmediatas.

Análisis de vulnerabilidades: la IA puede estudiar y evaluar la seguridad de los sistemas de las organizaciones en busca de posibles vulnerabilidades. De esta manera es posible prevenir las amenazas de ciberdelincuentes, tomando las medidas preventivas necesarias.

Autenticación y acceso seguro: el uso de técnicas de reconocimiento de voz, reconocimiento facial o análisis de comportamiento del usuario contribuye a fortalecer la autenticación y el acceso seguro a las cuentas o plataformas.

Peligros a tener en cuenta

Existe la llamada IA Ofensiva. Se refiere a la misma IA y sus capacidades, pero utilizada para alterar los procesos de la IA de defensa. Para este fin, introduce datos falsos en el algoritmo que usa el sistema, alterando el machine learning de los dispositivos.

La IA Ofensiva puede crear correos falsos para el phishing, falsificar identidades y hasta generar imágenes falsas con alta verosimilitud, como hemos visto en tendencia últimamente con la imagen del Papa Francisco con una chaqueta blanca acolchada.

"Mientras más evolucionan estas tecnologías, más beneficios y riesgos se desarrollan. Es por eso que no debemos tomar una postura negacionista, pero tampoco ignorar las diversas amenazas que hay al respecto. Es necesario introducirse en el tema, confiar en los especialistas y apostar por soluciones de máxima seguridad", concluye Carlos Oviedo Risi.

technocio.
contactof@technocio.com

F. PROCEDIMIENTO:

Desarrollar el artículo utilizando las etiquetas de párrafos y títulos

G. RECURSOS:

Visual Studio Code, Notepad++ o el de su elección

H. RESULTADOS (OPCIONAL, DE ACUERDO CON LA ACTIVIDAD):

Los resultados deben subir en formato Zip

I. BIBLIOGRAFIA:

Lemay, L., & Colburn, R. (2010). *Sams Teach Yourself Web Publishing With HTML and CSS in One Hour a Day* (6.ª ed.). Sams.

Lozano, G. F. J. C. G. (2017). *Desarrollo web con PHP y MySQL. Edición 2018* (1.ª ed.). ANAYA MULTIMEDIA.

Pollock, J. (2019). *Javascript: A Beginner's Guide, Fifth Edition* (5th ed.). McGraw-Hill Companies.

Puertas, J. P. (2006). *Creación de un portal con PHP y MySQL*. Alfaomega.

Thomson, L. W. (2017). *Desarrollo Web con PHP y MySQL. Quinta Edición* (1.ª ed.). ANAYA MULTIMEDIA.

J. RÚBRICAS:

Aspectos a Evaluar	Puntaje Máximo 100 pts.
Seguir Indicaciones	**15**
Desarrollo de forma clara	**10**
Resolución del problema	**75**
Total	**100**