

### PERFIL DEL TRABAJO DE TITULACIÓN

<b>FACULTAD:</b>	INFORMÁTICA Y ELECTRÓNICA
<b>CARRERA:</b>	SOFTWARE
<b>PERIODO ACADÉMICO:</b>	1 de ABRIL – 19 de AGOSTO 2024

#### DATOS DEL PROPONENTE(S)

<b>APELLIDOS:</b>	ZUMBA MORALES
<b>NOMBRES:</b>	JORGE ALEXANDER
<b>CÓDIGO DEL ESTUDIANTE:</b>	6918
<b>CEDULA DE CIUDADANÍA:</b>	1401003908
<b>CORREO ELECTRÓNICO INSTITUCIONAL:</b>	jorge.zumba@espoch.edu.ec

#### DATOS DEL DIRECTOR:

<b>APELLIDOS:</b>	CAMACHO CASTILLO
<b>NOMBRES:</b>	JAIME DAVID
<b>CEDULA DE CIUDADANÍA:</b>	0201732369
<b>CORREO ELECTRÓNICO INSTITUCIONAL:</b>	jaimed.camacho@espoch.edu.ec

#### DATOS DEL PERFIL DEL TRABAJO DE TITULACION

<b>OPCION:</b>	TRABAJO DE TITULACIÓN
<b>MODALIDAD:</b>	PROYECTO TÉCNICO
<b>TEMA:</b>	ANÁLISIS DEL SISTEMA DE CIBESSEGURIDAD DEL GAD DE RIOBAMBA UTILIZANDO TÉCNICAS DE INTELIGENCIA ARTIFICIAL
<b>OBJETIVO GENERAL:</b>	Analizar el sistema de ciberseguridad del GAD de Riobamba utilizando técnicas de inteligencia artificial para identificar sus fortalezas, debilidades y áreas de mejora.

ALINEACIÓN DEL TEMA		
<b>LINEA(S) Y PROGRAMA(S) DE INVESTIGACIÓN DE LA ESPOCH</b>	<b>LÍNEA DE INVESTIGACIÓN:</b> TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC)	
	<b>PROGRAMA:</b> CIBERSEGURIDAD	
<b>OBJETIVOS DE DESARROLLO SOSTENIBLE (ODS)</b>	<b>SELECCIONAR ODS QUE SE ARTICULAN CON LA LÍNEA DE INVESTIGACIÓN TIC:</b> <input type="checkbox"/> 3. SALUD Y BIENESTAR <input type="checkbox"/> 4. EDUCACIÓN DE CALIDAD <input type="checkbox"/> 8. TRABAJO DECENTE Y CRECIMIENTO ECONÓMICO <input checked="" type="checkbox"/> 9. INDUSTRIA, INNOVACIÓN E INFRAESTRUCTURAS	<b>OTROS ODS:</b> <input type="checkbox"/> 10. REDUCCIÓN DE LAS DESIGUALDADES <input type="checkbox"/> 11. CIUDADES Y COMUNIDADES SOSTENIBLES <input type="checkbox"/> 12. PRODUCCIÓN Y CONSUMO RESPONSABLES <input type="checkbox"/> 15. VIDA DE ECOSISTEMAS TERRESTRES.
<b>PROBLEMA</b> (BREVE DESCRIPCIÓN)		
<p>La creciente dependencia de las instituciones gubernamentales de riobamba en los sistemas digitales expone al gobierno autónomo descentralizado (gad) a diversas amenazas cibernéticas, como ataques de malware, phishing, y vulnerabilidades en la infraestructura de red. la falta de un sistema de ciberseguridad robusto y adaptado a las últimas tecnologías de inteligencia artificial deja al gad de riobamba vulnerable a estas amenazas, poniendo en riesgo la integridad y confidencialidad de la información sensible y la prestación eficiente de servicios públicos. este problema resalta la necesidad urgente de evaluar y mejorar el sistema de ciberseguridad del gad de riobamba para garantizar la protección de los activos digitales y la confianza de los ciudadanos en la gestión gubernamental.</p>		
<b>METODOLOGIA</b>		
<b>METODO</b>	Enfoque mixto de investigación (cualitativo y cuantitativo) para entrenar un modelo de inteligencia artificial que realice un análisis de vulnerabilidades del sistema de ciberseguridad del GAD de Riobamba. este enfoque incluye la recopilación de datos, preprocesamiento, entrenamiento del modelo, evaluación, implementación y monitoreo continuo.	
<b>TECNICA(S)</b>	1. Análisis de Datos: Recopilación activa y pasiva de información. 2. Aprendizaje Automático: Uso de algoritmos de aprendizaje supervisado y no supervisado para identificar patrones y predecir vulnerabilidades. 3. Análisis de Vulnerabilidades: Identificación de debilidades en el sistema mediante herramientas especializadas y técnicas de escaneo. 4. Explotación de Vulnerabilidades: Simulación de ataques para probar las debilidades identificadas y evaluar la capacidad del sistema para resistir dichos ataques.	

	<p>5. Validación Cruzada: Aplicación de validación cruzada para evaluar la precisión y evitar el sobreajuste del modelo.</p> <p>6. Evaluación del Modelo: Uso de métricas como precisión, recall, F1-score y AUC-ROC para medir el rendimiento del modelo.</p> <p>7. Simulación de Vulnerabilidades: Simulación de escenarios de ataques para probar la robustez del modelo.</p>
<b>INSTRUMENTO (S)</b>	<p>1. Herramientas de Análisis de Datos: Software como Python (pandas, scikit-learn) para procesamiento y análisis de datos.</p> <p>2. Plataformas de Aprendizaje Automático: Bibliotecas de Python como scikit-learn, TensorFlow, y Keras para el entrenamiento y evaluación de modelos de aprendizaje automático.</p> <p>3. Herramientas de Validación y Evaluación: Métodos estadísticos y bibliotecas de evaluación (scikit-learn) para medir el rendimiento del modelo.</p> <p>4. Simuladores de Vulnerabilidades: Herramientas de simulación de ataques como Metasploit para probar la eficacia del modelo en escenarios de ataques reales.</p> <p>5. Herramientas de Recolección de Información: Herramientas como Recon-ng, FOCA y Maltego para la recolección de información, facilitando la identificación de posibles vulnerabilidades y puntos débiles en el sistema.</p>
<b>TRABAJO REALIZADO / REVISIÓN DE LITERATURA</b>	
<b>INVESTIGACIONES RELACIONADAS REALIZADAS. (DENTRO Y FUERA DE LA ESPOCH)</b>	<ul style="list-style-type: none"> <li>MESIAS F. (2023). ANÁLISIS DE VULNERABILIDADES MEDIANTE PENTESTING A LA APLICACIÓN MÓVIL DESARROLLADA PARA EL CENTRO MÉDICO DE ESPECIALIDADES "LA DOLOROSA". RECUPERADO DE: <a href="http://dSPACE.esPOCH.edu.ec/handle/123456789/20880">HTTP://DSPACE.ESPOCH.EDU.EC/HANDLE/123456789/20880</a></li> <li>ASTUDILLO MUÑOZ, E. M., &amp; VIZUETE ULLOA, A. E. (2023). ANÁLISIS DE VULNERABILIDADES Y PRUEBAS DE ESTRÉS AL SISTEMA ACADÉMICO DE LA ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO. RECUPERADO DE: <a href="http://dSPACE.esPOCH.edu.ec/handle/123456789/20850">HTTP://DSPACE.ESPOCH.EDU.EC/HANDLE/123456789/20850</a></li> <li>BAUTISTA F. (2023) . CIBERSEGURIDAD EN PYMES: CASO DE ESTUDIO EN CAYAMBE. RECUPERADO DE: <a href="https://dominiodelasciencias.com/ojs/index.php/es/article/view/3597">HTTPS://DOMINIODELSCIENCIAS.COM/OJS/INDEX.PHP/ES/ARTICLE/VIEW/3597</a></li> <li>BRICEÑO, J. C. (2019). ANÁLISIS DE VULNERABILIDADES DE LOS SISTEMAS DE SEGURIDAD INFORMÁTICA DE LA EMPRESA KAPPA10 LTDA.. [PROYECTO APLICADO, UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD]. REPOSITORIO INSTITUCIONAL UNAD. <a href="https://repository.unad.edu.co/handle/10596/27">HTTPS://REPOSITORY.UNAD.EDU.CO/HANDLE/10596/27</a></li> </ul>

	<a href="#"><u>822</u></a>
--	----------------------------

FIRMA DEL ESTUDIANTE(S)

FIRMA DEL DIRECTOR