Logotipo

El contenido generado por IA puede ser incorrecto.

**Planteamiento del problema y revisión de literatura**

**El problema de investigación (panorama):**

*El problema de investigación* ***responde a un vacío de conocimiento de índole teórica o práctica*** *que requiere ser investigado para ofrecer una respuesta o propuesta de solución teórica o práctica.*

| Aun a pesar del uso intensivo de plataformas digitales por los alumnos de la carrera Técnico en Ingeniería en Computación de la Universidad Don Bosco sede Soyapango, existe una escasez notable tanto a nivel de conocimientos como de competencias para poder identificar ataques de phishing y para establecer medidas mínimas de ciberseguridad; la alegación de casos reales de compañeros afectados evidencian cómo esta falta de competencias aumenta la posibilidad de perder datos personales y académicos así como de sufrir fraudes económicos y de paralizan la actividad académica. Pero, a su vez, desconociéndose entonces cuáles son las causas de carácter personal, institucional y contextual que explican esta falta de competencias dentro del contexto de la Universidad local. |
| --- |

**La pregunta de investigación**

*La pregunta de investigación permite* ***identificar de manera puntual el objeto de estudio*** *al que se dará una respuesta teórica o práctica*

| ¿Cuál es el nivel de desarrollo de las competencias teóricas y prácticas en herramientas básicas de ciberseguridad, así como la tasa de exposición a ataques de phishing, entre los estudiantes de la carrera Técnico en Ingeniería en Computación de la Universidad Don Bosco, sede Soyapango? |
| --- |

**El objetivo de investigación**

*El objetivo planteado define con claridad qué se pretende lograr* ***como resultado de la investigación*** *para dar respuestas a un problema teórico o práctico.*

| Determinar el nivel de desarrollo de las competencias teóricas y prácticas en ciberseguridad básica con énfasis en la identificación y prevención de ataques de phishing y estimar la tasa de exposición a dichos ataques entre los estudiantes de la carrera Técnico en Ingeniería en Computación de la Universidad Don Bosco, sede Soyapango, con el fin de generar una línea base que oriente el diseño de intervenciones formativas y recursos didácticos contextualizados. |
| --- |

**Estado del arte o estado de la cuestión:**

*Expone* ***hasta qué punto el problema propuesto ha sido abordado por otras investigaciones****: qué y cómo ha sido investigado. Lo expuesto se sustenta en revisión bibliográfica.*

| Abu-Shanab & Al-Jamal (2023) compararon respuestas al phishing en países árabes vs. occidentales, hallando que usuarios en sociedades con alta confianza interpersonal (como Japón o países escandinavos) son más vulnerables a mensajes que apelan a la reciprocidad, sin embargo, no solo en los países occidentales se ve con mucha frecuencia ataques de phishing si no que tambien paises mas conservadores en ese tipo de ámbitos las personas siguen callendo y siguen siendo objeto de estos ataque.  Rajivan & Gonzalez (2022) demostraron que las mujeres tienden a ser más desconfiadas ante correos sospechosos, mientras que los hombres son más propensos a hacer clic en enlaces maliciosos por exceso de confianza, sin embargo, aunque las mujeres son más precavidas en estos puntos siguen siendo objeto ya que a personas de edad más avanzada siguen pensando que lo que se les promete o que se les dice en tales ataques es real por lo cual siguen callendo esto mismo sucede con niños jóvenes y adolescentes, y pasa en el tecnico en ingenieria en computacion.  Un estudio de Zhao et al. (2021) encontró que los millennials (25-40 años) tienen mayor confianza en su capacidad para detectar phishing, pero caen con más frecuencia en ataques sofisticados que los adultos mayores, quienes son más cautelosos pero menos técnicos, sin embargo muchos adultos mayores y jóvenes caen por confiarse en sus conocimientos y dejan de lado la investigacion del sitio o fuente en la que buscan sacar ese provecho que se les promete.  Estudios sobre el Nivel de Conocimiento en Ciberseguridad Diversas investigaciones (Hadlington, 2017; Furnell et al., 2019) han evaluado el conocimiento general de los usuarios en temas como contraseñas seguras, detección de correos maliciosos y protección de datos, sin embargo no se hacen cursos o campañas de concientización de la ciberseguridad ya que a pesar de que las personas sepan que hay posibilidad de robo de cuentas, siguen utilizando contraseñas inseguras.  La mayoría de los usuarios no identifica correctamente señales de phishing (dominios falsos, errores gramaticales).  Existe un gran problema en: adultos mayores y adolescentes son los más vulnerables (Williams et al., 2020) Nosotros como grupo hemos visto que en estos casos nunca se esta lo suficientemente preparado para un ataque de phishing pero si se puede evitar caer con facilidad.  Investigaciones sobre Técnicas de Phishing y Vulnerabilidad Humana Estudios experimentales (Jansen & Leukfeldt, 2021) han usado simulaciones de phishing para medir tasas de clics en enlaces maliciosos.  El phishing emocional (mensajes de urgencia o premios) tiene mayor efectividad (Workman, 2022). Esto vemos que es debido a que las personas al ver que es de una marca conocida se confía y no busca en redes oficiales de la institución si esto que se promete es real y por ende caen en esos ataques.  Al ver un mensaje de un conocido que perdió supuestamente el celular y pide dinero para poder trasladarse a cualquier lugar, las personas por lo inesperado lo primero que hacen es atender a ese llamado sin corroborar que la persona qe esta al otro lado de verdad sea su familiar o amigo.  Usuarios con mayor formación digital siguen cayendo en ataques sofisticados (spear phishing).Estrategias de Concientización y su Efectividad Se han probado diferentes métodos para mejorar la educación en ciberseguridad:  Gamificación: Programas como Anti-Phishing Phil (Sheng et al., 2010) redujeron un 40% las caídas en phishing.  Enfoques psicológicos: Enseñar mediante historias reales aumenta la retención del aprendizaje (Canham et al., 2021).  Ferrari & Rosi (2022) identificaron que el phishing que menciona eventos locales (Por Ejemplo: "Actualice sus datos para el censo nacional") tiene tasas de éxito un 45% mayores que mensajes genéricos. Brechas Identificadas en la Literatura A pesar de los avances, persisten desafíos: Chandler et al. (2023) alertaron sobre el uso de ChatGPT y DeepL para crear correos de phishing sin errores gramaticales, aumentando su credibilidad en un 60%. Pocos estudios abordan comunidades con acceso limitado a tecnología (zonas rurales, adultos mayores). La mayoría de las soluciones son para cuando ya se recibió el ataque (tras un ataque) y no para evitar el ataque. |
| --- |

**El marco teórico**

*El marco teórico expone el posicionamiento teórico desde el cual el investigador desarrollará su investigación. El marco teórico hace referencia a teoría general y sustantiva.*

| .El phishing, una forma de ingeniería social, se basa en engañar a los usuarios para que les proporcionen información delicada (contraseñas, datos bancarios) o para hacer que realicen acciones que comprometen dispositivos o redes; en los últimos años la técnica ha evolucionado (tipos de spear-phishing, Phishing-as-a-Service o PhaaS), lo que ha mejorado su eficiencia y el riesgo para ciertos usuarios con una alta exposición digital, de tal forma que, teniendo en cuenta el uso intensivo de plataformas digitales por parte del estudiantado universitario, el phishing representa un vector de riesgo crucial para la comunidad universitaria (ENISA, 2020; revisiones de vectores de correo malicioso). Al aplicar esta evidencia al **objeto de estudio** —los estudiantes de la carrera Técnico en Ingeniería en Computación de la Universidad Don Bosco, sede Soyapango— la investigación debe centrarse en identificar **las causas** (personales, institucionales y contextuales) del déficit de competencias teórico-prácticas para reconocer y prevenir estos ataques, más que en las herramientas específicas. Las instituciones educativas han registrado incidentes donde correos maliciosos generan robo de cuentas institucionales, accesos no autorizados a servicios académicos, paradas administrativas e impacto reputacional; además, estudios en contextos universitarios muestran que el conocimiento auto-reportado de los estudiantes no siempre se corresponde con su conducta real frente a correos maliciosos, lo que obliga a medir simultáneamente el saber y el hacer para evaluar la vulnerabilidad universitaria (informes sectoriales y estudios de caso). La literatura especializada sostiene que la educación puede reducir la vulnerabilidad ante el phishing, aunque su efecto depende del diseño pedagógico: intervenciones puntuales y genéricas tienden a producir mejoras temporales limitadas, mientras que actividades continuas, interactivas y contextualizadas —incluyendo simulacros éticos y autoevaluaciones— favorecen mayor retención y cambio de conducta; por ello, las intervenciones deberían combinar teoría y práctica y emplear indicadores objetivos para evaluar efectividad (revisiones y programas de concienciación). Organismos expertos como NIST/NICE y ENISA recomiendan además caracterizar competencias, crear perfiles, aplicar encuestas para detectar debilidades educativas, adecuar contenidos a la audiencia y usar métricas objetivas (simulaciones, exámenes prácticos), lo que sustenta la necesidad de un diagnóstico local mixto: encuestas validadas para medir conocimientos declarativos, pruebas de ejecución/exámenes de rendimiento para habilidades concretas, simulaciones controladas para observar conducta real, y entrevistas o análisis de casos para identificar causas subyacentes (investigaciones metodológicas sobre medición de vulnerabilidad). En contextos latinoamericanos debe considerarse la compartición de dispositivos, la predominancia de mensajería móvil y las barreras socioeconómicas que limitan la adopción de medidas (por ejemplo MFA) o el acceso a formación continua, dado que programas estandarizados no adaptados culturalmente muestran eficacia reducida. Siguiendo las posturas complementarias de los investigadores: la posición de **Daniel** enfatiza la necesidad de un diagnóstico cuantitativo riguroso que determine el grado de conocimientos y conductas de riesgo como línea base para intervención, mientras que la posición de **Arturo** aboga por incorporar desde las etapas iniciales evidencia práctica (documentación de casos reales en la cohorte y simulaciones controladas) para que los hallazgos sean aplicables y orienten recursos didácticos que respondan a fallos reales; la combinación de ambas posiciones propone una secuencia metodológica lógica —diagnóstico inicial (saber y hacer), documentación de casos, simulaciones éticas, diseño de intervenciones contextualizadas y evaluación iterativa mediante métricas objetivas (por ejemplo, reducción de clics en simulaciones y mejora en puntuaciones)— que responde a las recomendaciones de ENISA, NIST/NICE y la evidencia empírica sobre la eficacia de intervenciones mixtas, y que permite orientar de manera específica las causas a intervenir en la UDB — campus Soyapango |
| --- |