

<b>Información general</b>			
Facultad: Ingeniería de Sistemas			
Programa académico: Ingeniería de Sistemas		Grupo(s) de investigación: GRIIS	
Nombre del semillero – SEIIS		Fecha creación: 20-abril - 2025	Logo 
		Campus: Bucaramanga	
Líneas de Investigación: Investigación			
Áreas del saber *			
	1. Agronomía veterinaria y afines		5. Ciencias sociales y humanas
	2. Bellas artes		6. Economía, administración, contaduría y afines
X	3. Ciencias de la educación		7. Matemáticas y ciencias naturales
	4. Ciencias de la salud		8. Ingenierías, arquitectura, urbanismo y afines

Al diligenciar este documento autorizo a UNIDADES TECNOLÓGICAS DE SANTANDER, ubicada en Calle de los estudiantes 9-82 Ciudadela Real de Minas y con teléfono de contacto 6076917700, para que recolecte, almacene, use, circule y/o suprima mis datos personales. Lo anterior para dar cumplimiento a las finalidades incorporadas en la Política de Tratamiento de Información disponible en [www.uts.edu.co](http://www.uts.edu.co), la cual declaro conocer y saber que en esta se especifican cuáles datos son sensibles. Así mismo, conozco que como titular me asisten los derechos a conocer, actualizar, rectificar y suprimir mis datos y revocar la autorización. Igualmente declaro que poseo autorización, de los otros titulares de datos que suministro, para que UNIDADES TECNOLÓGICAS DE SANTANDER les dé tratamiento conforme a las finalidades consignadas en la Política.

**Información del Director del Proyecto**

Nombre: Carlos Carrascal Avendaño		No. de identificación y lugar de expedición: 1004942907 de Bucaramanga	
Nivel de formación académica: Magister			Asesor:
		X	Líder de semillero:
Celular: 3146230103		Correo electrónico: calbertocarrascal@correo.uts.edu.co	

**Información de los autores**

Nombre	No. Identificación y lugar de expedición	Celular	Correo electrónico
Jeisy Dayana Jiménez Rincón	1099543992 de Bucaramanga	3185680749	jdayanajimenez@uts.edu.co
Paula Andrea Llanes Rincón Identificación	1116853801 de Bucaramanga	300 6254917	pllanes@uts.edu.co

**Proyecto**

1. Título del proyecto: Análisis del Conocimiento sobre Phishing entre los Estudiantes de las UTS en Bucaramanga: Un Estudio de Concienciación y Prevención de Ciberamenaza	MODALIDAD DEL PROYECTO **				
	PA	PI	TI	RE	Otra. ¿Cuál?
		X			
<p>2. Planteamiento de la problemática:</p> <p>El phishing representa una de las amenazas cibernéticas más comunes y sofisticadas. Se basa en técnicas de engaño para obtener información personal sensible. A pesar de que los estudiantes universitarios usan frecuentemente tecnologías digitales, muchos no poseen conocimientos suficientes para identificar y prevenir ataques de phishing. En Colombia, la ausencia de estrategias educativas robustas en ciberseguridad incrementa esta vulnerabilidad. Según el APWG (2023), los ataques de phishing aumentaron significativamente, y en Colombia se registraron más de 30 millones de incidentes. Esta investigación busca analizar el nivel de conocimiento sobre phishing entre estudiantes de las UTS para proponer estrategias efectivas de prevención.</p> <p>Pregunta problema:</p> <p>¿Cuál es el nivel de conocimiento sobre el phishing entre los estudiantes de las Unidades Tecnológicas de Santander en Bucaramanga?</p>					
<p>3. Antecedentes:</p> <p>Diversos estudios han identificado que el desconocimiento sobre phishing es una constante entre los jóvenes universitarios. Las cifras de ataques han ido en aumento, y las campañas de concienciación no siempre logran su objetivo. A nivel nacional, la Ley 1273 de 2009 y la Ley 1581 de 2012 establecen marcos legales para combatir este tipo de delitos y proteger los datos personales. Sin embargo, se hace necesario fortalecer la educación y prevención desde las instituciones educativas.</p>					
<p>4. Justificación:</p> <p>El proyecto permite detectar vacíos de conocimiento en temas de ciberseguridad entre los estudiantes y propone estrategias para reducir la exposición a amenazas cibernéticas. Prevenir el phishing ayuda a evitar pérdidas financieras y protege la privacidad digital. Además, puede generar un impacto social positivo al capacitar a los estudiantes para ser multiplicadores del conocimiento en sus comunidades.</p>					
<p><b>5. Marcos referenciales:</b></p> <p><b>Marco Teórico:</b></p> <ul style="list-style-type: none"> <li>• Phishing: tipo de ciberataque basado en el engaño para obtener datos sensibles.</li> <li>• Seguridad informática: medidas de protección de datos y sistemas.</li> <li>• Educación en ciberseguridad: herramienta fundamental para mitigar amenazas.</li> </ul> <p><b>Marco Tecnológico:</b></p> <ul style="list-style-type: none"> <li>• Herramientas: Google Forms, Excel, Google Drive, Google Docs.</li> <li>• Recolección y análisis de datos a través de encuestas estructuradas.</li> </ul> <p><b>Marco Legal:</b></p> <ul style="list-style-type: none"> <li>• Ley 1273 de 2009: penaliza accesos no autorizados.</li> <li>• Ley 1581 de 2012: regula el tratamiento de datos personales.</li> </ul>					
<p>6. Objetivo general y objetivos específicos:</p> <p><b>Objetivo General</b></p> <p>Evaluar el nivel de conocimiento sobre phishing entre los estudiantes de las UTS en Bucaramanga para proponer</p>					

estrategias de prevención.

**Objetivos específicos**

- Identificar los conceptos y tipos de phishing conocidos por los estudiantes.
- Determinar la exposición y experiencias previas frente a ataques.
- Analizar los métodos de protección utilizados por los estudiantes.
- Evaluar la eficacia de recursos educativos disponibles sobre phishing.

**7. Metodología:**

Estudio descriptivo con enfoque cuantitativo y método deductivo. La muestra será representativa de estudiantes UTS. Se aplicarán encuestas estructuradas y técnicas de correlación para análisis de resultados.

**8. Avances realizados:**

- Diseño de la encuesta en Google Forms.
- Pruebas piloto con estudiantes para validar comprensión.
- Consolidación de datos preliminares para análisis.
- Revisión de recursos educativos actuales.

**9. Resultados esperados:**

- Diagnóstico del nivel de conocimiento de phishing.
- Identificación de brechas y vacíos informativos.
- Propuestas de campañas de sensibilización.
- Recomendaciones para fortalecer la educación digital en UTS.

**10. Cronograma:**

Actividad	Semana 1	Semana 2	Semana 3	Semana 4	Semana 5	Semana 6
Definición del problema y objetivos	X					
Revisión de literatura y marco teórico	X	X				
Diseño de encuesta (Google Forms)		X				
Aplicación de encuestas			X	X		
Análisis de resultados				X	X	
Propuesta de estrategias y conclusiones					X	X
Socialización de resultados y entrega final						X

**Referencias Bibliográficas**

- Anti-Phishing Working Group (APWG). (2023). Phishing Activity Trends Report. Obtenido de <https://apwg.org/trendsreports/>
- Barbosa, O. E. (2020). PRINCIPIOS DE SEGURIDAD INFORMATICA . Obtenido de <https://repositorio.usam.ac.cr/xmlui/bitstream/handle/11506/2069/LEC%20ING%20SIST%200033%202020.pdf?sequence=1>
- Secretaria general del Senado. (2009). Ley 1273 . Obtenido de [http://www.secretariassenado.gov.co/senado/basedoc/ley\\_1273\\_2009.html](http://www.secretariassenado.gov.co/senado/basedoc/ley_1273_2009.html)
- Smowltech. (2024). Delitos informáticos: en qué consisten y cuántos tipos existen. Obtenido de <https://smowl.net/es/blog/delitos-informaticos/>

- Gutierrez, N. (2024). Estadísticas de Phishing en Latinoamérica. Bogotá: Prey. Obtenido de <https://preyproject.com/es/blog/phishing-en-latinoamerica>

\* Organización para la Cooperación y Desarrollo Económico (OCDE)

\*\* PA: Proyecto de Aula, PI: Proyecto integrador, TI: Trabajo de Investigación, RE: Recursos Educativos Digitales Abiertos (REDA)