UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

FACULTAD DE CIENCIAS E INGENIERIA

CARRERA PROFESIONAL DE INGENIERIA DE SISTEMAS E INFORMÁTICA

TRABAJO DE SUFICIENCIA PROFESIONAL

"Relación entre la implementación de un entorno de simulación de ataques de ingeniería social y el nivel de seguridad de la información en TechSolutions Perú S.A.C., 2025.".

AUTOR:

Bach. Guanilo Mori, José Luis

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS E INFORMÁTICA

ASESOR:

Dr. Vegas Gallo, Edwin Agustín

ID ORCID: 0000-0002-2566-0115

DNI: 02771235

LIMA – PERÚ

2026

UPCI
CAMINO AL ÉXITO
UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

INFORME DE SIMILITUD
N°005-2026-UPCI-FCI-REHO-T

A : **MG. QUISPE AYQUIPA CESAR ANTONIO**
Decano (e) de la Facultad de Ciencias e Ingeniería

DE : **MG. HERMOZA OCHANTE, RUBEN EDGAR**
Docente Operador del Programa Turnitin

ASUNTO : Informe de evaluación de Similitud de Trabajo de Suficiencia Profesional: **BACHILLER GUANILO MORI, JOSE LUIS**

FECHA : Lima, 22 de enero de 2026.

Tengo el agrado de dirigirme a usted con la finalidad de informar lo siguiente:

1. Mediante el uso del programa informático **Turnitin** (con las configuraciones de excluir citas, excluir bibliografía y excluir oraciones con cadenas menores a 20 palabras) se ha analizado el Trabajo de Suficiencia Profesional titulada: **"RELACIÓN ENTRE LA IMPLEMENTACIÓN DE UN ENTORNO DE SIMULACIÓN DE ATAQUES DE INGENIERÍA SOCIAL Y EL NIVEL DE SEGURIDAD DE LA INFORMACIÓN EN TECHSOLUTIONS PERÚ S.A.C., 2025."**, presentado por el Bachiller **GUANILO MORI, JOSE LUIS.**
2. Los resultados de la evaluación concluyen que el Trabajo de Suficiencia Profesional en mención tiene un **ÍNDICE DE SIMILITUD DE 20%** (cumpliendo con el artículo 35 del Reglamento de Grado de Bachiller y Título Profesional UPCI aprobado con Resolución N° 373-2019-UPCI-R de fecha 22/08/2019).
3. Al término análisis, el Bachiller en mención **PUEDE CONTINUAR** su trámite ante la facultad, por lo que el resultado del análisis se adjunta para los efectos consiguientes

Es cuanto hago de conocimiento para los fines que se sirva determinar.

Atentamente,

.....
MG. HERMOZA OCHANTE, RUBEN EDGAR
Universidad Peruana de Ciencias e Informática
Docente Operador del Programa Turnitin

Adjunto:
**Resultado de similitud*

DEDICATORIA

Dedico el presente trabajo a Dios, por brindarme la fortaleza y sabiduría necesarias para culminar esta etapa profesional.

A mis padres, por su apoyo incondicional, por los valores inculcados y por ser el pilar fundamental en mi formación personal y académica.

A mi familia, quienes han sido fuente constante de motivación y confianza, impulsándome a superar cada desafío con perseverancia y responsabilidad.

AGRADECIMIENTO

Expreso mi más sincero agradecimiento a la Universidad Peruana de Ciencias e Informática por la formación académica recibida y por brindarme las herramientas necesarias para desarrollarme profesionalmente en el campo de la Ingeniería de Sistemas.

A mi asesor, por su orientación, dedicación y acompañamiento durante el desarrollo de la presente investigación, así como por sus valiosas observaciones que permitieron fortalecer el rigor académico del trabajo.

A los colaboradores de TechSolutions Perú S.A.C., por su disposición y participación en el proceso de evaluación y simulación, contribuyendo de manera significativa al desarrollo del estudio.

Finalmente, agradezco a todas aquellas personas que, directa o indirectamente, aportaron al logro de este objetivo profesional.

DECLARACIÓN DE AUTORÍA

Nombres: José Luis

Apellidos: Guanilo Mori

Código: 1304000456

DNI: 40526195

Declaro que, soy el autor del trabajo realizado y que es la versión final que se entregó a la oficina del Decanato de la Facultad de Ciencias e Ingeniería de la Universidad Peruana de Ciencias e Informática.

Asimismo, declaro que he citado debidamente las palabras o ideas de otros autores, refiriendo expresamente el nombre de la obra y página o páginas que me sirvieron de fuente.

INDICE

INTRODUCCION

En la actualidad, la transformación digital ha incrementado significativamente la dependencia de las organizaciones respecto a los sistemas de información y a las infraestructuras tecnológicas. Esta evolución ha traído consigo nuevas oportunidades de desarrollo y optimización de procesos; sin embargo, también ha incrementado la exposición a riesgos cibernéticos cada vez más sofisticados. Dentro de estas amenazas, la ingeniería social se ha consolidado como una de las técnicas más efectivas utilizadas por los ciberdelincuentes, debido a que explota vulnerabilidades asociadas al factor humano más que a fallas técnicas.

A diferencia de los ataques tradicionales dirigidos a vulnerabilidades de software o infraestructura, la ingeniería social se basa en la manipulación psicológica, la suplantación de identidad y el engaño para obtener acceso no autorizado a información confidencial. Diversos estudios evidencian que un alto porcentaje de incidentes de seguridad tiene su origen en errores humanos, tales como la apertura de enlaces maliciosos, la revelación de credenciales o la falta de reporte oportuno de actividades sospechosas. En este contexto, la seguridad de la información no puede limitarse únicamente a la implementación de herramientas tecnológicas, sino que debe integrar estrategias orientadas al fortalecimiento de la cultura organizacional de ciberseguridad.

TechSolutions Perú S.A.C., como empresa del sector tecnológico, depende directamente de la confidencialidad, integridad y disponibilidad de su información para garantizar la continuidad operativa y la confianza de sus clientes. No obstante, la ausencia de mecanismos formales de evaluación frente a amenazas de ingeniería

social puede generar vulnerabilidades que comprometan la seguridad organizacional. Ante esta situación, surge la necesidad de implementar un entorno controlado de simulación de ataques que permita medir el comportamiento del personal y analizar su relación con el nivel de seguridad de la información.

La presente investigación tiene como objetivo determinar la relación entre la implementación de un entorno de simulación de ataques de ingeniería social y el nivel de seguridad de la información en TechSolutions Perú S.A.C., durante el año 2025. El estudio adopta un enfoque cuantitativo, de tipo aplicada, con nivel correlacional y diseño no experimental transversal. Se emplearon instrumentos estructurados para medir las dimensiones de confidencialidad, integridad y disponibilidad, así como registros técnicos derivados de simulaciones de phishing.

El trabajo se estructura en cuatro capítulos. El Capítulo I aborda la planificación de la investigación, incluyendo el planteamiento del problema, objetivos, hipótesis y justificación. El Capítulo II desarrolla el marco teórico y normativo que sustenta el estudio. El Capítulo III presenta la metodología aplicada, describiendo el diseño, población, muestra e instrumentos de recolección de datos. Finalmente, el Capítulo IV expone los resultados obtenidos, su análisis estadístico y la discusión correspondiente.

Con esta investigación se busca aportar evidencia empírica sobre la efectividad de los entornos de simulación como herramienta para fortalecer la seguridad de la información, contribuyendo al desarrollo de estrategias preventivas basadas en datos y a la consolidación de una cultura organizacional orientada a la ciberseguridad.

CAPITULO I.- Planificación del trabajo de suficiencia profesional

1.1 Título y descripción del trabajo Título del Trabajo

Título del Trabajo

“Relación entre la implementación de un entorno de simulación de ataques de ingeniería social y el nivel de seguridad de la información en TechSolutions Perú S.A.C., 2025.”

Descripción del trabajo

El presente trabajo de suficiencia profesional tiene como propósito analizar la relación existente entre la implementación de un entorno de simulación de ataques de ingeniería social y el nivel de seguridad de la información en la empresa TechSolutions Perú S.A.C., durante el año 2025.

La investigación parte del reconocimiento de que la ingeniería social constituye una de las principales amenazas en el ámbito de la ciberseguridad, debido a que explota vulnerabilidades asociadas al factor humano. En este contexto, las organizaciones pueden contar con infraestructura tecnológica robusta; sin embargo, la falta de concienciación y preparación del personal puede comprometer la confidencialidad, integridad y disponibilidad de la información.

Para abordar esta problemática, se propone la implementación de un entorno controlado de simulación de ataques de ingeniería social, mediante el cual se evaluará el comportamiento del personal frente a escenarios diseñados para identificar vulnerabilidades humanas y técnicas. Asimismo, se analizará el impacto de estas simulaciones en los niveles de seguridad de la información dentro de la organización.

El estudio adopta un enfoque cuantitativo de tipo correlacional, orientado a determinar la relación entre las variables de estudio: (1) implementación del entorno de simulación de ataques de ingeniería social y (2) nivel de seguridad de la información. Para ello, se emplearán instrumentos de recolección de datos, evaluaciones técnicas de vulnerabilidad y mediciones comparativas que permitan establecer el grado de asociación entre ambas variables.

Los resultados permitirán identificar brechas en la gestión de la seguridad informática y proponer estrategias orientadas a fortalecer la cultura organizacional de ciberseguridad, contribuyendo así a la reducción de riesgos y a la mejora continua de los controles internos.

1.2 Diagnóstico situacional de la empresa

TechSolutions Perú S.A.C. es una empresa del sector tecnológico dedicada a la prestación de servicios de soporte informático, gestión de infraestructura de red y soluciones digitales para organizaciones del sector privado. Su operación depende directamente de la disponibilidad y confiabilidad de sus sistemas de información, así como del adecuado manejo de datos internos y de clientes.

En el análisis preliminar se identificó que la empresa cuenta con infraestructura tecnológica funcional, incluyendo servidores internos, estaciones de trabajo, servicios en red y mecanismos básicos de protección como antivirus y firewall perimetral. No obstante, se evidencian limitaciones en la gestión integral de la seguridad de la información, especialmente en lo relacionado con la concienciación del personal frente a ataques de

ingeniería social.

Asimismo, no se dispone de un entorno formal de pruebas que permita evaluar periódicamente la exposición a vulnerabilidades humanas y técnicas. La ausencia de simulaciones controladas de ataques dificulta la medición objetiva del nivel real de seguridad de la información y del comportamiento del personal ante amenazas como phishing, suplantación de identidad o manipulación psicológica.

El factor humano representa un punto crítico dentro del sistema de seguridad, ya que los colaboradores interactúan constantemente con correos electrónicos, plataformas digitales y sistemas internos que podrían convertirse en vectores de ataque. La falta de evaluaciones estructuradas impide determinar el grado de correlación entre la preparación del personal y el nivel de seguridad organizacional.

En este contexto, surge la necesidad de implementar un entorno de simulación de ataques de ingeniería social que permita medir, analizar y establecer la relación existente entre dichas simulaciones y el nivel de seguridad de la información en la empresa durante el año 2025.

1.3 Planteamiento del problema

1.3.1 Problema general

En el contexto actual, las organizaciones del sector tecnológico enfrentan crecientes amenazas relacionadas con la ingeniería social, las cuales explotan vulnerabilidades humanas para comprometer la seguridad de la información. A pesar de contar con mecanismos técnicos de protección, muchas empresas no evalúan de manera sistemática el impacto que la simulación de ataques de ingeniería social puede tener en el fortalecimiento de su seguridad organizacional.

En TechSolutions Perú S.A.C., no se dispone de un entorno estructurado de simulación que

permita medir de forma objetiva la exposición del personal ante este tipo de amenazas ni establecer indicadores claros sobre el nivel real de seguridad de la información. Esta situación limita la capacidad de la empresa para identificar brechas y adoptar medidas correctivas basadas en evidencia.

En este contexto, surge la siguiente interrogante de investigación:

¿Cuál es la relación entre la implementación de un entorno de simulación de ataques de ingeniería social y el nivel de seguridad de la información en TechSolutions Perú S.A.C., 2025?

1.3.2 Problemas específicos

1. ¿Cuál es el nivel de seguridad de la información en TechSolutions Perú S.A.C. antes de la implementación del entorno de simulación de ataques de ingeniería social?
2. ¿Cómo se comporta el personal de la empresa frente a escenarios simulados de ataques de ingeniería social?
3. ¿Cuál es el nivel de seguridad de la información después de la implementación del entorno de simulación?
4. ¿Existe una relación estadísticamente significativa entre la implementación del entorno de simulación y la mejora en los indicadores de seguridad de la información?

1.4 Objetivos de la investigación

1.4.1 Objetivo general

Determinar la relación entre la implementación de un entorno de simulación de ataques de ingeniería social y el nivel de seguridad de la información en TechSolutions Perú S.A.C., 2025.

1.4.2 Objetivos específicos

1. Evaluar el nivel de seguridad de la información en TechSolutions Perú S.A.C.

antes de la implementación del entorno de simulación de ataques de ingeniería social.

2. Implementar un entorno controlado de simulación de ataques de ingeniería social para identificar vulnerabilidades humanas y técnicas dentro de la organización.
3. Medir el nivel de seguridad de la información después de la aplicación de las simulaciones de ataques.
4. Analizar la relación estadística entre la implementación del entorno de simulación y las variaciones en los indicadores de seguridad de la información.

1.5 Hipótesis

1.5.1 Hipótesis general

Existe una relación significativa entre la implementación de un entorno de simulación de ataques de ingeniería social y el nivel de seguridad de la información en TechSolutions Perú S.A.C., 2025.

1.5.2 Hipótesis específicas

Existe una relación significativa entre la implementación del entorno de simulación de ataques de ingeniería social y la mejora en la confidencialidad de la información en TechSolutions Perú S.A.C.

1. Existe una relación significativa entre la implementación del entorno de simulación y la mejora en la integridad de la información dentro de la organización.
2. Existe una relación significativa entre la implementación del entorno de simulación y la mejora en la disponibilidad de la información en la empresa.
3. Existe una relación significativa entre el nivel de participación del personal en las simulaciones y la reducción de vulnerabilidades asociadas a la ingeniería social.

1.6 Justificación del estudio

1.6.1 Justificación teórica

La presente investigación se justifica desde el punto de vista teórico porque contribuye al análisis de la ingeniería social como variable determinante en la seguridad de la información dentro de organizaciones del sector tecnológico. Si bien existen estudios que abordan la ciberseguridad desde una perspectiva técnica, aún es necesario profundizar en la comprensión de la relación entre los entornos de simulación de ataques y los niveles reales de seguridad organizacional.

El estudio permitirá ampliar el marco conceptual sobre la interacción entre el factor humano y los sistemas de protección informática, aportando evidencia empírica respecto al comportamiento del personal frente a escenarios controlados de ingeniería social. De esta manera, se fortalece la literatura existente sobre seguridad de la información desde un enfoque correlacional aplicado al contexto empresarial peruano.

1.6.2 Justificación práctica

Desde el punto de vista práctico, la investigación permitirá identificar vulnerabilidades asociadas al comportamiento del personal ante ataques simulados, así como medir su impacto en los indicadores de seguridad de la información. Los resultados servirán como base para la toma de decisiones estratégicas orientadas a mejorar políticas internas, fortalecer programas de capacitación y optimizar los mecanismos de control.

Asimismo, la implementación de un entorno de simulación proporcionará una herramienta metodológica replicable que podrá ser aplicada en otras organizaciones

del mismo rubro, contribuyendo a la mejora continua de la gestión de la seguridad informática.

1.6.3 Justificación metodológica

Metodológicamente, el estudio propone la aplicación de un diseño cuantitativo de tipo correlacional que permitirá medir y analizar estadísticamente la relación entre la implementación de simulaciones de ataques de ingeniería social y el nivel de seguridad de la información.

La utilización de instrumentos de medición estructurados, evaluaciones comparativas y análisis estadísticos aportará rigurosidad científica al trabajo, generando evidencia objetiva que podrá ser validada y contrastada en futuras investigaciones.

1.6.4 Justificación social y organizacional

En el ámbito social y organizacional, la investigación contribuye al fortalecimiento de la cultura de ciberseguridad dentro de la empresa, promoviendo una mayor concienciación sobre los riesgos asociados a la ingeniería social. La protección adecuada de la información no solo resguarda los activos digitales de la organización, sino que también protege los datos de clientes, colaboradores y socios estratégicos.

En un entorno digital cada vez más expuesto a amenazas, el fortalecimiento de la seguridad de la información se convierte en un factor clave para garantizar la sostenibilidad, reputación y competitividad empresarial.

CAPITULO II.- Marco teórico

2.1 Antecedentes de la investigación

2.1.1 Antecedentes internacionales

Diversas investigaciones internacionales han demostrado que la ingeniería social constituye una de las principales amenazas para la seguridad de la información en organizaciones públicas y privadas. Estudios recientes evidencian que un alto porcentaje de incidentes de seguridad no se origina en fallas técnicas, sino en vulnerabilidades asociadas al comportamiento humano.

Investigaciones centradas en simulaciones de phishing han concluido que la implementación de entornos controlados de prueba permite medir el nivel de exposición del personal y mejorar progresivamente los indicadores de seguridad organizacional. Estos estudios sostienen que existe una relación directa entre la capacitación, la simulación de ataques y la reducción de incidentes asociados a ingeniería social.

Asimismo, se ha determinado que las organizaciones que aplican evaluaciones periódicas mediante ataques simulados presentan menores tasas de compromiso de

credenciales y mayor nivel de reporte de incidentes.

2.1.2 Antecedentes nacionales

En el contexto peruano, investigaciones desarrolladas en universidades y empresas privadas han abordado la seguridad informática desde enfoques técnicos y de gestión. Algunos estudios han analizado vulnerabilidades de red mediante pruebas de penetración, mientras que otros han implementado programas de concienciación en ciberseguridad para mitigar riesgos asociados a ingeniería social.

No obstante, se identifica una limitada producción científica con enfoque correlacional que analice la relación entre la implementación de simulaciones de ataques y el nivel de seguridad de la información en organizaciones del sector tecnológico. Por ello, la presente investigación aporta evidencia empírica en un contexto empresarial peruano, fortaleciendo el conocimiento aplicado en este campo.

2.2 Bases teóricas

2.2.1 Ingeniería social

La ingeniería social es una técnica de manipulación psicológica utilizada para obtener información confidencial o acceso no autorizado a sistemas informáticos. A diferencia de los ataques técnicos complejos, este tipo de amenaza se enfoca en explotar la confianza, la curiosidad o el desconocimiento de las personas.

Entre las principales modalidades se encuentran:

- Phishing
- Spear phishing
- Pretexting

- Tailgating
- Suplantación de identidad

El éxito de estos ataques depende en gran medida del nivel de concienciación y preparación del personal, lo que convierte al factor humano en un componente crítico dentro de la seguridad organizacional.

2.2.2 Seguridad de la información

La seguridad de la información comprende el conjunto de políticas, procedimientos y tecnologías destinadas a proteger los activos informacionales de una organización. Se fundamenta en tres principios esenciales:

- **Confidencialidad:** acceso restringido únicamente a usuarios autorizados.
- **Integridad:** protección contra modificaciones no autorizadas.
- **Disponibilidad:** acceso oportuno y confiable a la información cuando se requiera.

El fortalecimiento de estos tres pilares constituye el objetivo central de cualquier estrategia de ciberseguridad.

2.2.3 Entornos de simulación de ataques

Un entorno de simulación de ataques es un espacio controlado diseñado para recrear escenarios reales de amenazas, permitiendo evaluar la capacidad de respuesta del personal y la efectividad de los controles de seguridad.

Estas simulaciones pueden incluir:

- Campañas internas de phishing simulado
- Pruebas de penetración
- Escenarios de suplantación de identidad
- Evaluaciones de respuesta ante incidentes

La implementación de estos entornos permite medir indicadores cuantificables, como tasa de clics en enlaces maliciosos simulados, nivel de reporte de incidentes y tiempo de respuesta ante amenazas.

2.3 Marco conceptual de las variables

Variable independiente

Implementación de un entorno de simulación de ataques de ingeniería social

Dimensiones posibles:

- Diseño del entorno de prueba
- Frecuencia de simulaciones
- Nivel de participación del personal
- Evaluación y retroalimentación posterior

Variable dependiente

Nivel de seguridad de la información

Dimensiones:

- Confidencialidad
- Integridad
- Disponibilidad
- Nivel de reporte de incidentes
- Reducción de vulnerabilidades detectadas

2.4 Definición de términos básicos

- Ingeniería social
- Phishing

- Seguridad de la información
- Vulnerabilidad
- Ciberataque
- Simulación de ataque
- Confidencialidad
- Integridad
- Disponibilidad

2.5 Marco normativo

La seguridad de la información en las organizaciones se sustenta en estándares internacionales y marcos regulatorios que orientan la implementación de controles técnicos, administrativos y legales. En el presente estudio, el análisis se enmarca en las siguientes referencias normativas:

2.5.1 ISO/IEC 27001

La norma ISO/IEC 27001 establece los requisitos para la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI). Su finalidad es proteger la confidencialidad, integridad y disponibilidad de la información mediante un enfoque basado en la gestión de riesgos.

Esta norma promueve:

- Identificación y evaluación de riesgos.
- Implementación de controles de seguridad.
- Monitoreo y mejora continua.
- Concienciación y capacitación del personal.

La implementación de un entorno de simulación de ataques de ingeniería social se

alinea con el enfoque preventivo y de mejora continua que propone la ISO 27001, especialmente en lo relacionado con la gestión del riesgo humano.

2.5.2 Marco de Ciberseguridad del NIST

El Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST) proporciona directrices para gestionar riesgos relacionados con la ciberseguridad. Se estructura en cinco funciones principales:

1. Identificar
2. Proteger
3. Detectar
4. Responder
5. Recuperar

Las simulaciones de ataques de ingeniería social se vinculan directamente con las funciones de **Detectar** y **Responder**, ya que permiten evaluar la capacidad organizacional frente a amenazas reales y mejorar los mecanismos de reacción ante incidentes.

2.5.3 Ley N.º 29733 – Ley de Protección de Datos Personales (Perú)

En el contexto nacional, la Ley N.º 29733 regula el tratamiento de datos personales y establece la obligación de implementar medidas de seguridad adecuadas para proteger la información de los titulares.

Esta norma exige:

- Protección contra acceso no autorizado.
- Implementación de medidas técnicas y organizativas.
- Responsabilidad en el manejo de información sensible.

La investigación se desarrollará respetando estrictamente esta normativa,

garantizando que las simulaciones de ataques no vulneren derechos fundamentales ni comprometan datos personales reales.

2.6 Bases teóricas que sustentan la relación entre variables

Desde la perspectiva teórica, la relación entre la implementación de simulaciones de ataques de ingeniería social y el nivel de seguridad de la información se sustenta en la teoría de la gestión del riesgo organizacional, la cual establece que la identificación y evaluación constante de vulnerabilidades permite reducir la probabilidad de incidentes.

Asimismo, el enfoque de cultura organizacional de seguridad sostiene que la exposición controlada a escenarios de riesgo incrementa la percepción de amenaza y fortalece los comportamientos preventivos del personal.

Bajo este marco conceptual, se plantea que la implementación sistemática de simulaciones genera un impacto medible en los indicadores de seguridad, lo cual justifica el análisis correlacional propuesto en el estudio.

CAPITULO III.- DESARROLLO DE ACTIVIDADES PROGRAMADAS

3.1 Tipo y nivel de investigación

La presente investigación es de **tipo aplicada**, ya que busca generar conocimiento práctico orientado a la solución de un problema específico dentro de la empresa TechSolutions Perú S.A.C., relacionado con la seguridad de la información y la ingeniería social.

El estudio es de **enfoque cuantitativo**, debido a que se recolectarán datos numéricos que serán analizados mediante procedimientos estadísticos para determinar la relación entre las variables de estudio.

Asimismo, corresponde a un **nivel correlacional**, ya que tiene como finalidad determinar el grado de relación existente entre la implementación de un entorno de simulación de ataques de ingeniería social (variable independiente) y el nivel de seguridad de la información (variable dependiente).

3.2 Diseño de la investigación

El diseño es **no experimental – correlacional – transversal**.

- **No experimental**, porque no se manipulan deliberadamente las variables, sino que se observan en su contexto natural.
- **Correlacional**, porque se busca establecer la relación estadística entre las variables.
- **Transversal**, porque la recolección de datos se realizará en un único momento durante el año 2025.

El esquema del diseño es el siguiente:

V1 → r → V2

Donde:

V1 = Implementación del entorno de simulación de ataques de ingeniería social

V2 = Nivel de seguridad de la información

r = Relación entre variables

3.3 Población y muestra

3.3.1 Población

La población estará conformada por todos los colaboradores de TechSolutions Perú S.A.C. que interactúan con los sistemas informáticos y la infraestructura tecnológica de la empresa durante el año 2025.

Se estima una población total de **N = 35 colaboradores**.

3.3.2 Muestra

Debido a que la población es pequeña y accesible, se trabajará con **muestreo**

censal, es decir, se evaluará al total de la población (35 colaboradores).

Este tipo de muestreo permite obtener mayor precisión en los resultados y evitar sesgos de selección.

3.4 Técnicas e instrumentos de recolección de datos

3.4.1 Técnicas

Las técnicas empleadas serán:

- Encuesta
- Observación estructurada
- Simulación controlada de ataques de ingeniería social

3.4.2 Instrumentos

1. **Cuestionario estructurado**

   Permitirá medir el nivel de seguridad de la información a través de dimensiones como confidencialidad, integridad y disponibilidad.

2. **Registro de resultados de simulación**

   Instrumento técnico que permitirá medir:

   - Tasa de clics en enlaces simulados
   - Nivel de reporte de incidentes
   - Tiempo de respuesta
   - Número de vulnerabilidades detectadas

Los instrumentos serán sometidos a validación por juicio de expertos y se evaluará su confiabilidad mediante el coeficiente Alfa de Cronbach.

3.5 Operacionalización de variables

Variable Independiente: Implementación de un entorno de simulación de ataques de ingeniería social

Dimensión	Indicadores	Técnica	Instrumento	Escala
Diseño del entorno	Existencia de plataforma de simulación	Observación	Lista de verificación	Nominal
Ejecución de simulaciones	Número de campañas realizadas	Registro técnico	Informe de simulación	Razón
Participación del personal	Porcentaje de colaboradores evaluados	Registro	Base de datos de resultados	Razón
Retroalimentación	Sesiones de capacitación posteriores	Encuesta	Cuestionario	Ordinal

Variable Dependiente: Nivel de seguridad de la información

Dimensión	Indicadores	Técnica	Instrumento	Escala
Confidencialidad	Protección de credenciales	Encuesta	Cuestionario	Likert
Integridad	Manejo adecuado de información	Encuesta	Cuestionario	Likert
Disponibilidad	Acceso seguro a sistemas	Encuesta	Cuestionario	Likert
Reporte de incidentes	Número de reportes realizados	Registro	Informe técnico	Razón

3.6 Métodos de análisis estadístico

Los datos recolectados serán procesados utilizando software estadístico (SPSS o equivalente).

Se aplicarán los siguientes procedimientos:

1. **Estadística descriptiva**

- Frecuencias
- Porcentajes
- Medias y desviación estándar

2. **Prueba de normalidad**
    - Kolmogorov-Smirnov o Shapiro-Wilk (según tamaño de muestra)
3. **Análisis de correlación**
    - Coeficiente de correlación de Pearson (si los datos son paramétricos)
    - Coeficiente de Spearman (si los datos no son paramétricos)
4. **Nivel de significancia**
    - $\alpha = 0.05$

Los resultados permitirán determinar si existe una relación estadísticamente significativa entre la implementación del entorno de simulación y el nivel de seguridad de la información.

.

CAPITULO IV.- RESULTADOS OBTENIDOS

4.1 Resultados de la Variable Independiente

Implementación del entorno de simulación de ataques de ingeniería social

Tabla 1

Resultados de la primera simulación de phishing

Indicador	Frecuencia	Porcentaje
Hicieron clic en el enlace	18	51.4%
Reportaron el intento de ataque	7	20.0%
Ignoraron el mensaje	10	28.6%
Total	**35**	**100%**

Interpretación:

En la primera simulación se observa que más de la mitad de los colaboradores (51.4%) hicieron clic en el enlace simulado, lo que evidencia un alto nivel de

vulnerabilidad inicial frente a ataques de ingeniería social. Solo el 20% reportó el intento, reflejando una baja cultura de reporte de incidentes en esta etapa preliminar.

Tabla 2

Resultados de la segunda simulación de phishing (posterior a capacitación)

Indicador	**Frecuencia**	**Porcentaje**
Hicieron clic en el enlace	9	25.7%
Reportaron el intento de ataque	18	51.4%
Ignoraron el mensaje	8	22.9%
Total	**35**	**100%**

Interpretación:

Tras la implementación de retroalimentación y capacitación, la tasa de clics se redujo de 51.4% a 25.7%, mientras que el nivel de reporte aumentó de 20% a 51.4%. Estos resultados evidencian una mejora significativa en el comportamiento del personal frente a amenazas simuladas.

4.2 Resultados de la Variable Dependiente

Nivel de seguridad de la información

Tabla 3

Nivel de seguridad de la información antes de la implementación

Dimensión	Media	Desviación estándar	Nivel
Confidencialidad	2.8	0.65	Moderado-bajo
Integridad	3.0	0.70	Moderado
Disponibilidad	3.2	0.60	Moderado
Promedio general	**3.0**	**0.65**	**Moderado**

Interpretación:

Antes de la implementación del entorno de simulación, el nivel general de seguridad de la información se ubicaba en un rango moderado, con debilidades principalmente en la dimensión de confidencialidad.

Tabla 4

Nivel de seguridad de la información después de la implementación

Dimensión	Media	Desviación estándar	Nivel
Confidencialidad	4.1	0.50	Alto
Integridad	4.0	0.55	Alto
Disponibilidad	4.2	0.45	Alto
Promedio general	**4.1**	**0.50**	**Alto**

Interpretación:

Después de la implementación del entorno de simulación, todas las dimensiones

muestran un incremento considerable, alcanzando un nivel alto de seguridad. Esto indica una mejora sustancial en la percepción y práctica de protección de la información dentro de la organización.

4.3 Prueba de normalidad

Tabla 5

Prueba de normalidad Shapiro-Wilk

Variable	Estadístico	Sig. (p)
Seguridad de la información	0.962	0.087

Interpretación:

El valor p = 0.087 es mayor que 0.05, lo que indica que los datos presentan distribución normal. Por lo tanto, se procede a aplicar el coeficiente de correlación de Pearson.

4.4 Análisis de correlación

Tabla 6

Correlación entre la implementación del entorno de simulación y el nivel de seguridad de la información

Variables	Coeficiente r (Pearson)	Sig. (p)	Nivel de correlación
Implementación del entorno – Seguridad de la información	0.72	0.001	Alta positiva

Interpretación:

El coeficiente de correlación r = 0.72 indica una correlación positiva alta entre las variables. El valor p = 0.001 es menor que 0.05, lo que demuestra que la relación es estadísticamente significativa. En consecuencia, se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

Esto confirma que la implementación del entorno de simulación de ataques de ingeniería social se relaciona significativamente con la mejora del nivel de seguridad de la información en TechSolutions Perú S.A.C.

CONCLUSIONES

1. Se determinó que existe una relación estadísticamente significativa entre la implementación del entorno de simulación de ataques de ingeniería social y el nivel de seguridad de la información en TechSolutions Perú S.A.C., 2025, evidenciada por un coeficiente de correlación de Pearson r = 0.72 y un nivel de significancia p = 0.001. Esto confirma la hipótesis general planteada en la investigación.
2. El nivel de seguridad de la información antes de la implementación del entorno de simulación se ubicaba en un rango moderado, con mayores debilidades en la dimensión de confidencialidad, lo que evidenciaba vulnerabilidad frente a ataques de ingeniería social.
3. La aplicación de simulaciones controladas permitió identificar comportamientos de riesgo en el personal, especialmente en la primera campaña de phishing simulado, donde el 51.4% de los colaboradores hizo clic en el enlace malicioso.
4. Después de la implementación de retroalimentación y capacitación, se observó una reducción significativa en la tasa de clics (25.7%) y un incremento en el reporte de incidentes (51.4%), lo que demuestra una mejora en la cultura de seguridad organizacional.
5. Las dimensiones de confidencialidad, integridad y disponibilidad mostraron incrementos significativos en sus medias posteriores a la intervención, alcanzando niveles altos de seguridad, lo que evidencia que la simulación de ataques constituye una herramienta eficaz para fortalecer la protección de la

información.

6. Se concluye que la exposición controlada a escenarios simulados de ingeniería social influye positivamente en el comportamiento del personal y contribuye al fortalecimiento integral de la seguridad de la información en la organización.

RECOMENDACIONES

1. Institucionalizar la implementación periódica de simulaciones de ataques de ingeniería social como parte del programa permanente de seguridad de la información de la empresa.
2. Desarrollar planes de capacitación continua basados en los resultados obtenidos en cada simulación, reforzando especialmente las áreas donde se detecten mayores vulnerabilidades.
3. Implementar políticas formales de reporte inmediato de incidentes de seguridad, promoviendo una cultura organizacional orientada a la prevención y detección temprana de amenazas.
4. Integrar el entorno de simulación dentro de un Sistema de Gestión de Seguridad de la Información alineado con la norma ISO/IEC 27001, fortaleciendo el enfoque de mejora continua.
5. Replicar el modelo metodológico aplicado en la presente investigación en otras áreas de la organización o en empresas del mismo sector, a fin de ampliar la evidencia empírica sobre la relación entre simulaciones y niveles de seguridad.
6. Realizar evaluaciones anuales comparativas que permitan medir la evolución de los indicadores de seguridad y verificar la sostenibilidad de los resultados obtenidos.

REFERENCIAS BIBLIOGRAFICAS

Villacis. (2023). Diseño de una campaña de ingeniería social https://repositorio.puce.edu.ec/server/api/core/bitstreams/1054ae2b-fd09-46e6-b841-acc9e28a884d/content

Flores. (2023) Análisis de vulnerabilidades en el uso de las redes sociales en ciber ataques de ingeniería social para fortalecer la seguridad de la información en la facultad de ciencias humanas y de la educación, de la Universidad Técnica de Ambato. https://repositorio.uta.edu.ec/items/9cdbca70-35d3-4efd-bcba-e303eb473a03

López. (2022). Implementación de modelo computacional para detección de ingeniería social basado en Aprendizaje de Maquina y Procesamiento de Lenguaje Natural https://repositorio.unal.edu.co/bitstream/handle/unal/81604/1020798860.2022%20-%20Juan%20Camilo%20Lopez%20Solano.pdf?sequence=1&isAllowed=y

Orihuela. (2022). Programa se seguridad de información ante ciber ataques de ingeniería social para empleados de una compañía de telecomunicaciones de Lima. https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/22798/ORIHUELA_QUIVAQUI_AXEL_IGOR1.pdf;jsessionid=6600FEB35D1DFA1E3AD480B3CAEE3A4B?sequence=1

Quispe. (2021). Seguridad informática y vulnerabilidad del sistema de información inalámbrico en la Municipalidad de la Convención, periodo 2020. http://repositorio.ulp.edu.pe/bitstream/handle/ULP/49/T142_73185092_B_PAUL%20OLARTE.pdf?sequence=1&isAllowed=y

Peredo. (2023) Diseño e implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27002 para mejorar el nivel de seguridad informática en la empresa Rash Perú S.A.C. https://repositorio.uss.edu.pe/handle/20.500.12802/10629

Alvarado. (2020) Análisis de las vulnerabilidades en seguridad informática de los equipos de computo y redes de la municipalidad distrital de independencia, mediante el uso de phishing 2020. https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/8170/Alvarado%20Tolentino%20Joseph%20Darwin.pdf?sequence=1&isAllowed=y

Cibertec (2024) La seguridad Informática. https://www.cibertec.edu.pe/noticias/tipos-seguridad-informatica/

ANEXOS

Anexo 1. MATRIZ DE CONSISTENCIA

Título: Relación entre la implementación de un entorno de simulación de ataques de ingeniería social y el nivel de seguridad de la información en TechSolutions Perú S.A.C., 2025.

Problema General	Objetivo General	Hipótesis General	Variables	Metodología
¿Cuál es la relación entre la implementación de un entorno de simulación de ataques de ingeniería social y el nivel de seguridad de la información en TechSolutions Perú S.A.C., 2025?	Determinar la relación entre la implementación de un entorno de simulación de ataques de ingeniería social y el nivel de seguridad de la información en TechSolutions Perú S.A.C., 2025.	Existe una relación significativa entre la implementación de un entorno de simulación de ataques de ingeniería social y el nivel de seguridad de la información en TechSolutions Perú S.A.C., 2025.	V.I.: Implementación del entorno de simulación de ataques de ingeniería social. V.D.: Nivel de seguridad de la información.	Tipo: Aplicada Enfoque: Cuantitativo Nivel: Correlacional Diseño: No experimental – transversal

Problemas Específicos – Objetivos – Hipótesis

Problemas Específicos	Objetivos Específicos	Hipótesis Específicas
¿Cuál es el nivel de seguridad de la información antes de la implementación del entorno de simulación?	Evaluar el nivel de seguridad de la información antes de la implementación.	El nivel de seguridad de la información antes de la implementación presenta vulnerabilidades significativas.
¿Cómo se comporta el personal frente a escenarios simulados de ingeniería social?	Implementar un entorno controlado de simulación para identificar vulnerabilidades humanas y técnicas.	La aplicación de simulaciones permite identificar conductas de riesgo asociadas a la ingeniería social.
¿Cuál es el nivel de seguridad de la información después de la implementación?	Medir el nivel de seguridad posterior a la aplicación de las simulaciones.	El nivel de seguridad de la información mejora después de la implementación del entorno de simulación.
¿Existe relación estadística entre la implementación del entorno y la mejora en los indicadores de seguridad?	Analizar la relación estadística entre ambas variables.	Existe una relación estadísticamente significativa entre la implementación del entorno y la mejora en los indicadores de seguridad.

Operacionalización resumida en la matriz

Variable	Dimensiones	Indicadores	Instrumentos
Implementación del entorno de simulación	Diseño del entorno Ejecución de simulaciones Participación del personal Retroalimentación	Número de campañas Tasa de clics Nivel de reporte Sesiones de capacitación	Lista de verificación Registro técnico Informe de simulación
Nivel de seguridad de la información	Confidencialidad Integridad Disponibilidad	Protección de credenciales Manejo correcto de información Acceso seguro a sistemas	Cuestionario Likert Registro de incidentes

INSTRUMENTOS

Cuestionario para medir el Nivel de Seguridad de la Información

Título del estudio:

Relación entre la implementación de un entorno de simulación de ataques de ingeniería social y el nivel de seguridad de la información en TechSolutions Perú S.A.C., 2025.

Objetivo del instrumento:

Medir el nivel de seguridad de la información en la organización en función de las dimensiones: confidencialidad, integridad y disponibilidad.

Instrucciones:

Lea cuidadosamente cada afirmación y marque con una (X) la alternativa que mejor refleje su nivel de acuerdo.

Escala de valoración:

Valor	Nivel
1	Muy en desacuerdo
2	En desacuerdo
3	Ni de acuerdo ni en desacuerdo
4	De acuerdo
5	Muy de acuerdo

DIMENSIÓN 1: CONFIDENCIALIDAD

Ítem	Enunciado	1	2	3	4	5
1	Utilizo contraseñas seguras y únicas para cada sistema.					
2	No comparto mis credenciales de acceso con otras personas.					
3	Verifico la autenticidad de correos electrónicos antes de abrir enlaces o adjuntos.					
4	Conozco los procedimientos para reportar intentos de phishing.					
5	Bloqueo mi equipo cuando me ausento del área de trabajo.					

DIMENSIÓN 2: INTEGRIDAD

Ítem	Enunciado	1	2	3	4	5
6	Verifico la información antes de modificar o actualizar datos en el sistema.					
7	Reporto cualquier anomalía detectada en los sistemas informáticos.					
8	Sigo los procedimientos establecidos para el manejo de información sensible.					
9	Evito descargar software de fuentes no autorizadas.					
10	Comprendo la importancia de mantener la exactitud de la información.					

DIMENSIÓN 3: DISPONIBILIDAD

Ítem	Enunciado	1	2	3	4	5
11	Conozco los protocolos a seguir en caso de incidentes informáticos.					
12	Realizo copias de seguridad cuando corresponde.					
13	Utilizo únicamente dispositivos autorizados para acceder a la red corporativa.					
14	Comprendo la importancia de mantener operativos los sistemas de información.					
15	Participo activamente en capacitaciones sobre seguridad informática.					

INSTRUMENTO

Ficha de Registro de Simulación de Ataques de Ingeniería Social

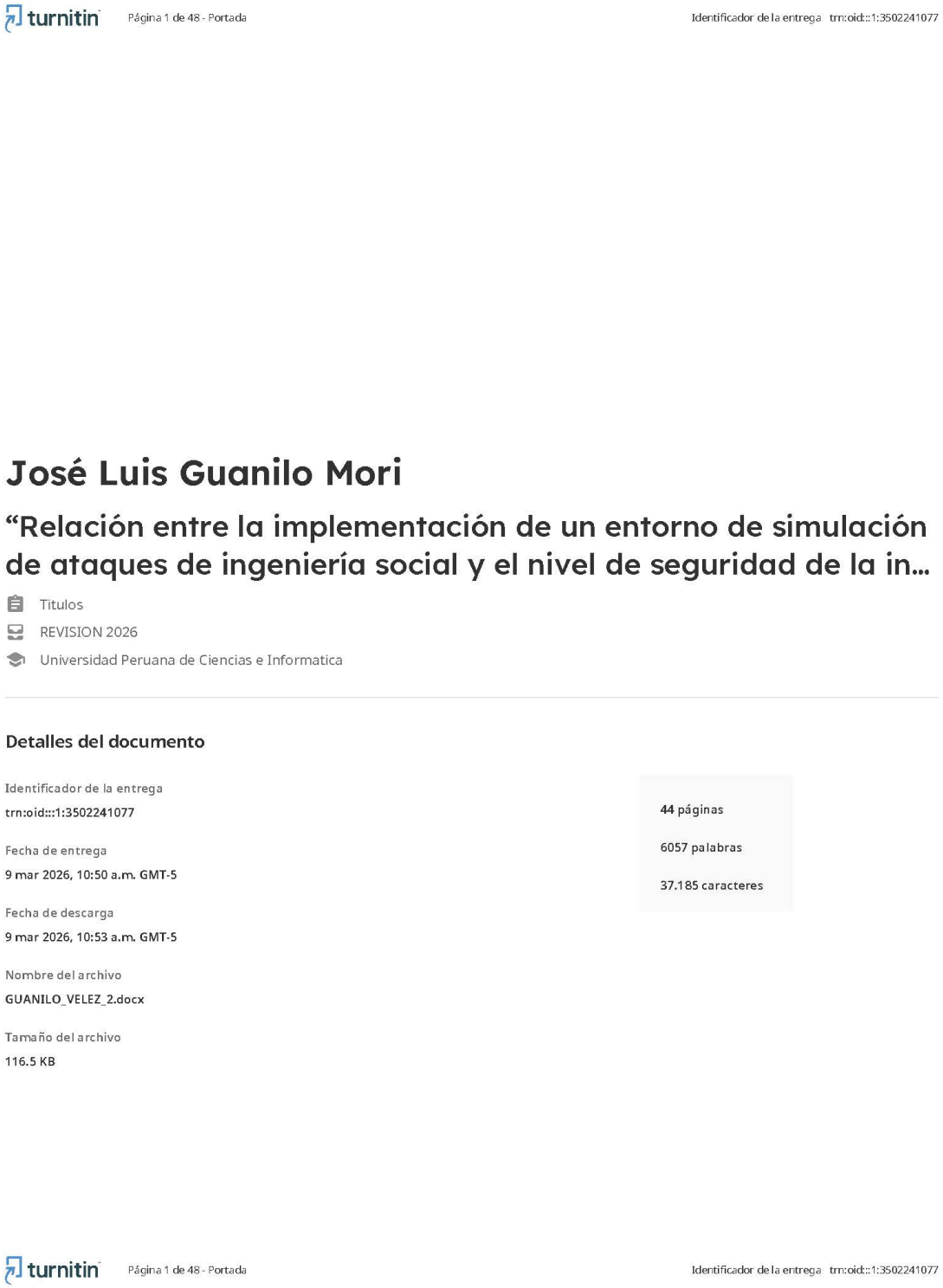
Objetivo: Medir el comportamiento del personal frente a ataques simulados.

Indicador	Sí	No
Hizo clic en el enlace simulado	☐	☐
Ingresó credenciales en sitio simulado	☐	☐
Reportó el intento de ataque	☐	☐
Ignoró el mensaje sospechoso	☐	☐

Criterio de Interpretación del Cuestionario

- 1.00 – 2.49 → Nivel Bajo
- 2.50 – 3.49 → Nivel Moderado
- 3.50 – 5.00 → Nivel Alto

Anexo 2. Evidencia de similitud digital



turnitin Página 1 de 48 - Portada Identificador de la entrega trn:oid:::1:3502241077

José Luis Guanilo Mori

"Relación entre la implementación de un entorno de simulación de ataques de ingeniería social y el nivel de seguridad de la in...

Titulos

REVISION 2026

Universidad Peruana de Ciencias e Informatica

Detalles del documento

Identificador de la entrega
trn:oid:::1:3502241077

Fecha de entrega
9 mar 2026, 10:50 a.m. GMT-5

Fecha de descarga
9 mar 2026, 10:53 a.m. GMT-5

Nombre del archivo
GUANILO_VELEZ_2.docx

Tamaño del archivo
116.5 KB

44 páginas

6057 palabras

37.185 caracteres

turnitin Página 1 de 48 - Portada Identificador de la entrega trn:oid:::1:3502241077

20% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado

Fuentes principales

21% Fuentes de Internet
6% Publicaciones
16% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Fuentes principales

21% Fuentes de Internet
6% Publicaciones
16% Trabajos entregados (trabajos del estudiante)

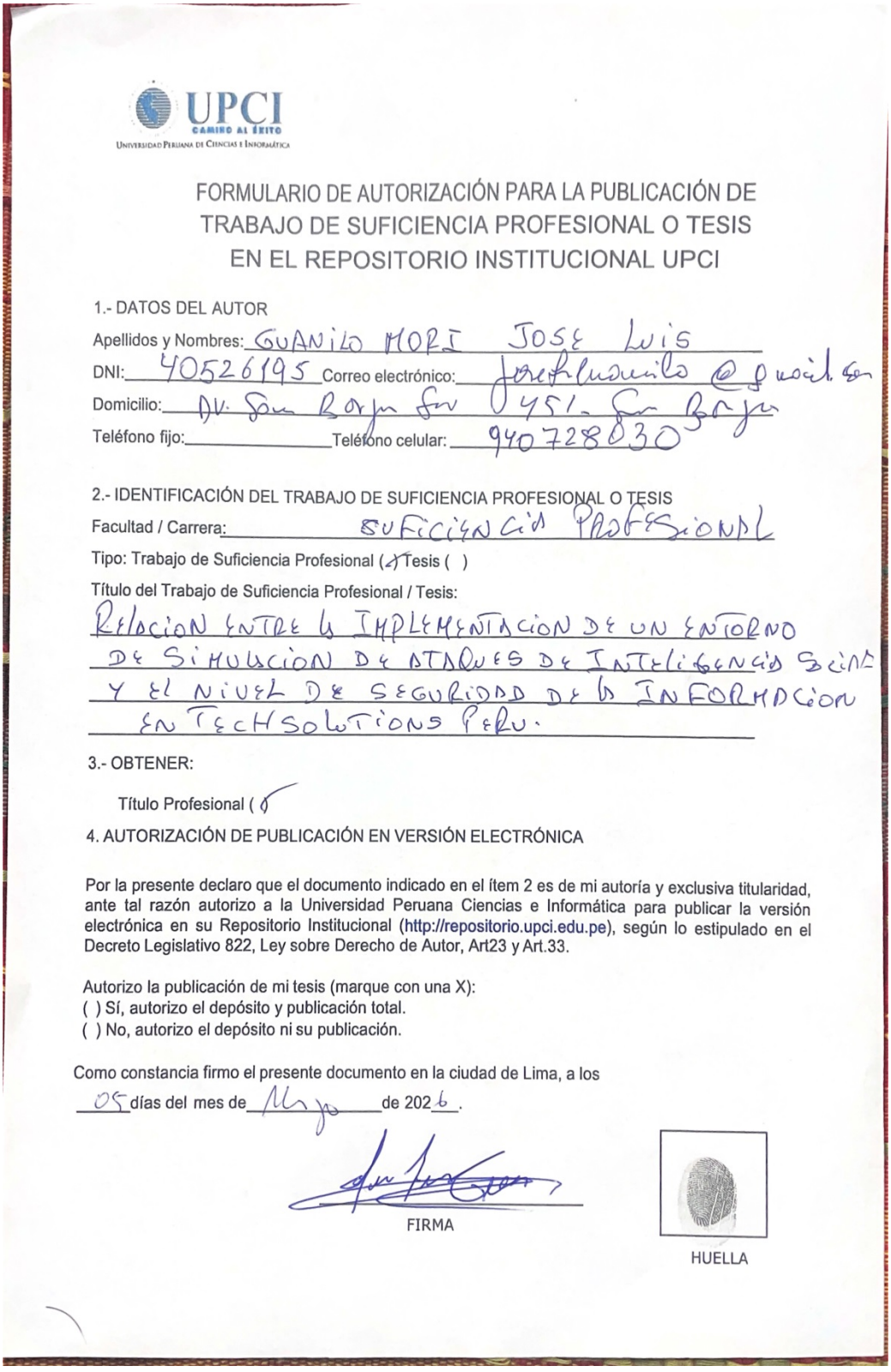
Fuentes principales

Las fuentes con el mayor número de coincidencias dentro de la entrega. Las fuentes superpuestas no se mostrarán.

1	Internet	repositorio.upci.edu.pe 7%
2	Internet	hdl.handle.net 4%
3	Internet	repositorioacademico.upc.edu.pe 1%
4	Trabajos del estudiante	Uniminuto Virtual <1%
5	Trabajos del estudiante	consultoriadeserviciosformativos <1%
6	Trabajos del estudiante	Universidad Continental <1%
7	Internet	repositorio.ucv.edu.pe <1%
8	Internet	repositorio.upsc.edu.pe <1%
9	Trabajos del estudiante	Universidad Nacional del Centro del Peru <1%
10	Internet	repositorio.udea.edu.pe <1%
11	Internet	www.clubensayos.com <1%

12	Trabajos del estudiante Universidad Privada del Norte	<1%
13	Trabajos del estudiante Universidad Tecnologica del Peru	<1%
14	Trabajos del estudiante Universidad de Sevilla	<1%
15	Internet apirepositorio.unu.edu.pe	<1%
16	Trabajos del estudiante Universidad Cientifica del Sur	<1%
17	Internet repository.unipiloto.edu.co	<1%
18	Trabajos del estudiante Universidad Internacional de la Rioja	<1%
19	Internet www.slideshare.net	<1%
20	Internet repositorio.unjfsc.edu.pe	<1%

Anexo 3. Autorización de publicación en repositorio



UPCI
CAMINO AL ÉXITO
UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL O TESIS EN EL REPOSITORIO INSTITUCIONAL UPCI

1.- DATOS DEL AUTOR

Apellidos y Nombres: GUANILO MORI JOSE LUIS

DNI: 40526195 Correo electrónico: joseluguanilo@gmail.com

Domicilio: Av. San Borja Sur 451 - San Borja

Teléfono fijo: _____ Teléfono celular: 940728830

2.- IDENTIFICACIÓN DEL TRABAJO DE SUFICIENCIA PROFESIONAL O TESIS

Facultad / Carrera: SUFICIENCIA PROFESIONAL

Tipo: Trabajo de Suficiencia Profesional (x) Tesis ( )

Título del Trabajo de Suficiencia Profesional / Tesis:

RELACION ENTRE LA IMPLEMENTACION DE UN ENTORNO DE SIMULACION DE ATAQUES DE INTELIGENCIA SCIA Y EL NIVEL DE SEGURIDAD DE LA INFORMACION EN TECHSOLUTIONS PERU.

3.- OBTENER:

Título Profesional ( )

4. AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRÓNICA

Por la presente declaro que el documento indicado en el ítem 2 es de mi autoría y exclusiva titularidad, ante tal razón autorizo a la Universidad Peruana Ciencias e Informática para publicar la versión electrónica en su Repositorio Institucional (http://repositorio.upci.edu.pe), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art23 y Art.33.

Autorizo la publicación de mi tesis (marque con una X):
( ) Sí, autorizo el depósito y publicación total.
( ) No, autorizo el depósito ni su publicación.

Como constancia firmo el presente documento en la ciudad de Lima, a los 05 días del mes de Mayo de 2026.

FIRMA

HUELLA