



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Dirección General de Estudios de Posgrado

Facultad de Ingeniería de Sistemas e Informática

Unidad de Posgrado

**Un framework para la gestión de la ciberseguridad
social en instituciones privadas de educación superior
de Lima Metropolitana**

TESIS

Para optar el Grado Académico de Magíster en Ingeniería de
Sistemas e Informática con mención en Gestión de Tecnología de
Información y Comunicaciones

AUTOR

Elton Nick Roy RODRIGUEZ DULANTO

ASESOR

Dr. José Luis SANTISTEBAN PAZOS

Lima, Perú

2025



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

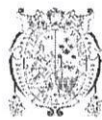
Referencia bibliográfica

Rodriguez, E. (2025). *Un framework para la gestión de la ciberseguridad social en instituciones privadas de educación superior de Lima Metropolitana*. [Tesis de maestría, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Unidad de Posgrado]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Elton Nick Roy Rodriguez Dulanto
Tipo de documento de identidad	DNI
Número de documento de identidad	76029540
URL de ORCID	https://orcid.org/0000-0001-5314-9448
Datos de asesor	
Nombres y apellidos	José Luis Santisteban Pazos
Tipo de documento de identidad	DNI
Número de documento de identidad	41570960
URL de ORCID	https://orcid.org/0000-0003-4526-642X
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	William Martín Enriquez Maguiña
Tipo de documento	DNI
Número de documento de identidad	06179457
Miembro del jurado 1	
Nombres y apellidos	Yamil Alexander Quiñones Nieto
Tipo de documento	DNI
Número de documento de identidad	42863390
Miembro del jurado 2	
Nombres y apellidos	Ciro Rodriguez Rodriguez
Tipo de documento	DNI
Número de documento de identidad	06040421
Miembro del jurado 3	
Nombres y apellidos	José Luis Santisteban Pazos
Tipo de documento	DNI
Número de documento de identidad	41570960

Datos de investigación	
Línea de investigación	C.0.3.20. Gestión de los Sistemas informáticos y de Información
Grupo de investigación	No aplica.
Agencia de financiamiento	Sin financiamiento.
Ubicación geográfica de la investigación	País: Perú Departamento: Lima Provincia: Lima Metropolitana Distrito: Lima Latitud: -12.056445 Longitud: -77.085994
Año o rango de años en que se realizó la investigación	Junio 2023 - Julio 2025
URL de disciplinas OCDE	Ingeniería de sistemas y comunicaciones https://purl.org/pe-repo/ocde/ford#2.02.04 Informática y Ciencias de la Información https://purl.org/pe-repo/ocde/ford#1.02.00



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. Decana de América
Facultad de Ingeniería de Sistemas e Informática
Vicedecanato de Investigación y Posgrado
Unidad de Posgrado

**ACTA DE SUSTENTACIÓN DE TESIS PARA OPTAR EL GRADO ACADÉMICO DE
MAGÍSTER EN INGENIERÍA DE SISTEMAS E INFORMÁTICA CON MENCIÓN EN
GESTIÓN DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES**

A los diecinueve (19) días del mes de noviembre de 2025, siendo las 6:00 pm., se reunieron en el Auditorio Alfredo Celso Alva Bravo, el Jurado de Tesis conformado por los siguientes docentes:

Mg. William Martín Enriquez Maguiña (Presidente)
Mg. Yamil Alexander Quiñones Nieto (Miembro)
Dr. Ciro Rodriguez Rodriguez (Miembro)
Dr. José Luis Santisteban Pazos (Miembro Asesor)

Se inició la Sustentación invitando al candidato a Magíster **ELTON NICK ROY RODRIGUEZ DULANTO**, para que realice la exposición oral de la tesis para optar el Grado Académico de Magíster en Ingeniería de Sistemas e Informática con mención en Gestión de Tecnología de Información y Comunicaciones, siendo la Tesis intitulada:

**“UN FRAMEWORK PARA LA GESTIÓN DE LA CIBERSEGURIDAD SOCIAL EN
INSTITUCIONES PRIVADAS DE EDUCACIÓN SUPERIOR DE LIMA METROPOLITANA”.**

Concluida la exposición, los miembros del Jurado de Tesis procedieron a formular sus preguntas que fueron absueltas por el graduando; acto seguido se procedió a la evaluación correspondiente, habiendo obtenido la siguiente calificación:

DIECISIETE (17) MUY BUENO

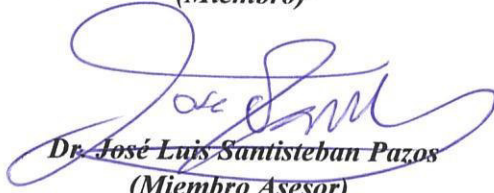
Por tanto, el presidente del Jurado, de acuerdo con el Reglamento General de Estudios de Posgrado, otorga al Bachiller **ELTON NICK ROY RODRIGUEZ DULANTO** el Grado Académico de Magíster en Ingeniería de Sistemas e Informática con mención en Gestión de Tecnología de Información y Comunicaciones.

Siendo las 14:20 horas, el presidente del Jurado de Tesis, da por concluido el acto académico de Sustentación de Tesis.


Mg. William Martín Enriquez Maguiña
(Presidente)


Mg. Yamil Alexander Quiñones Nieto
(Miembro)


Dr. Ciro Rodriguez Rodriguez
(Miembro)


Dr. José Luis Santisteban Pazos
(Miembro Asesor)



UNIVERSIDAD NACIONAL MAYOR DE
SAN MARCOS
Universidad del Perú, Decana de América

CERTIFICADO DE SIMILITUD

Yo, José Luis Santisteban Pazos, en mi condición de asesor acreditado con Dictamen N° 000462-2024-UPG-VDIP-FISI/UNMSM de la tesis, cuyo título es **UN FRAMEWORK PARA LA GESTIÓN DE LA CIBERSEGURIDAD SOCIAL EN INSTITUCIONES PRIVADAS DE EDUCACIÓN SUPERIOR DE LIMA METROPOLITANA**, presentado por el bachiller **ELTON NICK ROY RODRIGUEZ DULANTO**, para optar el grado académico de Magíster en Ingeniería de Sistemas e Informática con mención en Gestión de Tecnología de Información y Comunicaciones,

CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante la plataforma PIDS, el documento evaluado cuenta con el 16% de similitud, nivel **PERMITIDO** para continuar con los trámites correspondientes y para su **publicación en el repositorio institucional**.

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del grado académico de Magíster en Ingeniería de Sistemas e Informática con mención en Gestión de Tecnología de Información y Comunicaciones.

Lima, 5 de abril de 2025

Firma del Asesor

Nombres y Apellidos del asesor: José Luis Santisteban Pazos

DNI: 41570960

DEDICATORIA

A mi querido padre, Alfredo Rodriguez, quien a lo largo de su vida me ha inspirado a ser constante en el aprendizaje y a ser valiente en la búsqueda del conocimiento a través de la investigación.

AGRADECIMIENTOS

Deseo expresar mi más sincero agradecimiento al Dr. José Luis Santisteban Pazos, por su valiosa guía y asesoría durante todo el proceso de investigación. Sin su apoyo, esta tesis no habría alcanzado su culminación con éxito.

Asimismo, extendo mi agradecimiento a todos los profesionales de las áreas de tecnología de las universidades privadas de Lima, quienes, con sus valiosos aportes, contribuyeron al fortalecimiento de esta investigación.

Finalmente, quiero expresar mi más sincero agradecimiento a mi familia, por su constante motivación y apoyo incondicional, que fueron esenciales para alcanzar esta meta.

ÍNDICE GENERAL

ÍNDICE DE TABLAS.....	vii
ÍNDICE DE FIGURAS.....	viii
RESUMEN.....	ix
ABSTRACT.....	x
CAPÍTULO 1: INTRODUCCIÓN.....	1
1.1. Antecedentes del problema.....	1
1.2. Formulación del problema.....	3
1.3. Importancia del problema.....	4
1.4. Motivación.....	5
1.5. Objetivos.....	6
1.5.1. Objetivo General.....	6
1.5.2. Objetivos Específicos.....	6
1.6. Hipótesis.....	6
1.6.1. Hipótesis General.....	6
1.6.2. Hipótesis Específicas.....	6
1.7. Propuesta.....	7
1.8. Organización de la tesis.....	8
CAPÍTULO 2: MARCO TEÓRICO.....	8
2.1. Antecedentes del problema.....	8
2.1.1. Antecedentes Internacionales.....	8
2.1.2. Antecedentes Regionales.....	10
2.1.3. Antecedentes Nacionales.....	11
2.2. Bases teóricas.....	12
2.2.1. Teoría general de la disuasión.....	12
2.2.2. Teoría de la identidad social.....	12
2.2.3. Teoría de las redes sociales.....	13
2.2.4. Teoría general de sistemas.....	13
2.2.5. Marcos de referencia tecnológicos.....	13
2.3. Marcos conceptuales.....	14

2.3.1. Ciberseguridad	14
2.3.2. Ingeniería social	15
2.3.3. Riesgo cibernético	15
2.3.4. Gestión de TI	16
2.3.5. Ciberseguridad social	17
2.3.6. Marcos de referencia	18
CAPÍTULO 3: REVISIÓN DE LA LITERATURA.....	19
3.1. Metodología de la investigación	19
3.1.1. Planificación de la revisión	20
3.1.2. Desarrollo de la revisión	22
3.1.3. Resultados de la revisión.....	23
3.2. Análisis de resultados	25
CAPÍTULO 4: FRAMEWORK PARA LA GESTIÓN DE LA CIBERSEGURIDAD SOCIAL EN UNIVERSIDADES PRIVADAS (SCERA)33	
4.1. Motivación.....	33
4.2. Factores humanos y comportamiento.....	35
4.3. Ciberseguridad en entornos específicos	36
4.4. Modelos existentes.....	36
4.5. Hipótesis.....	37
4.6. Framework inicial.....	44
CAPÍTULO 5: VALIDACIÓN	45
5.1. Metodología y diseño de la investigación	45
5.1.1. Tipo y diseño de la investigación	45
5.1.2. Unidad de análisis	45
5.1.3. Población y muestra	45
5.1.4. Recolección de datos.....	46
5.1.5. Procedimiento	47
5.1.6. Confiabilidad de datos	48
5.1.7. Análisis e interpretación de datos.....	48
5.2. Resultados y Discusión	48
5.2.1 Análisis de los datos.....	48
5.2.2. Descripción del modelo en PLS-SEM	51
5.2.3. Evaluación del modelo de medida (Modelo exterior)	51

5.2.4.	Fiabilidad de los ítems	52
5.2.5.	Fiabilidad de los constructos	54
5.2.6.	La validez convergente	54
5.2.7.	La validez discriminante.....	55
5.2.8.	Evaluación del modelo estructural (Modelo exterior)	56
5.2.9.	Framework final	58
5.2.10.	Discusión.....	59
CAPÍTULO 6: CONCLUSIONES		62
6.1.	Conclusiones	62
6.1.1.	Conclusión general	62
6.1.2.	Conclusiones específicas	63
6.2.	Limitaciones	65
6.3.	Trabajos futuros	66
REFERENCIAS BIBLIOGRÁFICAS		67
ANEXOS		87

ÍNDICE DE TABLAS

TABLA 1 <i>CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN DE ARTÍCULOS</i>	21
TABLA 2 <i>CRITERIOS DE INCLUSIÓN</i>	21
TABLA 3 <i>CRITERIOS DE EXCLUSIÓN</i>	22
TABLA 4 <i>OBTENCIÓN DE BÚSQUEDAS DE DOCUMENTOS</i>	23
TABLA 5 <i>HIPÓTESIS PLANTEADAS</i>	43
TABLA 6 <i>CONSTRUCTOS CONSIDERADOS</i>	49
TABLA 7 <i>PERFIL SOCIODEMOGRÁFICO DE LA MUESTRA (N=30)</i>	49
TABLA 8 <i>MODELO DE MEDICIÓN DE FIABILIDAD INDIVIDUAL Y DE LOS CONSTRUCTOS</i> ...	53
TABLA 9 <i>MODELO DE MEDICIÓN DE VALIDEZ CONVERGENTE</i>	55
TABLA 10 <i>VALIDEZ DISCRIMINANTE</i>	56
TABLA 11 <i>RESULTADOS DEL MODELO ESTRUCTURAL</i>	57

ÍNDICE DE FIGURAS

FIGURA 1. PROPUESTA DEL FRAMEWORK DE GESTIÓN DE LA CIBERSEGURIDAD SOCIAL	7
FIGURA 2. FLUJO DEL PROCESO DE SELECCIÓN DE ARTÍCULOS	23
FIGURA 3. CANTIDAD DE ARTÍCULOS PUBLICADOS	24
FIGURA 4. FRECUENCIA DE FACTORES HALLADOS	27
FIGURA 5. <i>RADAR DE MARCOS DE TRABAJOS APLICADOS EN CIBERSEGURIDAD</i>	28
FIGURA 6. MODELOS DESARROLLADOS QUE SE ESTÁN APLICANDO	30
FIGURA 7. <i>TECNOLOGÍAS USADAS EN CIBERSEGURIDAD</i>	32
FIGURA 8. <i>FRAMEWORK SCERA</i>	44
FIGURA 9. <i>MODELO DE INVESTIGACIÓN A EVALUAR</i>	51
FIGURA 10. <i>RESULTADO DEL ANÁLISIS BÁSICO DEL MODELO</i>	58

RESUMEN

La ciberseguridad en las universidades privadas de nivel superior es un desafío creciente debido a los riesgos derivados de la ingeniería social, que explota las vulnerabilidades humanas para acceder a datos sensibles. Esta investigación tiene como objetivo diseñar un marco de trabajo para gestionar la ciberseguridad social en estas instituciones, enfocándose en la prevención de filtraciones de datos. La propuesta del Framework SCERA busca mejorar la gestión de la ciberseguridad social considerando factores culturales, educativos y tecnológicos.

La metodología incluye una revisión sistemática de la literatura, encuestas a 30 universidades privadas de Lima y validación estadística mediante modelado de ecuaciones estructurales. La investigación identifica los factores que influyen en la pérdida de datos y propone directrices para una gestión eficaz de la ciberseguridad social.

Los resultados destacan que la seguridad técnica y las normativas de ciberseguridad son esenciales para mitigar los riesgos de ciberataques sociales, y que la concientización sobre ciberseguridad es clave para implementar políticas efectivas.

En síntesis, se presenta un marco innovador que puede ser adoptado por universidades privadas para reducir riesgos cibernéticos y proteger la información sensible.

Palabras clave: Ciberseguridad social, Ingeniería social, Ciberseguridad, Framework, Gestión de la ciberseguridad.

ABSTRACT

Cybersecurity in private higher education institutions is an increasing challenge due to the risks associated with social engineering, which exploits human vulnerabilities to access sensitive data. This research aims to design a framework for managing social cybersecurity in these institutions, focusing on data breach prevention. The SCERA framework proposal seeks to enhance the management of social cybersecurity by considering cultural, educational, and technological factors.

The methodology includes a systematic literature review, surveys from 30 private universities in Lima, and statistical validation using structural equation modeling. The research identifies factors influencing data loss and provides guidelines for effective management of social cybersecurity.

The results highlight that technical security and cybersecurity regulations are essential for mitigating the risks of social cyberattacks, and that cybersecurity awareness is key to implementing effective policies.

In summary, an innovative framework is presented that can be adopted by private universities to reduce cyber risks and protect sensitive information.

Keywords: Social cybersecurity, Social engineering, Cybersecurity, Framework, Cybersecurity management.

CAPÍTULO 1: INTRODUCCIÓN

Dentro de la presente investigación se fundamenta una situación problemática dentro del campo de la ciberseguridad, que, a través de una justificación teórica, se analiza un nuevo paradigma de la ciberseguridad directamente relacionada con la ingeniería social en busca de una nueva propuesta que permita reducir la filtración de datos en las universidades.

Además, se plantean los cimientos para la creación de un marco, el cual podrá ser utilizado por las distintas instituciones educativas que deseen incorporar la ciberseguridad desde un enfoque cultural y así logren disminuir la exposición de información sensible que pueda perjudicar en el deterioro de la reputación institucional.

En el capítulo 1, se contextualiza la situación problemática a partir de la realidad nacional y se presenta una justificación que incluye los objetivos principales y secundarios, junto con los objetivos de investigación. El capítulo 2 establece las bases teóricas que servirán como fundamento para el desarrollo del artefacto propuesto. En el capítulo 3, se expone la revisión sistemática de la literatura. Posteriormente, en el capítulo 4, se describe la metodología basada en la ciencia del diseño, orientada hacia la creación de un artefacto conceptual. Además, se formulan las hipótesis necesarias para el proceso de validación del modelo propuesto. En el capítulo 5, se detalla el diseño y procedimiento de la investigación, que se ejecuta mediante la aplicación de una encuesta. Tras el análisis de los datos recopilados, se valida el modelo propuesto y se desarrollan las discusiones derivadas de los hallazgos obtenidos. Finalmente, el epílogo presenta las conclusiones, limitaciones y recomendaciones dirigidas a las instituciones privadas de nivel superior en Lima Metropolitana, con el propósito de enfrentar eficazmente los nuevos métodos de ciberataques que buscan afectar su responsabilidad social.

1.1. Antecedentes del problema

Según The Identity Theft Resource Center ITRC (2019) en su informe de filtración de datos de fin de año hallaron que, de un total de 1638 empresas, entre ellas instituciones educativas del continente americano, se reconocieron 1473 brechas de ciberseguridad que en consecuencia generaron exponer más de 165 millones de

registros confidenciales de las organizaciones que participaron en el estudio, dejando en evidencia que más del 89% de estas sufrió un ataque de ciberseguridad con el objetivo de filtrar datos e información.

Durante el 2020, el mundo se enfrentó a una crisis epidemiológica, la cual afectó a múltiples sectores que dependían de una presencia física de una persona; y a raíz del surgimiento de medidas para hacerle frente al avance de la pandemia, tales como el distanciamiento social o la virtualidad de las interacciones humanas, fueron también aumentando de manera acelerada la adopción de aplicaciones y sistemas de información entre toda la población, permitiendo así abrir paso al teletrabajo, la teleeducación y la telemedicina. Según Katz en su estudio sobre El estado de la digitalización de América Latina frente a la pandemia del COVID-19 detallan que la imposición de medidas sanitarias “ha ocasionado un salto en el uso de redes de telecomunicaciones por parte de la población” a lo largo de todo Latinoamérica y el Caribe. (Katz et al., 2020, p. 32).

Así mismo, en el informe de seguridad de ESET (2021) denominado Security Report, donde se involucró a 17 países de Latinoamérica con un total de 1800 encuestados, se evidenció que el Perú es uno de los países que más ataques de ciberseguridad sufrió en toda la región durante el 2021, debido a que un 40% de ataques cibernéticos estaban dirigidos a las empresas con el objetivo de secuestrar información mediante los canales como el correo electrónico y los enlaces web no seguros.

En adición, Rojas y Gilberto en su investigación sobre la Influencia del COVID 19 en el incremento de los Ciberataques a Nivel Mundial halló que una de “las formas utilizadas por los ciberdelincuentes es la ingeniería social” (Rojas & Gilberto, 2022, p. 5), ya que a través de ella logran obtener información sensible del individuo mediante técnicas de adivinación o suplantación, dejando en evidencia que al crecer las telecomunicaciones, a su lado surgió un crecimiento de ataques cibernéticos que dejaron en evidencia nuevas técnicas para engañar al usuario con la finalidad de generar una brecha de información de las organizaciones o entidades gubernamentales.

Según el estudio realizado por Hong et al., (2023) sobre la influencia del nivel de educación social en la conciencia y el comportamiento de ciberseguridad en estudiantes universitarios y graduados que trabajan, se encontró que existe una variación en los conocimientos de seguridad cibernética entre los estudiantes universitarios. Además, se evidenció que la influencia o presión social tiene un efecto

directo en los estudiantes, modificando tanto su actitud como su comportamiento hacia la ciberseguridad. Estos resultados destacan la relevancia de tener una formación social para fomentar una cultura de ciberseguridad dentro del entorno universitario.

El Perú, tampoco es ajeno a los ciber ataques malintencionados, puesto que en el informe elaborado por ASBANC y presentado a la Presidencia de Consejos de Ministros (PCM), se especifica que a raíz de una masiva filtración de datos personales de un gran porcentaje de peruanos causada en abril del 2022, se podía encontrar la comercialización de esta información sensible en los medios sociales y de venta al público final; logrando provocar un riesgo multisectorial en la elaboración de trámites y validaciones de identidades que llevan a cabo entidades públicas o privadas (Radio Programas del Perú - RPP, 2022).

Hoy en un mundo donde las opiniones, creencias y actitudes se mezclan con la tecnología generando infoxicación a través de medios sociales en la internet, surge un nuevo fenómeno particular denominado ciberseguridad social, que bajo el contexto científico de la ingeniería, Carley en su estudio definió la Ciberseguridad social como una ciencia emergente, detallando que este nuevo concepto se centra en “cómo se puede manipular el entorno digital para alterar tanto la comunidad como la narrativa” (Carley, 2020, p. 371) dando alcance a una nueva forma de generar ataques cibernéticos, la cual ha tomado mayor afluencia durante los últimos años, ya que utilizando técnicas sociales que permitan manipular al usuario y en un mundo donde todos tienen ya la posibilidad de concentrarse a la red, se hizo más probable que existan divulgaciones y exposiciones de información sensible tanto para organizaciones como instituciones educativas. En base a ello, se plantea la necesidad de estudiar este fenómeno, con el propósito de reducir la alta incidencia de ciberataques, diseñando un nuevo marco de referencia que aborde estas nuevas necesidades ligadas a la ciberseguridad.

1.2. Formulación del problema

La gestión de la ciberseguridad se ha transformado en una preocupación cada vez más relevante debido a las amenazas cibernéticas a nivel nacional e internacional. En ese enfoque se destaca la importancia de abordar el problema de la gestión seguridad en las instituciones universitarias, ya que se encuentran expuestas a amenazas similares a las que enfrentan las organizaciones nacionales e internacionales,

las cuales son producidas por diferentes causas. Además, según Buchanan (2017) en su libro resalta la importancia de fomentar la confianza en la gestión de la ciberseguridad, lo que pone en manifiesto la urgencia de establecer una cultura de seguridad en las instituciones universitarias. También menciona que los dilemas éticos y legales plantean la necesidad de abordar la ciberseguridad social de manera integral, considerando aspectos como la protección de datos personales, la privacidad y el cumplimiento normativo. Estos puntos respaldan la existencia de una falta de gestión (Ver Anexo C) y subrayan la relevancia de tratarlo de forma eficaz para garantizar tanto la protección de la información como la confianza en el ámbito digital.

Las instituciones privadas de nivel superior al no tener un ámbito a seguir como referencia ante este nuevo fenómeno que ha surgido, autores como Hong et al., (2023) destacan la influencia del nivel de educación social en la conciencia y el comportamiento de ciberseguridad entre estudiantes universitarios es de suma importancia. Además, las universidades son susceptibles a riesgos y amenazas relacionadas con la ciberseguridad social, como la divulgación no autorizada de información sensible y el uso inadecuado de datos.

Basado en estas evidencias la presente investigación busca exponer y resolver la siguiente interrogante:

PG: ¿Cómo el diseño de un nuevo marco de trabajo permite asegurar la gestión de la ciberseguridad social en las instituciones privadas de educación superior que sufren pérdidas de datos?

En consecuencia, de la pregunta declarada, y en busca de brindar una visión holística del problema, se establecen los siguientes cuestionamientos específicos:

PE1: ¿Cuáles son los factores de la ciberseguridad social que influyen en la pérdida de datos en las instituciones privadas de educación superior?

PE2: ¿Qué criterios deben considerarse para asegurar la gestión de la ciberseguridad social en las instituciones privadas de educación superior?

PE3: ¿Cómo puede diseñarse un marco de trabajo para la gestión de la ciberseguridad social en las instituciones privadas de educación superior?

1.3. Importancia del problema

A raíz del incremento de ataques cibernéticos dirigidos a empresas e instituciones, y el surgimiento de nuevos modelos que permiten engañar al usuario con

el objetivo de manipularlo y obtener información, es fundamental reconocer tanto las fortalezas como las debilidades que se pueden tener no solo en los sistemas informáticos, sino también a nivel organizacional. Además, es imprescindible preocuparse también por asegurar una resiliencia de la información utilizada por las diversas áreas de negocio de una institución y que es administrada desde el área de tecnología.

Por lo que el objetivo del estudio es desarrollar un marco de trabajo en la forma en cómo se diligencia la ciberseguridad social, no desde un enfoque social, sino desde un punto de partida organizacional y tecnológico; con la finalidad de reducir la pérdida de información mediante medios tecnológicos, sociales o a través de la internet.

El estudio busca proponer un marco de referencia relevante que mejore las propuestas revisadas en literatura reciente, que permitirá a las instituciones universitarias impedir la fuga de información y a su vez, generar conciencia sobre la ciberseguridad social en los trabajadores, sentando las bases para gestionar un cambio en la cultura organizacional. Así mismo, para el mundo académico el estudio pretende generar un aporte en el entendimiento y la gestión de la ciberseguridad enfocado desde una perspectiva de responsabilidad social y la protección de los datos ayudando así a ordenar el fenómeno reconociendo las partes, elementos y formas en la que se puede diligenciar.

1.4. Motivación

El motivo principal de la elaboración del estudio nace a partir del aumento de un 617% de ataques de ingeniería social según Kaspersky durante el 2023 frente al 2022 (Kaspersky, 2023) y de cómo estos pueden afectar a múltiples organizaciones e instituciones causando pérdidas de hasta varios miles de dólares debido a la venta de la información obtenida mediante técnicas de sugestión y engaño dirigidas hacia los usuarios del negocio. A su vez, esto puede causar un impacto considerable en la confianza y percepción que deposita el consumidor en la marca, causando rechazo en la adquisición de productos o servicios ofertados por la organización o institución afectada. Así mismo, el presente estudio se centra únicamente en las instituciones educativas universitarias privadas, debido a que son más susceptibles y almacenan gran cantidad de información sensible, incluyendo datos personales de estudiantes y/o del personal administrativo, investigaciones académicas y propiedad intelectual. Por

lo tanto, la pérdida o exposición de estos datos podría tener graves consecuencias que se materializan de manera moral o económica. Por tal motivo, dentro de este estudio se considera conveniente plantear un nuevo marco que permita guiar una concientización temprana de los colaboradores de una institución educativa superior sobre la ciberseguridad social y a su vez permita minimizar el riesgo de pérdidas de información en instituciones privadas de nivel superior.

1.5. Objetivos

1.5.1. Objetivo General

Diseñar un marco de trabajo para asegurar la gestión de la ciberseguridad social en las instituciones privadas de educación superior que sufren pérdidas de datos.

1.5.2. Objetivos Específicos

- a. Identificar los factores de la ciberseguridad social que influyen en la pérdida de datos en las instituciones privadas de educación superior.
- b. Describir un conjunto de criterios que aseguren la gestión de la ciberseguridad social en las instituciones privadas de educación superior.
- c. Diseñar un marco de trabajo para la gestión de la ciberseguridad social en las instituciones privadas de educación superior.

1.6. Hipótesis

1.6.1. Hipótesis General

El marco de trabajo propuesto permitirá asegurar la gestión de la ciberseguridad social en las instituciones privadas de educación superior que sufren pérdidas de datos.

1.6.2. Hipótesis Específicas

- a. La identificación de los factores de la ciberseguridad social permitirá establecer las principales dimensiones que inciden en pérdidas de datos en las instituciones privadas de educación superior.
- b. La descripción de los criterios servirá como base para la estructuración del marco de trabajo para la gestión de la ciberseguridad social en las instituciones

privadas de educación superior.

- c. El marco de trabajo diseñado permite la gestión de la ciberseguridad social en las instituciones privadas de educación superior.

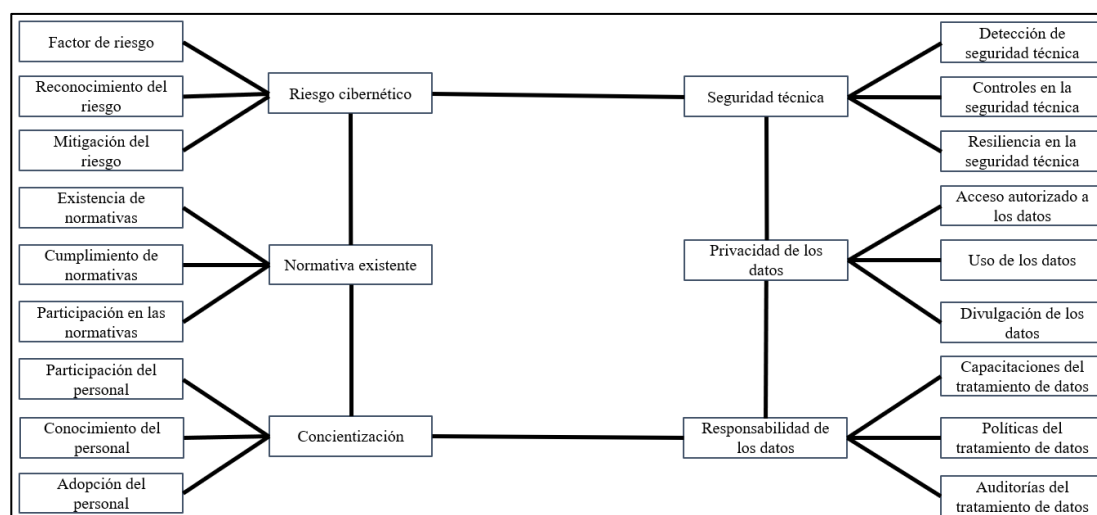
1.7. Propuesta

Este estudio propone desarrollar un framework conceptual que vincule los factores clave para tener en cuenta para ejecutar una correcta gestión de la ciberseguridad social dentro de las instituciones educativas de nivel superior de Lima Metropolitana, como se muestra en la figura 1. Además, se observa que cada factor se encuentra condicionado por otros indicadores, los cuales juegan un papel crucial en la identificación de riesgos, la adopción de medidas preventivas y el impulso de una cultura de ciberseguridad a nivel institucional.

Estos indicadores incluyen aspectos como la concienciación, la capacitación continua, la seguridad tecnológica, y las políticas o procedimientos claros. La interacción entre estos indicadores busca garantizar un enfoque integral que permita mejorar y fortalecer la resiliencia digital de las instituciones educativas frente a posibles amenazas cibernéticas de carácter social.

Figura 1.

Propuesta del framework de gestión de la ciberseguridad social



Fuente. Elaboración propia.

1.8. Organización de la tesis

La investigación se encuentra organizada en seis capítulos. El capítulo 1 aborda los antecedentes del estudio, la formulación del problema, la relevancia del tema, la motivación detrás de la investigación, los objetivos establecidos, así como la descripción de la propuesta y la organización de la tesis.

En el capítulo 2 se presenta el marco teórico, que expone los conceptos clave relacionados con el tema de investigación, definidos por la variable independiente “Marco de trabajo” y la variable dependiente “Gestión de la ciberseguridad social”.

El capítulo 3 ofrece un estado del arte, donde se realiza una revisión sistemática de la literatura, recopilando información actual sobre el tema de investigación a partir de estudios previos.

El capítulo 4 describe la contribución de la investigación, presentada como un artefacto, específicamente el marco conceptual que vincula los seis constructos necesarios para implementar una adecuada gestión de la ciberseguridad social en las instituciones de educación superior de Lima Metropolitana.

En el capítulo 5 se presenta la validación estadística del marco propuesto, mediante la validación de un modelo. Para ello, se aplica un instrumento de medición y se lleva a cabo un análisis de confiabilidad y validación del marco conceptual utilizando la técnica de mínimos cuadrados parciales.

Finalmente, en el capítulo 6 se exponen las conclusiones, limitaciones y recomendaciones para futuras investigaciones.

CAPÍTULO 2: MARCO TEÓRICO

2.1. Antecedentes del problema

2.1.1. Antecedentes Internacionales

Según Das (2016) se planteó como objetivo principal confirmar si las redes sociales impulsan comportamientos que puedan vulnerar a la seguridad, hallando que el aumento de la adopción de herramientas digitales generaba dentro de las organizaciones un nuevo fenómeno denominado Ciberseguridad Social, para el cual se debe proponer alternativas o medidas correctivas que actúen desde cualquier nivel de la organización y aseguren una resiliencia de la información confidencial tanto de

las personas como del negocio. Es importante resaltar que, a través del aumento de una adopción tecnológica se generan nuevas brechas de seguridad.

Además, Khidzir et al., (2016) hallaron que a través de la ingeniería social muchas organizaciones han sido víctimas de robos de información, dejando una alta valla a la comunidad cibernética en cómo reconocer y en quien sospechar frente a la alta existencia de usuarios o contenidos falsos que pueden lograr manipular a los empleados de una organización. Así mismo, llegaron a la conclusión que los medios sociales además de acelerar las vías de comunicación y exposición de marca, pueden manifestar riesgos cibernéticos, por lo que es crucial identificar cuáles son los factores clave que aseguren la reducción de estos riesgos en las redes sociales y permitan la generación de una comunidad socialmente cibersegura.

Carley et al., (2018) resaltó que la ciberseguridad social cuenta con desafíos que van de la mano con la relación de los avances tecnológicos y el control que se les puede ofrecer a los datos, sumando la regulación normativa que puede impartir cada país, sea de forma individual o conjunta. Así mismo la abundancia de comunicaciones falsas y fenómenos relacionados con la ingeniería social como el phishing, vishing, etc.; han desatado como consecuencia la manipulación de personas con el objetivo de comprometer al personal de una organización y por siguiente generar una brecha de seguridad. A raíz de ello, proponen que la ciberseguridad social aún es una ciencia emergente que busca la generación de un daño a través de una manipulación o influencia grupal, dejando en evidencia que se necesita promover una cultura de seguridad social cibernética.

Así mismo, según Beskow et al., (2019) encontraron que los atacantes pueden manipular tanto la información como el medio mediante maniobras que denotan falsas creencias o ideas con la finalidad de manipular a las masas. Así mismo, el uso de bots generadores de tendencias pueden multiplicar la fuerza de viralización de estas falsas creencias o ideas, logrando perjudicar tanto a los medios como a los individuos que se encuentren dentro. Por tal motivo, es imprescindible defender todas las debilidades internas existentes en una organización de las posibles manipulaciones externas, proponiendo controles, políticas y normativas que permitan reconocer y guiar a las organizaciones y su equipo de seguridad ante un ataque de ciberseguridad que utilice maniobras sociales con el objetivo de producir un daño de imagen o económico.

El estudio de Wu et al., (2022) mencionan que la autopresentación de un individuo en un medio físico, el acceso a los recursos colaborativos y la forma de autenticarse de manera individual y social en medios digitales son los principales dominios de la ciberseguridad que producen fricciones sociales o comportamientos desadaptativos de los trabajadores de una organización, lo cual comprueba que al momento de construir sistemas de información no se debe de ignorar los comportamientos sociales de las personas, pudiendo lograr una cultura de seguridad y privacidad cibernética.

2.1.2. Antecedentes Regionales

Forero et al., (2020) enfatizaron en que la ingeniería social es uno de los medios por donde los criminales digitales buscan engañar a las personas, consiguiendo generar confianza en la víctima para consolidar sus fraudes y suplantaciones. Por tal motivo, existe una clara necesidad de implementar estándares o metodologías que permitan fortalecer la seguridad cibernética de las organizaciones, no solo pensando en la información, sino también en la fuerza laboral. A través de este impulso, se pueden definir responsables de gestionar los riesgos, lograr controlarlos y mediante una posterior evaluación proponer mejoras continuas.

Según Batista (2021) demostró que la ciberseguridad abarca escenarios holísticos, mediante los aspectos individual, social, organizacional y político; así mismo, la dinámica que se evidencia en medios sociales es la de generar manipulación colectiva, con la finalidad de influir con un fin o a un medio; por lo que es importante definir un ámbito de conocimiento capaz de describir una cibercultura de seguridad en el ciberespacio, junto a la implementación de buenas prácticas y pensamientos que permitan a las personas u organizaciones desarrollarse en el ciberespacio asegurando una resiliencia de su información confidencial.

Así mismo, González et al., (2021) proponen que la ciberseguridad sea divulgada masivamente, así como también sean estudiadas y explicadas meticulosamente por y hacia toda la fuerza laboral perteneciente a una organización, ya que, sin importar los roles que existan, se puede contribuir en fortalecer la seguridad de la información. También, al generar una cultura de autoprotección, se reducen los niveles de vulnerabilidad y se aumentan las propuestas de políticas o normas que ayuden a salvaguardar la información pública, confidencial y del negocio, ayudando a

generar una nueva cultura organizacional cibernética.

Para Peralta et al., (2021) hallaron que, si un individuo usa medios sociales de manera particular, este también lo utilizará en su espacio de trabajo debido a que existe una presión o corriente social que dirige la adopción temprana de medios sociales o también llamados “early adopters”. A su vez, es importante considerar los efectos que pueden ocasionar el uso de medios sociales emergentes o ya consolidados frente a los procesos internos de una organización y su vinculación con las diversas áreas de negocio que manipulan información confidencial o no de individuos internos o externos.

2.1.3. Antecedentes Nacionales

Para Poma et al., (2019) describen que el 70% de las organizaciones coinciden que después del 2017 la adopción de tecnologías causó un crecimiento en el nivel de riesgo de seguridad como también el aumento de la productividad, así mismo, el crecimiento de ciberataques aumentó hasta en un 43.60% afectando a múltiples organizaciones privadas y pertenecientes al estado peruano. Esto deja en evidencia que localmente, en el Perú el delito o fraude informático ha estado en aumento desde el 2017, por lo que es imprescindible aplicar estrategias que puedan impedir estos nuevos actos delictivos.

Ormachea (2020) infiere que el estado y la sociedad peruana carece de concientización cibernética, por lo que se genera un reto que constituye tanto el compromiso social como la articulación de los sectores públicos y privados, con la finalidad de concretar reglamentos, políticas y normas generales que salvaguarden la información confidencial de las personas, como también ayuden en la formación de una sociedad segura e inteligente.

Así mismo, Zevallos (2021) concluye que cuando un individuo expone una cantidad significativa de información en los medios o redes sociales, mayor es el nivel de riesgo latente al que se somete, debido a que existen delincuentes cibernéticos que usan estos datos con la finalidad de vulnerar los derechos privados de las personas, creando brechas en su vida personal, social o laboral. Por tal motivo, es preciso resaltar que existe una relación entre la vulneración del derecho a la privacidad e intimidad y el uso no controlado de las redes sociales, los cuales pueden perjudicar a una

organización si es que uno de sus colaboradores se encuentra comprometido.

También, Salinas (2022) precisa que existen nuevas metodologías capaces de garantizar un acceso seguro a los activos informáticos (físicos o digitales) sin importar que estos se encuentren distribuidos, denominada Confianza Cero (Zero Trust). La implementación de metodologías que aseguren una defensa en profundidad permite a las organizaciones proteger el perímetro, pero cuando se vulnera a los individuos, a pesar de que se generen múltiples controles de acceso, se sigue sufriendo de ciberataques que parten por la ingeniería social y se transforman en un fenómeno donde la opinión social se muestra como referente.

2.2. Bases teóricas

2.2.1. Teoría general de la disuasión

Dentro de los principios básicos de la ciberseguridad los cuales son analizar, proteger y prevenir, el presente estudio propone establecer un lineamiento entre el prevenir y el nuevo fenómeno que ha surgido en el ámbito de la ciberseguridad, donde los actores malintencionados buscan disuadir a personas o empleados de las organizaciones con la finalidad de puedan realizar actos no deseados, los cuales pueden desencadenar en fugas de información, pérdidas económicas o ataques cibernéticos de mayor complejidad (Straub, 1998).

La teoría general de la disuasión se fundamenta dentro de la presente investigación a través del reconocimiento de la disuasión generada a los empleados con la finalidad de obtener información de manera ilícita. Así mismo, se determinará si las decisiones de las personas establecen un punto de partida a la generación de nuevas puertas traseras que puedan ser vulneradas.

2.2.2. Teoría de la identidad social

Para mantener un perímetro seguro dentro de las organizaciones, es importante definir si los colaboradores se esfuerzan por lograr y mantener una identidad social responsable y positiva (Tajfel, 1974).

Por ello, la teoría de la identidad social contribuirá con la medición de la influencia de un actor individual o de un grupo malintencionado en los colaboradores

de una organización, además de corroborar si se puede afectar únicamente de manera individual o colectiva, con la finalidad de convencer y traspasar las barreras de seguridad, los cuales pasarían a ser un riesgo para las instituciones universitarias.

2.2.3. Teoría de las redes sociales

Para lograr un mayor entendimiento de la forma de actuar de actores malintencionados, es imprescindible supervisar las vías de comunicación cibernéticas, ya que si en algún determinado punto en el tiempo, un actor interfiere en una comunicación entre dos interlocutores, este puede conocer y exponer los datos intervenidos, tomando el control de las decisiones y o roles (Freeman, 1978).

La teoría de las redes sociales aportará un mayor panorama del comportamiento de los nuevos ciber atacantes, quienes ahora utilizan tácticas de seducción en los empleados para interceptar comunicaciones clave o elevar los privilegios. Además, aportará en la creación de un framework de protección frente a los ciberataques, permitiendo afianzar la seguridad de las instituciones privadas de nivel superior, ya no desde sus identidades o dispositivos, sino partiendo de la cultura organizacional y de cómo los empleados se relacionan entre sí.

2.2.4. Teoría general de sistemas

En un mundo globalizado, donde los sistemas rodean tanto a las organizaciones como a los empleados, surgen nuevos elementos complejos, que, interconectados entre sí, son capaces de contribuir en la psicología social y patológica de quienes la usan, sea en beneficio propio o de una comunidad (Bertalanffy, 1969).

Por ello, la adopción de sistemas organizacionales seguirá en aumento, pero a su vez se crearán nuevas necesidades de aseguramiento y control de la información dentro de estos sistemas, por lo que requerirán de un aporte parcial o total para así absolver dicha necesidad. La teoría general de sistemas ayudará a definir un marco de referencia directamente relacionado con los sistemas existentes en las instituciones privadas de nivel superior.

2.2.5. Marcos de referencia tecnológicos

Una de las herramientas que nos puede ayudar analizar conceptualmente los comportamientos de los empleados en torno a las tecnologías son los marcos de

referencia tecnológicos, los cuales proponen examinar desde el punto de vista teórico para transformar los procesos en estrategias digitales (Orlikowski et al., 1994).

Para lograr el cumplimiento del objetivo principal de la presente investigación, es importante comprender antes cómo se estructura y cuáles son los puntos de partida de un marco de referencia, para lo cual se realizará una examinación profunda de los conceptos y de las personas que interactúen en torno a la información que es susceptible ante cualquier falta de prevención o resiliencia de la ciberseguridad.

2.3. Marcos conceptuales

2.3.1. Ciberseguridad

La ciberseguridad surge como una necesidad económica y social que se encuentra relacionada con el estudio de la influencia de los sistemas informáticos y los fenómenos que pueden surgir con el objetivo de comprometer las cualidades o el correcto funcionamiento de estos sistemas, por lo que es imprescindible generar activos informáticos que sean confiables y seguros dentro del ciberespacio (Ormachea, 2020).

Dentro de la presente investigación, se estudiará un fenómeno relacionado a la ciberseguridad, el cual puede afectar a los diversos sistemas informáticos y a la información que son propiedad de la organización o de los colaboradores.

Así mismo, la ciberseguridad se ha convertido en un área estratégica para múltiples organizaciones, donde se reconoce que la responsabilidad de su correcta gestión y cumplimiento ya no solo depende del área de TI, sino que se transforma en una responsabilidad compartida de manera transversal dentro de una organización (Doig et al, 2019).

Tanto para las empresas que nacieron utilizando tecnología como para las aquellas que se transformaron durante los años es clave promover a la ciberseguridad de manera holística dentro de toda la estructura organizacional.

También, se puede considerar a la ciberseguridad como un conjunto de métodos capaces de proteger la información y los activos tecnológicos dentro del ciberespacio; para así resistir ante un ataque cibernético con la finalidad de garantizar

una defensa de la sociedad y continuidad de los flujos de información (Rossi, 2021).

Por ende, la ciberseguridad juega un rol importante tanto dentro de la sociedad como en las organizaciones o instituciones educativas, y asegurar una defensa por defecto podría afianzar la continuidad de un medio o comunidad social generado por una motivación intrínseca.

2.3.2. Ingeniería social

Una definición exacta de la ingeniería social expresa que es el conjunto de declaraciones y tendencias ordenadas lógicamente con la finalidad de crear un sistema de hipótesis (Jaramillo, 1996); donde menciona a la ingeniería social como un arte que genera la creación e implantación de ideas distintas entre dos interlocutores.

El fenómeno dentro del presente estudio también se orienta en generar un sistema de ideas con la finalidad de vulnerar a un colaborador, comprometerlo y convertirlo en una fuente de fuga de información.

Para considerar una perspectiva lo suficientemente amplia de la ingeniería social es imprescindible involucrar a cualquier tipo de conocimiento que puede tener una comunidad, tergiversarlo y utilizarlo con otros individuos o grupos de una organización o comunidad distinta en un periodo de tiempo (Aarón et al., 2018).

Es por ello, que el estudio propondrá como una dimensión el grado de vulnerabilidad frente a engaños que permita transparentar una información mediante la confiabilidad y veracidad perteneciente a una organización.

Así mismo, la ingeniería social es un arte con el cual se influye a las personas, exponiéndose y explotando sus vulnerabilidades con un fin malintencionado (Chetioui et al., 2022).

El arte del engaño radica principalmente como una constante dentro de los ciberataques sociales, por lo que evaluar caminos que ayuden a reconocer, prevenir y reaccionar frente a este nuevo fenómeno se considera valioso para una organización o sociedad.

2.3.3. Riesgo cibernético

Al considerar un riesgo que afecte a las operaciones y sistemas de una

organización se nombra riesgo cibernético (Villa, 2018); el cual genera como consecuencia la vulneración de la información de la organización y la interoperabilidad de los sistemas. Al vulnerar a un individuo dentro de una organización se puede lograr vulnerar a los sistemas y afectar a la operación, provocando pérdidas económicas y daños a la imagen de una organización.

Pero en una organización, el riesgo cibernético ya no solo debe recaer como responsabilidad en los departamentos de tecnología, sino que debería ser un punto de discusión en las agendas de las distintas áreas de negocio que puede tener una empresa (Martínez, 2020).

Por lo que el riesgo cibernético no es un tema que se discuta recurrentemente al interno de muchas organizaciones o entidades educativas, hecho que se debe cambiar para generar una cultura cibernética segura y sostenible.

Así mismo, los riesgos cibernéticos pueden afectar a una gran cantidad de empresas, ya que al ser heterogéneas y con diversos grados de penetración pueden ocasionar impactos cualificables y cuantificables (Malavasi et al., 2022).

Por ello, dentro del problema se remarca que este nuevo fenómeno es un riesgo cibernético capaz de impactar directamente en la cadena de valor de las instituciones privadas de nivel superior, pudiendo así generar beneficios para los actores que la utilizan, que pueden ser beneficios ideológicos como económicos.

2.3.4. Gestión de TI

La gestión de tecnologías de la información (Gestión de TI) es el monitoreo del rendimiento, nivel de servicio y cumplimiento de los activos tecnológicos existentes en una organización (Peña et al., 2021).

Dentro del problema de investigación se menciona que existe una falta de normas que deben cumplirse dentro de una organización con la finalidad de evitar ciberataques, pero a su vez, no se debe descuidar el monitoreo constante de los activos tecnológicos que son accedidos por los empleados de la organización.

La gestión de TI es la encargada de establecer procedimientos y normas para acceder a los recursos tecnológicos de una manera adecuada, así mismo, rinde cuentas ante la alta dirección con la finalidad de cumplir las metas y exigencias que estos

puedan diligenciar (Amón et al., 2020).

Al mencionar el compromiso de los altos directivos de una organización frente a los ciberataques, la gestión de TI se vuelve un jugador principal debido a que son sus integrantes denominados como un conjunto de expertos, los que evalúan, proponen, despliegan y controlan toda la gestión de la ciberseguridad.

En muchas organizaciones al realizar una alineación de la gestión de riesgos con las implementaciones u adopciones de buenas prácticas, se logra sentar las bases fundamentales para definir una gestión de TI que permita la evaluación del riesgo y el soporte continuo de los distintos sistemas existentes (Santana et al., 2019).

Por tal motivo, dentro de la investigación se busca generar una base fundamentada que posibilite un sostén para las instituciones de educación superior que sufren de ataques por ingeniería social y que afectan a los múltiples sistemas internos, provocando descontento.

2.3.5. Ciberseguridad social

La ciberseguridad social se describe como un campo enfocado en los factores humanos y tecnológicos que busca proteger a individuos u organizaciones frente a las amenazas de manipulación derivadas de las actividades maliciosas dentro de la red (Mulahuwaish et al., 2025).

En el contexto de las instituciones educativas, la ciberseguridad social se convierte en un componente esencial en la gestión de tecnologías de la información. La conciencia, la ética y la responsabilidad en el uso de la información resultan determinantes para comprender como los usuarios interactúan con los medios digitales, por lo que surge la necesidad de fortalecer esa protección desde la gestión tecnológica.

Así mismo, desde la perspectiva de la comunidad científica en los últimos años la ciberseguridad social constituye un enfoque interdisciplinario que busca comprender, prevenir e influir en el comportamiento de las personas al utilizar los medios tecnológicos, con el fin de asegurar una resiliencia frente a amenazas que tergiversen la verdad (Thomson et al., 2025).

Este enfoque complementa la dimensión tecnológica con un punto de vista

educativo, reconociendo que el factor humano es el punto de mayor vulnerabilidad. Por ello, promover conductas digitales responsables y resilientes contribuyen en mitigar los riesgos de desinformación, ingeniería social y filtración de datos en múltiples comunidades.

De esta manera, la ciberseguridad social surge como una disciplina científica que responde a las amenazas, manipulaciones y violaciones éticas, enfocándose en la defensa de la veracidad de los datos (Zhou et al., 2025).

En consecuencia, la necesidad de contar lineamientos específicos se vuelve prioritaria. En ese sentido, el presente trabajo se centra en diseñar un marco de trabajo que permita promover prácticas éticas para la gestión de la ciberseguridad social, permitiendo que las instituciones de educación superior puedan prevenirse y mantenerse resilientes mediante un conjunto de medidas defensivas.

2.3.6. Marcos de referencia

Los marcos de referencia permiten obtener términos y procesos con los que se pueden mapear de manera detallada los mecanismos para desarrollar, evaluar y lograr tareas que ayuden a un propósito (Peña et al., 2020).

Dentro del problema se reconoce la falta de mecanismos que ayuden en la guía y en los parámetros de evaluación y control de la ciberseguridad social, donde se propone obtener un mapa vial que detalle los pasos a seguir desde el momento en el que se sufre un ataque cibernético hasta la generación de una resiliencia informática.

Así mismo los marcos de referencia son considerados espacios que describen modelos que sean útiles para construir otros modelos, volviendo a un fenómeno más holístico (Cestero et al., 2018).

Es importante mencionar que los marcos de referencia de arquitectura empresarial pueden ayudar a las organizaciones a alinear sus estrategias de negocio con la tecnología de manera efectiva, porque proporcionan un enfoque práctico para el diseño y la implementación de arquitecturas empresariales que permiten a las organizaciones aprovechar al máximo sus inversiones en tecnología y lograr una ejecución exitosa de la estrategia tecnológica (Ross et al., 2006).

Es por ello, que el uso de un marco de referencia tecnológico adecuado permite

a las instituciones universitarias establecer una base sólida para la ejecución de su estrategia de ciberseguridad mediante la alineación estratégica, la definición de capacidades y procesos, y la gestión del cambio; proporcionando una guía práctica para gestionar la seguridad de la información y proteger los datos sensibles de las universidades.

De la literatura revisada se concluye que la ciberseguridad social como espacio u objeto de estudio actualmente se encuentra escasamente indagado, por lo que es pertinente elaborar marcos de referencia que permitan orientar las distintas teorías o conceptos clave que describan el fenómeno.

Finalmente, un marco de referencia logra diseñar y orquestar una estrategia basada en la innovación y el desbloqueo de valor de una organización (Gil, 2020).

En el presente estudio, se propone la elaboración de conceptos y estrategias que permitan controlar y dirigir las reacciones frente a los ciberataques que se incluyen dentro de la ciberseguridad social.

CAPÍTULO 3: REVISIÓN DE LA LITERATURA

En el presente capítulo revisamos la literatura sobre las prácticas para llevar a cabo la transformación digital en empresas del sector público, así como también de los factores.

3.1. Metodología de la investigación

Dentro de la presente investigación se llevará a cabo una revisión sistemática de la literatura siguiendo una metodología compuesta por las siguientes tres fases originalmente planteadas por Kitchenham y Charters (2007):

Planificación: En esta etapa se definirán los objetivos de la revisión y se establecerá un protocolo de búsqueda que incluirá las bases de datos a utilizar, las palabras clave, los criterios de inclusión y exclusión, y los criterios de calidad de los estudios seleccionados.

Desarrollo: Durante esta fase se realizará la búsqueda de artículos en las bases de datos seleccionadas, se aplicarán los criterios de inclusión y exclusión para

seleccionar los estudios relevantes, y se llevará a cabo la extracción de datos de los estudios incluidos. Además, se realizará una evaluación de la calidad de los estudios seleccionados para asegurar la validez y fiabilidad de los resultados.

Resultados: En esta etapa se analizará y se sintetizará los datos extraídos de los estudios seleccionados. Se identificarán los patrones, tendencias y hallazgos más relevantes relacionados con la ciberseguridad social, la ingeniería social y la protección de datos.

3.1.1. Planificación de la revisión

Con el propósito de llevar a cabo la búsqueda de artículos se proponen cuatro preguntas de investigación que buscan profundizar sobre la ciberseguridad social:

P1: ¿Qué factores influyen en el desarrollo de un marco de trabajo?

P2: ¿Qué marcos de trabajo se han empleado?

P3: ¿Qué modelos se han desarrollado?

P4: ¿Qué tecnologías emergentes se están aplicando?

A continuación, se describe el proceso de búsqueda y selección de artículos, el cual se enfocará en tres bases de datos científicas. Se aplicará un filtro de búsqueda para cada una de ellas utilizando los conectores “AND” y “OR” con el objetivo de agilizar y refinar los criterios de búsqueda. La estructura de la consulta de búsqueda se definirá de la siguiente manera: (“social cybersecurity”) AND ((factor OR variable) OR (framework OR construct) OR (model OR paradigm) OR (“emerging technologies” OR “technology trends”)).

Así mismo, se indica que la presente investigación aplicará la cadena de búsqueda en las siguientes bases de bases de datos: IEEE Xplore, ScienceDirect, SpringerLink y Web of Science. Para realizar la selección de documentos, se realizó la aplicación de la cadena de búsqueda en los ámbitos de título, resumen y palabras clave, además que se aplicaron criterios de inclusión y exclusión previamente definidos. En la Tabla 1 se detalla por cada base de datos las cadenas de búsquedas aplicadas.

Tabla 1*Criterios de inclusión y exclusión de artículos*

Bases de datos	Cadenas de búsquedas aplicadas
IEEE Xplore	((“social cybersecurity”) AND ((“factor” OR “variable”) OR (“framework” OR “construct”) OR (“model” OR “paradigm”) OR (“emerging technologies” OR “technology trends”)))
ScienceDirect	(“social cybersecurity”) AND ((“factor” OR “variable”) OR (“framework” OR “construct”) OR (“model” OR “paradigm”) OR (“emerging technologies” OR “technology trends”))
SpringerLink	'(“social cybersecurity”) AND ((“factor” OR “variable”) OR (“framework” OR “construct”) OR (“model” OR “paradigm”) OR (“emerging technologies” OR “technology trends”))'
Web of Science	TS=((“social cybersecurity”) AND ((“factor” OR “variable”) OR (“framework” OR “construct”) OR (“model” OR “paradigm”) OR (“emerging technologies” OR “technology trends”)))) and Open Access

Fuente. Elaboración propia

A continuación, como se especifica en la Tabla 2, se describen los criterios de aceptación que deben cumplir los documentos con la finalidad de ser evaluados en la presente revisión sistemática.

Tabla 2*Criterios de inclusión*

Criterio	Descripción
Nivel de acceso	Se incluirá todos los documentos con un acceso abierto y que no se encuentren en versión preliminar.
Idioma	Se incluirá todos los documentos pertenecientes al idioma inglés.
Área de estudio	Se incluirá todos los documentos en el área de las Ciencias de la computación o de Ciberseguridad.
Tipos de documentos	Se incluirá todos los documentos de tipo Artículos de investigación (Artículos de contribución).

Fuente. Elaboración propia

A continuación, en la Tabla 3, se describen los criterios de los documentos que serán discriminados dentro de la presente revisión sistemática.

Tabla 3

Criterios de exclusión

Criterio	Descripción
Duplicidad	No se incluirán todos los documentos que se encuentren duplicados en las distintas bases seleccionadas.
Antigüedad	No se incluirán los documentos publicados con un mayor tiempo a 5 años (2019-2023) debido a que en marzo Beskow y Carley (2019) introdujeron el concepto de la Ciberseguridad Social.
Objetividad	No se incluirán todos los documentos que no guarden relación con el propósito del estudio.

Fuente. Elaboración propia

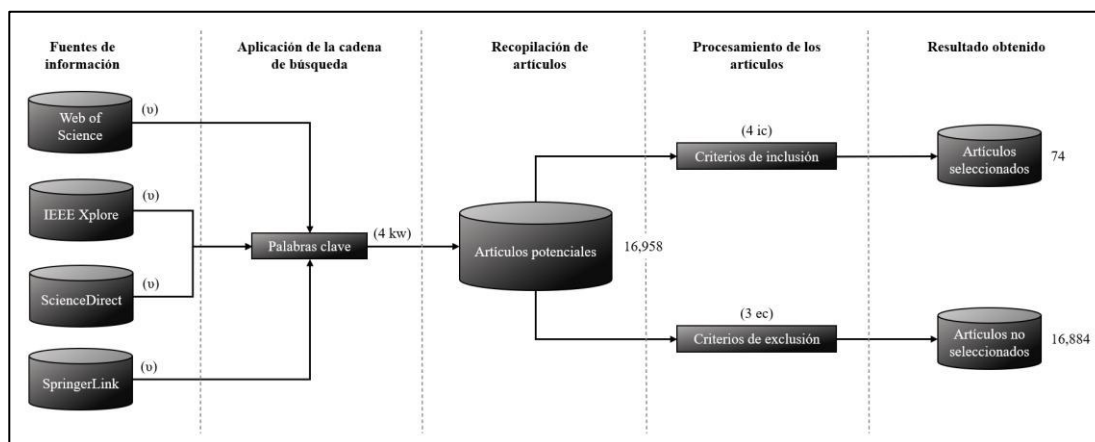
3.1.2. Desarrollo de la revisión

Luego de seleccionar las bases de datos y definir la estructura de indagación en base a los criterios de inclusión y exclusión, se ejecuta una búsqueda la cual permite obtener los siguientes resultados.

Se reconocen un total de 16,958 documentos, los cuales deberán ser partícipes de los criterios de inclusión y exclusión dentro de cada base de datos según se muestra en la figura 2.

Figura 2.

Flujo del proceso de selección de artículos



Fuente. Elaboración propia

3.1.3. Resultados de la revisión

Del procedimiento aplicado y descrito, se reconoce que gran número de los documentos excluidos no cumplían con la objetividad y la antigüedad deseada para la realización de la revisión, por lo que se procede a trabajar con los artículos restantes especificados en la Tabla 4.

Tabla 4

Obtención de búsquedas de documentos

IEEE Explore	Science Direct	Springer Link	Web of Science	Totales
432	9	16512	5	16958

Fuente. Elaboración propia

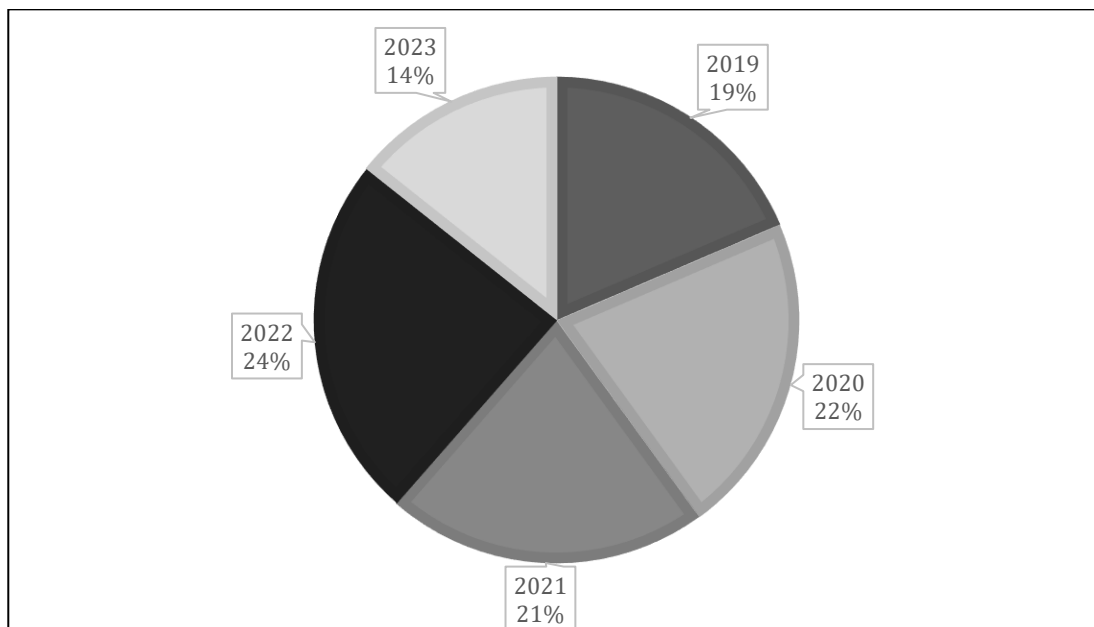
Por tal motivo, como resultado de la aplicación del estado del arte, según se describe en la Figura 2, se detalla el procedimiento de la selección de artículos, que ya aplicado, se procede a trabajar con los 70 artículos pertenecientes a artículos de investigación científica primarios, los cuales ayudarán a dar respuesta a las preguntas de la investigación.

Dentro de los artículos mencionados se reconoce que los países de los autores que generan una mayor contribución a la presente investigación son los siguientes: China con 18 artículos, Estados Unidos con 10 artículos, España con 7 artículos y Australia

con 6 artículos, los cuales en conjunto conforman un 42% del total de investigaciones seleccionadas para esta investigación.

Figura 3.

Cantidad de artículos publicados



Fuente. Elaboración propia

Así mismo, entre el 2019 y 2021 se reconoce una ligera tendencia positiva en la frecuencia de publicación de artículos como se aprecia en la Figura 3, además se evidencia que el 2022 fue el año con más publicaciones en las bases de datos seleccionadas, representadas por el 92% del total de artículos seleccionados de las bases de datos IEEE Xplore y SpringerLink. Esto deja en evidencia que existe una creciente demanda en abordar el tema de ciberseguridad en todo aspecto tecnológico. Como punto adicional, la investigación abarca un total de 11 revistas científicas, dentro las cuales IEEE Access, Cybersecurity e Information Processing & Management acrecientan un total de 89% de las investigaciones evaluadas en el presente estudio. Estas revistas dentro del mundo de la investigación están catalogadas en base a su factor de impacto, donde el cuartil al que pertenecen es el primero (Q1), ofreciendo por consecuencia un criterio de calidad adicional a la revisión sistemática realizada.

3.2. Análisis de resultados

Como resultado de aplicar la metodología definida en la sección anteriormente mencionada, y luego de revisar los 70 estudios seleccionados, se detallan los resultados que permiten responder a las preguntas de investigación.

P1: ¿Qué factores influyen en el desarrollo de un marco de trabajo?

Los riesgos y amenazas son elementos fundamentales que representan posibles eventos que pueden comprometer la integridad, confidencialidad y disponibilidad de los sistemas y datos dentro del entorno digital, y al ser reconocido como el principal factor que influye en la construcción de un marco, como se evidencia en la Figura 4, demuestra que son los riesgos como la exposición a ciberataques sofisticados, amenazas Sybil, espionaje en la comunicación, y rumores entre comunidades los principales causantes de pérdidas de datos. Así mismo, la identificación, evaluación y gestión adecuada de estos riesgos son esenciales para tomar medidas preventivas, como la detección y respuesta oportuna. La caracterización de malware, la evaluación de la probabilidad de ocurrencia de ataques o fallas técnicas, y el análisis de contenido y patrones en línea también son aspectos clave para mitigar estos riesgos. Además, se debe considerar la colaboración y cooperación, la protección de dispositivos IoT, la detección de actividades de desinformación en línea, y la conciencia del consumidor en el pago con criptomonedas como elementos que contribuyen a la comprensión y abordaje de estos riesgos. La detección y análisis de amenazas, así como la protección contra campañas de desinformación, también son fundamentales para la ciberseguridad. Los desafíos legales y políticos, la protección de la privacidad en tecnología de reconocimiento facial, y la protección de datos en sistemas multi-nube son factores adicionales que se deben tener en cuenta al enfrentar estos riesgos y amenazas. Es por ello por lo que el reconocimiento y gestión de los riesgos y amenazas son fundamentales para mantener un entorno digital seguro y confiable.

Por otro lado, la protección contra ciberataques implica salvaguardar los sistemas y datos de posibles amenazas, ataques y vulnerabilidades. Para lograr una defensa sólida, se debe considerar la colaboración y cooperación entre agencias y organizaciones, la implementación de tecnologías innovadoras, y la concienciación y educación como principales jugadores en este nicho. También, el análisis del comportamiento de ataques cibernéticos mediante el uso de técnicas de aprendizaje

automático contribuye significativamente a reforzar la seguridad en línea y fortalecen la protección contra ciberataques, la cual es una tarea en constante evolución que requiere una visión integral y estratégica para mantener un entorno digital seguro y confiable.

La gestión de riesgos es un proceso que tiene como objetivo identificar, evaluar y mitigar los riesgos asociados con la seguridad de los sistemas y datos en el entorno digital. Por lo que es un enfoque estratégico y proactivo que busca salvaguardar los activos digitales y garantizar la confiabilidad y seguridad del entorno en línea.

Además, la protección de la privacidad busca salvaguardar la información personal y confidencial de los usuarios o empresas en un entorno en constante evolución y amenazas digitales, por lo que es importante tener en cuenta diversos factores, como la detección de posturas en línea y desinformación, la implementación de técnicas de preservación de la privacidad en publicación de datos de redes, y el uso de datos sintéticos y privacidad diferencial para la estimación de frecuencia.

Así mismo, la conciencia y educación juegan un papel crucial para que los usuarios comprendan los riesgos y amenazas cibernéticas, mientras que una sólida cultura de seguridad fomenta prácticas seguras en todos los niveles de una organización.

Por otra parte, la constante innovación tecnológica ofrece soluciones avanzadas para contrarrestar las amenazas emergentes y mejorar la seguridad en línea, mientras que la colaboración y cooperación entre actores clave, como entidades gubernamentales y centros de investigación, fortalecen la detección y respuesta ante ataques.

En consecuencia, el lograr una resiliencia y recuperación ante desastres cibernéticos permiten a las organizaciones recuperarse rápidamente de incidentes y minimizar el impacto en sus operaciones, puesto que con ayuda de las políticas y regulaciones se establecen marcos legales y directrices para garantizar el cumplimiento y responsabilidad en materia de ciberseguridad yendo en conjunto con la evaluación y auditoría para identificar vulnerabilidades y áreas de mejora en los sistemas, definiendo así como la Industria y el contexto organizacional puede enfocarse en adaptar estrategias de ciberseguridad según las necesidades específicas de cada sector.

Figura 4.*Frecuencia de factores hallados*

Fuente. Elaboración propia

Finalmente, el cumplimiento de normativas y regulaciones puede asegurar que las organizaciones adopten prácticas de seguridad adecuadas y acordes a los estándares establecidos mediante una gobernanza de tecnologías donde se supervise y coordine esfuerzos para proteger los recursos digitales disponibles que, en términos de tecnología, son tanto el personal capacitado como la financiación los capaces de implementar una sólida estrategia de ciberseguridad.

P2: ¿Qué marcos de trabajo se han empleado?

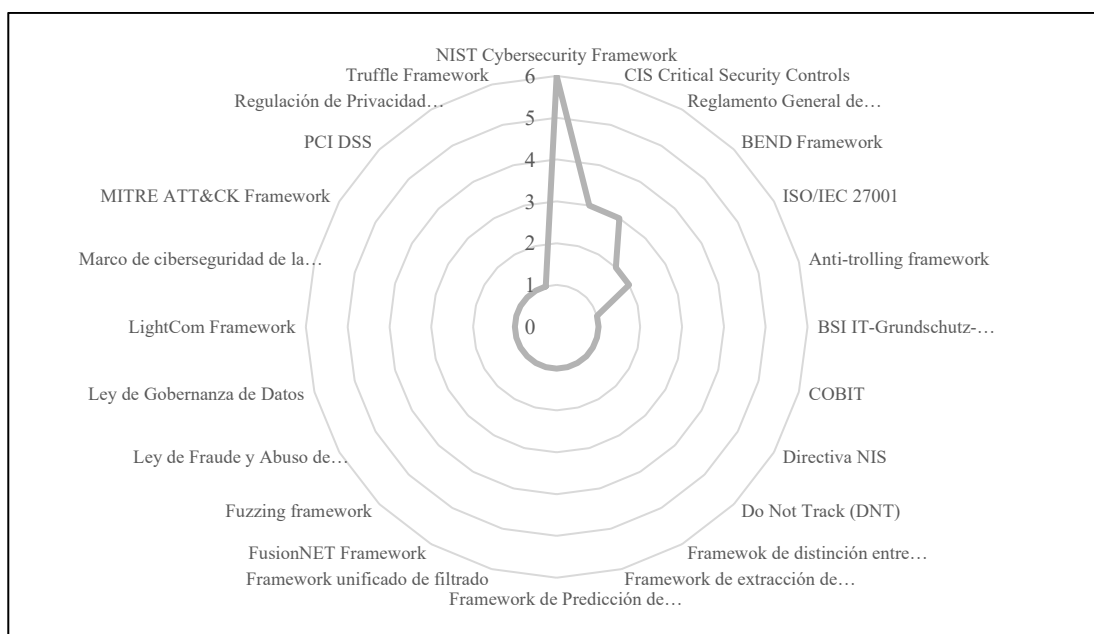
Dentro de las investigaciones enfocadas en ciberseguridad, diversos marcos de trabajo han sido desarrollados para abordar los desafíos relacionados con la protección de la información y la mitigación de riesgos como se evidencia en la Figura 5. Uno de los marcos más destacados es el NIST Cybersecurity Framework, propuesto por el Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos. Este marco ofrece una guía detallada para que las organizaciones gestionen y mejoren su postura de ciberseguridad a través de cinco funciones principales: identificar, proteger,

detectar, responder y recuperar; puesto que, al alinear sus estrategias con este marco, se puede establecer una base sólida para proteger activos tecnológicos críticos y enfrentar las amenazas cibernéticas con mayor eficiencia y eficacia.

Otro marco mencionado es el CIS Critical Security Controls, el cual complementa al NIST Cybersecurity Framework puesto que proporciona un conjunto específico de controles para mejorar la seguridad de los sistemas de información. Estos controles, los cuales están organizados por prioridad, abarcan desde medidas básicas hasta controles más avanzados y se mantienen actualizados en función de las amenazas emergentes. Al seguir este marco, las organizaciones pueden enfocarse en las áreas de mayor riesgo y establecer una línea de defensa más efectiva contra las vulnerabilidades y los ataques cibernéticos.

Figura 5.

Radar de Marcos de trabajos aplicados en ciberseguridad



Fuente. Elaboración propia

Así mismo, la protección de la privacidad es una preocupación clave en el ámbito de la ciberseguridad, y el Reglamento General de Protección de Datos (GDPR) es un marco legal crucial diseñado para abordar este tema, siendo aplicable en la Unión Europea. Este marco establece normas para la recopilación, el procesamiento y la protección de los datos personales de los ciudadanos, logrando imponer a las organizaciones la responsabilidad de garantizar la privacidad y el consentimiento

informado de los usuarios, así como de notificar a las autoridades y a los individuos afectados en caso de que existan brechas de seguridad.

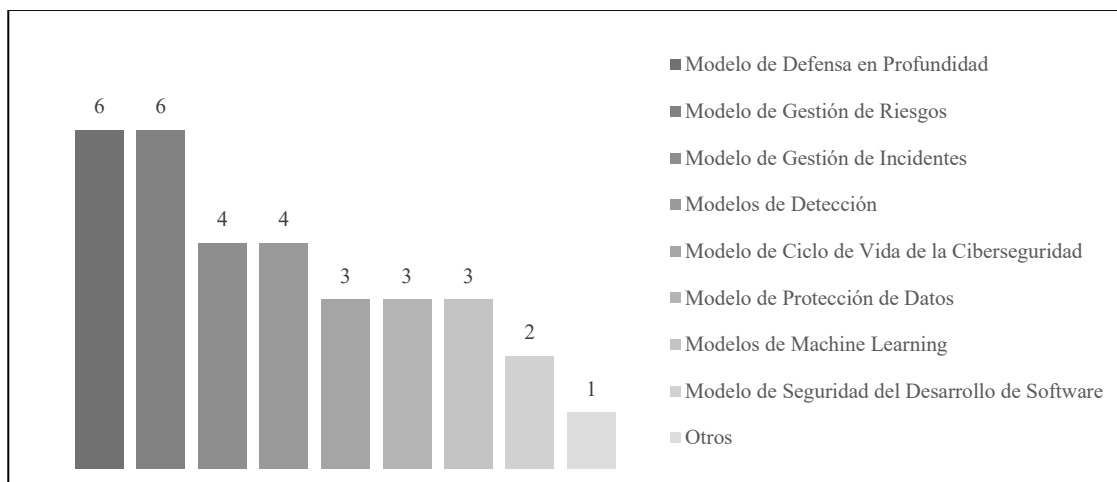
También, la norma "ISO/IEC 27001" es un marco para la gestión de seguridad de la información que proporciona requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI). Por último, el BEND Framework, como marco de ciberseguridad emergente que proporciona una solución para la identificación de fuentes de imágenes ofrece una forma de conceptualizar las tácticas utilizadas en las operaciones de información en línea y es utilizado para identificar y analizar maniobras de ciberseguridad social en las redes sociales.

En síntesis, estos marcos de trabajo desempeñan roles fundamentales en el fortalecimiento de la ciberseguridad y la protección de datos, ya que mediante la elaboración de una guía holística se puede mejorar drásticamente la postura de ciberseguridad de las organizaciones al considerar y aplicar estos marcos de manera conjunta, permitiendo desarrollar estrategias de ciberseguridad más sólidas y adaptables a las amenazas que surgen cada día.

P3: ¿Qué modelos se han desarrollado?

Dentro del campo de la ciberseguridad, el contar con una efectiva protección de los sistemas informáticos y de los datos requiere de la aplicación de diversos modelos que permitan abordar diferentes aspectos de la seguridad digital. Entre los más resaltantes, como se evidencia en la Figura 6, se destaca el Modelo de Defensa en Profundidad, donde se utiliza la metodología de sistemas inmunitarios artificiales (AIS) para seleccionar contramedidas óptimas contra ciberataques. Este enfoque propone una estrategia multicapa (Como si fueran capas de una cebolla roja) que involucra diferentes barreras de seguridad para prevenir, detectar y responder ante cualquier ataque.

Así mismo, otro modelo planteado dentro de muchos estudios detalla al Modelo de Gestión de Riesgos que es útil para identificar, evaluar y mitigar los riesgos asociados a las operaciones y activos de una organización, permitiendo tomar decisiones informadas en cuanto a la asignación de recursos y la implementación de controles de seguridad. También, el Modelo de Gestión de Incidentes es esencial para dar una respuesta ágil y efectiva ante eventos desafortunados puesto que define los procedimientos y roles a seguir en caso de que ocurra un incidente cibernético.

Figura 6.*Modelos desarrollados que se están aplicando**Fuente. Elaboración propia*

En cuanto a la aplicación de Modelos de Detección, existe cierta propincuidad con el Modelo de Clasificación de Eventos de Ciberseguridad permite categorizar eventos de seguridad en diferentes clases, facilitando la priorización y respuesta a incidentes; cómo también con el Modelo de Detección de Noticias Falsas basado en el aprendizaje automático que busca identificar información falsa o engañosa en las redes sociales y medios digitales. En conjunto, estos modelos juegan un papel importante en la protección contra las amenazas cibernéticas y la preservación de la integridad de la información digital, puesto que su aplicación adecuada proporciona a las organizaciones una mayor capacidad para anticiparse, enfrentar y mitigar los riesgos asociados al entorno digital en constante evolución.

Otros componentes críticos que deben considerarse abordan temas sobre el cómo elaborar un plan para el proceso completo de una ciberseguridad exitosa. Por ello, el Modelo de Ciclo de Vida de la Ciberseguridad detalla a medida la planificación y prevención hasta la recuperación y mejora continua de sistemas ciberseguros. Además, los Modelos de Protección de Datos ayudan a garantizar la privacidad y cumplir con las regulaciones relacionadas con el manejo y procesamiento de información sensible. Estos dos modelos ayudan de cerca en la creación de políticas y prácticas para asegurar que los datos sean capturados, almacenados y utilizados de forma ética y segura.

Finalmente, los Modelos de Machine Learning son una herramienta necesaria para la detección de amenazas y la toma de decisiones en tiempo real. Dentro de estos modelos se utilizan algoritmos de aprendizaje automático para identificar patrones y anomalías en grandes volúmenes de datos, los cuales también contribuyen a Modelos de Seguridad del Desarrollo de Software como el Software Assurance Maturity Model (SAMM), Application Security Verification Standard (OWASP ASVS), Building Security In Maturity Model (BSIMM) y el Security Development Lifecycle (Microsoft SDL) permitiendo una detección más precisa de ataques dentro de sistemas y ambientes informáticos.

En síntesis, existen diversos modelos desempeñan roles clave para asegurar una resiliencia, donde estos pueden abarcar desde la prevención y detección de amenazas hasta la gestión de incidentes y la protección de datos. Cada uno de los modelos existentes aporta desde su enfoque particular una guía para salvaguardar la confidencialidad, integridad y disponibilidad de la información y sistemas digitales, contribuyendo así a una sólida postura de seguridad cibernética.

P4: ¿ Qué tecnologías emergentes se están aplicando?

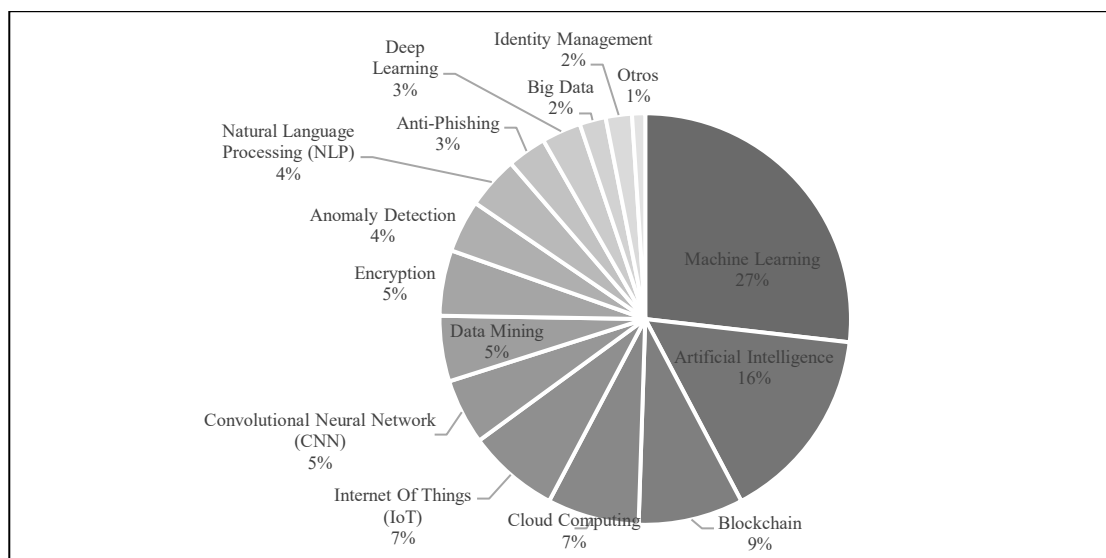
La aplicación de tecnologías emergentes en la ciberseguridad ofrece enfoques innovadores para proteger sistemas y datos contra las crecientes amenazas cibernéticas, estas tecnologías emergentes han sido aplicadas por varios investigadores como se aprecia en la Figura 7. La primera tecnología emergente por resaltar es el Machine Learning, el cual es fundamental en la detección de amenazas y en la detección de anomalías que se emplean para identificar actividades maliciosas que no siguen los patrones típicos de comportamiento, lo que puede indicar la presencia de ataques o actividades sospechosas. También el Machine Learning contribuye en la clasificación de eventos de seguridad, la identificación de patrones de comportamiento malicioso y la generación de respuestas automáticas a incidentes. Hoy, gracias a los algoritmos de Machine Learning somos capaces de analizar grandes volúmenes de datos en tiempo real, lo que facilita la identificación de actividades sospechosas y la toma de decisiones más rápidas y precisas.

Por otra parte, la Inteligencia Artificial, y el Deep Learning son utilizados para mejorar la detección de amenazas o malware, analizar comportamientos maliciosos, y fortalecer los mecanismos de defensa en general. Así mismo, uno de los actuales jugadores emergentes es el Blockchain que, mediante su uso en criptomonedas, ofrece

también un ámbito seguro para la construcción de aplicaciones, la verificación de identidad, el almacenamiento de datos y la verificación de la integridad de la información.

Figura 7.

Tecnologías usadas en ciberseguridad



Fuente. Elaboración propia

Así mismo, el uso del Cloud Computing plantea desafíos estrechamente relacionados con la privacidad, la protección de datos, la seguridad de los servicios y/o aplicaciones alojadas en la nube pública, sin embargo, también ofrece ventajas en términos de escalabilidad, redundancia y recuperación ante desastres, siempre que se apliquen buenas prácticas de adopción y de seguridad. Además, la encriptación utilizada para asegurar la confidencialidad y la integridad de la información que se encuentra en tránsito o en consumo por un punto final brinda un beneficio adicional en incorporar una barrera adicional como protección para los datos e impedir accesos no autorizados.

Finalmente, soluciones como los Anti-Phishing utilizan diferentes tecnologías para identificar y bloquear intentos de phishing, que consisten en engañar a usuarios para que revelen información personal o confidencial, donde el Procesamiento de Lenguaje Natural (NLP) permita analizar y clasificar grandes cantidades de texto en busca de contenido malicioso o sospechoso, como también las Redes Neuronales

Convolutionales (CNN) que aplica el análisis de imágenes para detectar anomalías y características maliciosas.

En síntesis, la aplicación de tecnologías emergentes como las ya mencionadas, han revolucionado la ciberseguridad al proporcionar herramientas innovadoras para la detección y prevención de amenazas cibernéticas. Estas tecnologías permiten una respuesta más rápida y efectiva ante los desafíos de seguridad actuales, fortaleciendo la protección de sistemas y datos frente a las crecientes y sofisticadas tácticas de los ciberdelincuentes como lo es la ciberseguridad social.

CAPÍTULO 4: FRAMEWORK PARA LA GESTIÓN DE LA CIBERSEGURIDAD SOCIAL EN UNIVERSIDADES PRIVADAS (SCERA)

4.1. Motivación

En los últimos años, las instituciones educativas han experimentado una transformación hacia la adopción digital de manera acelerada, donde la introducción de nuevas tecnologías ha mejorado significativamente la colaboración y la cercanía entre estudiantes, docentes y personal administrativo. Aun así, a medida que crecen en dependencia de estos activos digitales, es imperativo educar sobre seguridad y ética en el ciberespacio. Según la Unión Internacional de Telecomunicaciones (*International Telecommunication Union*), ITU por sus siglas en inglés, en su informe donde mide el índice de Ciberseguridad Global durante el 2024, detalla que a nivel mundial existe una deficiencia en la elaboración de estrategias mucho más eficaces para realizar actividades de concientización y adopción sobre la ciberseguridad, donde el Perú demuestra un compromiso básico en ciberseguridad, planteando un desafío continuo, en especial en el contexto social, donde el comportamiento de los usuarios internos de las universidades también son jugadores cruciales en la prevención y mitigación de incidentes.

Así mismo, el aumento del uso de la tecnología en las universidades ha provocado una preocupación notoria sobre la conciencia, la preocupación y el conocimiento previo sobre ciberseguridad que tienen los usuarios internos de las universidades, orientándose siempre hacia la victimización. Bajo ese contexto, surge el concepto emergente denominado "ciberseguridad social", que se refiere a cuáles son

las estrategias y políticas que permitan minimizar los riesgos cibernéticos a través de la concientización y comportamiento adecuado de los usuarios internos de las universidades. De esta manera, nace el desafío para las universidades privadas de diseñar un marco de trabajo que integre estas consideraciones en sus buenas prácticas de ciberseguridad, especialmente en Perú, donde el entorno normativo y tecnológico aún se encuentran en vías de desarrollo.

Según la Presidencia del Consejo de Ministros (PCM), en el Decreto Supremo N.º 085-2023-PCM, que aprueba la Política Nacional de Transformación Digital al 2030, el Perú enfrenta desafíos en cuanto al limitado desarrollo de la seguridad y confianza digital en la sociedad. Así mismo, en el Decreto Supremo N.º 029-2021-PCM se aprueba un marco de la seguridad digital, y establece los principios y componentes del modelo de seguridad digital. En febrero de 2024, y ante la falta de un equipo de respuesta a incidentes de seguridad digital, las universidades públicas se consideran infraestructuras críticas. A pesar de los esfuerzos para mejorar la cultura de ciberseguridad dentro de ellas, aún carecen de un enfoque holístico que aborde las dimensiones sociales de la seguridad cibernética. Además, de acuerdo con el Centro Nacional de Planeamiento Estratégico (CEPLAN), el país espera que las ciberamenazas crezcan a la par del progreso de la tecnología, llegando hasta un 67% en 2030. También se señala que la falta de recursos dedicados a la formación en ciberseguridad no solo ocasionará barreras tecnológicas, sino también daños físicos en los usuarios.

En el estudio de Eshetu (2024), se halló que las universidades de Etiopía eran vulnerables a infracciones cibernéticas dentro de sus sistemas web, dejando también en evidencia la falta de involucramiento por parte de los usuarios internos de las universidades. Por otra parte, las innovaciones tecnológicas demandan mayores conocimientos y habilidades por parte de los usuarios con la finalidad de democratizar la ciberseguridad a lo largo de la vida para todos, es por ello que Madrigal (2023) señala que es importante una buena preparación en tópicos basados en ciberseguridad y ciberdefensa desde los entornos universitarios, no solo enfocándose principalmente en los aspectos técnicos como la protección de redes y sistemas de información, sino teniendo en consideración la cultura digital.

A pesar de los esfuerzos realizados, no se ha podido corroborar un análisis en las dimensiones sociales de la ciberseguridad en universidades privadas. Estos estudios han puesto de manifiesto las amenazas técnicas existentes, pero sin profundizar en el

análisis de factores sociales que influyen en la ciberseguridad en las universidades privadas. Los modelos propuestos detallan su atención principalmente en la infraestructura técnica, minimizando los aspectos esenciales como el comportamiento de los usuarios y la cultura en torno a la seguridad digital. Esta carencia en la literatura crea una necesidad de proponer un modelo que incluya dimensiones sociales que sean esenciales para una ciberseguridad efectiva en universidades. Además, la falta de estudios que integren estos factores en un modelo para la gestión de la ciberseguridad social pone de manifiesto la necesidad de atender el tema.

El objetivo del estudio es diseñar un modelo para gestionar la ciberseguridad social en universidades privadas, basado en seis variables clave identificadas a partir de la revisión de la literatura. Este modelo proporciona a las universidades privadas una herramienta práctica para fortalecer su seguridad a través de la gestión de estas variables.

El modelo propuesto tendrá un enfoque interdisciplinario, combinando elementos de la cultura organizacional, la seguridad informática y la gestión normativa, buscando optimizar las prácticas de seguridad en respuesta a las amenazas cibernéticas mediante una mayor involucración de todos los actores sociales de las universidades privadas.

4.2. Factores humanos y comportamiento

La ciberseguridad es descrita como un fenómeno sociotécnico, que no solo se enfoca en la tecnología aplicada para defender, sino también en la interacción de las personas con los entornos y sistemas. McAlaney (2020) menciona que para poder desarrollar nuevas estrategias que permitan prevenir y mitigar riesgos, no solo se debe centrar en los atacantes o defensores, sino también a los usuarios que interactúan con los sistemas tecnológicos.

Por otra parte, Wu (2024) discutió acerca de cómo las personas equilibran constantemente el intercambio de información personal, sea dada a conciencia o no, con la creación de la confianza social, tanto fuera como dentro del ciberespacio, dejando como consecuencia una “brecha técnico-social” dentro de la ciberseguridad. Además, concluye que la influencia de los grupos sociales como las relaciones familiares, conocidos sociales y el público en masa pueden motivar a conductas positivas de seguridad y privacidad.

Por último, Shah (2023) evaluó la influencia de los factores humanos y la efectividad de políticas dentro de la ciberseguridad en dos regiones culturalmente distintas (Estados Unidos y Emiratos Árabes Unidos). En ambas regiones se destaca que el 31% de los encuestados experimentaron incidentes de ciberdelincuencia en lugares públicos, de trabajo y universidades. Por ello, se sugiere que debe considerarse una estrategia efectiva que incluya el desarrollo de habilidades técnicas, como la promoción de una cultura de ciberseguridad robusta definida en normas legales que reflejen ser adaptables a cualquier contexto sociocultural.

4.3. Ciberseguridad en entornos específicos

Según Nguyen (2020), las técnicas de ingeniería social se utilizan para comprometer la seguridad en instituciones de educación superior, destacando que la manipulación de la interacción humana es la principal técnica que afecta tanto a los sistemas como a las personas. Además, define al entorno educativo como dinámico y vulnerable, ya que al existir una alta rotación de personal y de estudiantes propone un modelo basado en el entrenamiento y la concienciación bajo un aprendizaje pasivo mediante tres fases: incorporación, concientización y actualización.

Así mismo, Erendor (2022) se enfocó en evaluar la eficacia de los programas de concientización en ciberseguridad en un entorno en línea. Durante el análisis, revela que los estudiantes desconocen sobre conceptos básicos de ciberseguridad y medidas esenciales que les permitan protegerse contra técnicas de engaño como el Phishing, Vishing, etc. Por último, propone incrementar la competencia técnica como la enseñanza sobre las dimensiones legales del cibercrimen, bajo marcos, normas y herramientas de comunicación capaces de intervenir en la experiencia preparativa de los estudiantes en formas de cómo navegar e interactuar de manera segura en un mundo digitalizado.

4.4. Modelos existentes

En la literatura revisada, se han desarrollado diversos modelos, por ejemplo, Rodriguez (2024) hace una revisión sistemática sobre la ciberseguridad social identificando aspectos como factores y modelos.

Khader (2021) propone un Marco de Concientización sobre Ciberseguridad para el Sector Académico (CAFA) orientado a la mejora de la conciencia sobre

ciberseguridad, enfocándose en la integración de las personas dentro del entorno, el desarrollo de las actividades, la entrega de procedimientos y controles, y, finalmente, la evaluación del conocimiento de la ciberseguridad a través del currículo universitario. Con ello logra enmarcar una guía base para las instituciones en cómo crear o modificar los procedimientos y políticas alineadas tanto a la ciberseguridad como a sus misiones institucionales.

Por otra parte, Hijji (2022) diseñó explícitamente un Marco de capacitación y concientización sobre ciberseguridad (CAT) para empleados que trabajan de forma remota que permita abordar una personalización de la educación y la formación en ciberseguridad no solo frente a las amenazas técnicas, sino también las manipulaciones sociales que pueden comprometer la seguridad de los clientes y el personal. Esto bajo tres niveles: la conciencia a partir de conceptos básicos, la formación mediante entrenamientos técnicos y la práctica/evaluaciones basadas en simulaciones.

Finalmente, Ramezianian (2024) construyó un Marco para el Desarrollo de la Educación en Ciberseguridad (FCED) con la finalidad de mejorar los programas educativos incorporando aspectos técnicos como sociales de la ciberseguridad, consultando marcos de trabajo reconocidos a nivel mundial como el NICE (National Initiative for Cybersecurity Education) y CSEC2017 (Cybersecurity Curricular Guidance 2017). Todo ello estructurado bajo cinco etapas, iniciando por la integración de competencias a la malla curricular, continuando con el desarrollo de competencias tecnológicas, luego evaluando y aplicando mejoras continuas asegurando una actualización constante, para después colaborar interdisciplinariamente entre departamentos académicos y finalizar con la ejecución de laboratorios y simulaciones que preparen a las personas a enfrentar riesgos técnicos y sociales en la ciberseguridad.

4.5. Hipótesis

4.5.1. Seguridad técnica como punto de partida

Actualmente, las medidas de seguridad técnica se desencadenan en sistemas robustos, los cuales permiten utilizar buenas prácticas en el ambiente digital, por ello, herramientas como el cifrado y el control de acceso son esenciales para dar una integridad y protección a los datos, asegurando que los datos no sean alterados, eliminados o sustraídos de manera indebida. Así mismo, el ejercer prácticas de

ingeniería o incorporar controles técnicos basándose en metodologías ya existentes, de la mano con un control organizacional, puede aportar en la protección de los datos, dejando en evidencia que para abordar una privacidad de datos se debe considerar un enfoque integrado a la ingeniería de la privacidad.

Por otra parte, Nejari (2024) detalla que el atractivo, la visibilidad y la tutela técnica son aspectos clave para crear oportunidades de ejecutar un ciberdelito, dejando en evidencia que las violaciones de seguridad parten de un mal uso de medidas técnicas dejando brechas de datos y sus consecuencias. Por otra parte, Oyewole (2024) discute la importancia de la adaptabilidad en las regulaciones y cómo de la mano con la seguridad técnica influye directamente en la privacidad de los datos, sugiriendo que una gestión efectiva de la ciberseguridad debe enmarcarse en la protección del consumidor o cliente final mediante la privacidad de datos, apoyándose de herramientas técnicas robustas.

Con la creciente ola de adopción de la inteligencia artificial generativa en múltiples sectores, es oportuno considerar la seguridad técnica y la gestión de consentimientos explícitos como las principales fuentes del aseguramiento de los datos, no solo con el fin de cumplir con requisitos legales, sino también para brindar una confianza a los usuarios que utilizan los medios digitales. Por lo tanto, se formula la siguiente hipótesis:

- Hipótesis 1 (H1). La “Seguridad técnica (ST)” influye positivamente en la “Privacidad de Datos (PD)”.

4.5.2. Aseguramiento de la privacidad de datos

En un mundo digitalizado, son los usuarios finales quienes adoptan comportamientos de protección de datos como un mecanismo para gestionar su propia privacidad frente a la recolección y uso de los datos por parte de instituciones y empresas, influyendo así en el surgimiento de una preocupación donde se destacan las acciones protectoras de la privacidad y el uso responsable de los datos, los cuales de manera relacionada abren el camino hacia el surgimiento de nuevas prácticas responsables y éticas en la forma de gestionar la recolección de datos. Así mismo, con la llegada de tecnologías emergentes como el metaverso, la inteligencia artificial y el procesamiento de lenguaje natural, es importante asegurar que los datos que se manejen en entornos digitales cuenten con una gestión de carácter moral y honesto, así

como el uso consciente y sensato para brindar un bienestar satisfactorio a los usuarios basado en la confianza y en la transparencia.

Ogbuke (2022) destaca la necesidad que las organizaciones e instituciones asuman una mayor responsabilidad en la gestión y uso que les dan a los datos, con la finalidad de brindar confianza a los consumidores y mitigar riesgos legales o éticos asociados a un problema de fuga de información. Así mismo, Anshari (2022) discute cómo la privacidad y la responsabilidad de los datos se encuentran relacionadas, resaltando que una violación a la privacidad no solo implica riesgos éticos, sino también legales y manejo responsable de la tecnología para garantizar una confianza en el mundo digital.

Es por lo que al manejar datos confidenciales podría ayudar a mitigar riesgos asociados que podrían ocasionar pérdidas monetarias, y, sobre todo, mantener la aprobación pública al mostrar transparencia dentro de los procesos y el correcto manejo de los datos. Es así como se aborda la siguiente hipótesis:

- Hipótesis 2 (H2). La “Privacidad de Datos (PD)” influye positivamente en la “Responsabilidad de los Datos (RD)”.

4.5.3. Reconocimiento de los riesgos cibernéticos

La adopción de tecnologías con la finalidad de mejorar la privacidad de los datos en pequeñas y medianas empresas está motivada por el aumento de la conciencia sobre los riesgos cibernéticos, además de ser impulsado por las regulaciones gubernamentales detalladas por cada país, los cuales ayudan a mostrar una relación directa entre cómo la seguridad técnica es resultado latente de un reconocimiento del riesgo. Por otra parte, en una cadena de suministro o un ambiente con un producto altamente rotativo, tecnologías como el blockchain han demostrado una protección significativa contra la falsificación, la manipulación y la ejecución de las transacciones digitales, asegurando una integridad de los datos y demostrando que el surgimiento de nuevos riesgos latentes puede ser mitigados por un aseguramiento técnico siempre y cuando sea adoptado y regulado.

Shaikh (2023) menciona que los altos costos que generan las brechas de ciberseguridad incrementan la atención de gestores de diversas áreas dentro de una empresa o institución, por lo cual se fomentan evaluaciones de riesgos que refuercen la seguridad técnica, pero que, a su vez, cuenten con un enfoque en la mejora continua de la preparación, respuesta y resiliencia frente a posibles brechas futuras. Así mismo,

Durst (2024) revela que la gestión absoluta de los riesgos cibernéticos mejora directamente la seguridad técnica, puesto que con ello los gestores de la ciberseguridad se encuentran preparados para afrontar un ataque cibernético. Además, son mucho más resilientes frente a las adversidades que puedan ocasionar ataques malintencionados, evitando así las pérdidas de confianza o monetarias significativas para instituciones y empresas.

Con los altos costos que pueden provocar las brechas de ciberseguridad, se impulsan las inversiones tomadas por las instituciones y empresas en adoptar o contratar medidas de seguridad técnica, con la finalidad de evitar posibles violaciones de acceso o fugas de información, los cuales pueden ser negativos en caso sucedan, pero que al prevenir son un principal catalizador para fortalecer la infraestructura tecnológica. Por consiguiente, se plantea la siguiente hipótesis:

- Hipótesis 3 (H3). Los “Riesgo de Ciberseguridad (RC)” influyen positivamente en la “Seguridad Técnica (ST)”.

4.5.4. Normativa aplicada

Actualmente, las regulaciones ejercen una influencia significativa en la toma de decisiones de personas, instituciones, empresas y gobiernos, las cuales son estructuradas no solo con buenas prácticas o guías, sino también con motivaciones que permitan evitar sanciones frente a sus incumplimientos ocasionados por riesgos, impulsando así una gestión más rigurosa y consciente de los problemas existentes. Es por ello por lo que al crear normativas de ciberseguridad donde se establezcan modelos y marcos de trabajo se puede lograr contar con una eficaz manera de manejar los riesgos cibernéticos, permitiendo a las instituciones anticiparse y reducir las posibles brechas de seguridad latentes.

Sharma (2024) resalta que el incumplimiento de regulaciones puede ocasionar una pérdida de datos y un aumento de los riesgos cibernéticos, enfatizando que una correcta gestión debe darse de manera rigurosa para poder cumplir con los altos estándares de seguridad y protección de datos. Asimismo, Abrahams (2024) menciona que estándares como la ISO 27001 y el NIST Cybersecurity Framework son fundamentales para mitigar los riesgos de ciberseguridad, destacando la importancia de las buenas prácticas y de las regulaciones existentes con la finalidad de proteger la información sensible y combatir las amenazas cibernéticas.

Así mismo, los cambios regulatorios pueden afectar negativamente en las estrategias de inversión en ciberseguridad de las organizaciones, sobre todo si están en la búsqueda de minimizar riesgos y mejorar la protección, llevándolas a adoptar una postura pasiva frente a qué regulación seguir.

Por otro lado, las estrategias o regulaciones existentes en materia de ciberseguridad están intrínsecamente vinculadas con la gestión de riesgos cibernéticos, puesto que plantean desafíos significativos al momento de elaborar nuevas normas basadas en tecnologías recientes en el mercado digital, dificultando un esfuerzo práctico hacia un liderazgo globalizado en ciberseguridad. Así mismo, las buenas prácticas técnicas y los actos legislativos ejercidos por gobiernos permiten una estructuración de modelos referentes de seguridad de la computación, donde prima la ciberresiliencia.

En la investigación de Kryshchanovych (2023), se discute cómo las normativas estatales mejoran la seguridad técnica, implementando tecnologías de seguridad, controles sistematizados, auditorías periódicas y formación en ciberseguridad, estableciendo así una integridad técnica que permita gestionar la seguridad en las empresas. Además, Saeed (2023) menciona que la motivación y percepción de la seguridad influye directamente en la implementación de políticas y medidas técnicas de seguridad de la información, pero también es necesario contar con una infraestructura legal y tecnológica capaz de garantizar un ecosistema digital de confianza para los clientes.

Es así como las normativas de ciberseguridad son jugadores principales en el fortalecimiento de la seguridad técnica, argumentando que un marco regulatorio robusto no solo puede mejorar la gestión de riesgos, sino también elevar las prácticas de seguridad técnica al estandarizar los procesos, procedimientos y protocolos frente a las amenazas cibernéticas. En discusión a ello, se formulan las siguientes hipótesis:

- Hipótesis 4 (H4). Las “Normativas de Ciberseguridad (NC)” influye positivamente en el “Riesgo de Ciberseguridad (RC)”.
- Hipótesis 5 (H5). Las “Normativas de Ciberseguridad (NC)” influye positivamente en la “Seguridad técnica (ST)”.

4.5.5. Concientización en ciberseguridad

En la sociedad actual, son las normativas quienes crean una mayor capacidad de respuesta que adoptan las cadenas de suministro frente a alguna crisis, puesto que

al contar con una toma de conciencia de manera preliminar se permite guiar a las personas en cómo reforzar sus capacidades reactivas frente a escenarios adversos, forjando así un cumplimiento de las políticas que resultan en un ambiente más seguro y preparado. Es por ello por lo que se considera crítico el implementar y cumplir con las normativas de ciberseguridad (sean gubernamentales o empresariales), ya que, de esta manera, se puede proteger mejor a los usuarios en línea.

En el estudio de Nwankpa (2023), se ilustra cómo el aumento de concientización en ciberseguridad, especialmente en personas de edades tempranas, permite una mejor comprensión de los riesgos cibernéticos. Estas personas, en el futuro, impactarán en las normas o regulaciones existentes con el fin de mejorarlas y convertirlas en más estrictas y, de esta manera, crear un ciberespacio seguro. También Mittal (2024) destaca que la creciente toma de conciencia sobre la ciberseguridad en los adolescentes es esencial para desarrollar estrategias efectivas contra los ciberdelincuentes, estimulando a que las normas sean mucho más robustas y orientadas a grupos vulnerables que hayan sido víctimas de malhechores digitales.

Por ello, las iniciativas de educación se destacan como principios fundamentales capaces de equipar a los adolescentes con el conocimiento y las habilidades necesarias (que pueden ser sociales y/o técnicas) para navegar de manera segura dentro del ciberespacio, protegiendo así los datos y contribuyendo a la seguridad de una institución o nación con la creación de políticas o modificaciones reglamentarias.

Por otra parte, al comprender mejor los riesgos y vulnerabilidades cibernéticas, los usuarios del área tecnológica pueden orientarse a construir prácticas que protejan los datos contra accesos no autorizados o manipulaciones indebidas, fundamentándose en generar confianza mediante el cumplimiento de regulaciones. Actualmente, mediante el aprendizaje de máquina pueden crearse modelos que acumulen conocimientos sobre cómo aprender de diversas tareas de seguridad, los cuales pueden ser implementados instantáneamente para proteger a las organizaciones e instituciones contra amenazas emergentes, reforzando la responsabilidad organizacional sobre la recopilación, el tratamiento y la protección de los datos.

Para Sulaiman (2022), la generación de conciencia frente a las amenazas emergentes impacta en la percepción de la severidad y vulnerabilidad de los riesgos cibernéticos, evidenciando que una mejor apreciación de la vulnerabilidad y la gravedad de las amenazas puede motivar a la creación de prácticas responsables en la

gestión de datos, conduciendo a comportamientos de seguridad efectivos. Así mismo, Argyridou (2023), mediante una encuesta basada en el riesgo, analizó cómo el nivel de concienciación impacta en las prácticas de responsabilidad de datos, donde se identificó que los empleados de una institución u organización con un alto nivel de conocimiento en ciberseguridad son más propensos a implementar, seguir prácticas y establecer controles que protegen la integridad y la confidencialidad de los datos que manejan.

La implementación de protocolos de ciberseguridad integrados con la educación y la capacitación continua en ciberseguridad son esenciales para que las instituciones y empresas no solo respondan a los incidentes, sino que también anticipen, resistan y mitiguen proactivamente los riesgos cibernéticos, estableciendo una base sólida para la protección de datos y la confianza. Como consecuencia a lo descrito, se proponen las siguientes hipótesis:

- Hipótesis 6 (H6). La “Concientización de la Ciberseguridad (CC)” influye positivamente en las “Normativas de Ciberseguridad (NC)”.
- Hipótesis 7 (H7). La “Concientización de la Ciberseguridad (CC)” influye positivamente en la “Responsabilidad de los Datos (RD)”.

La tabla 5 presenta las 7 hipótesis planteadas:

Tabla 5

Hipótesis planteadas

ID	Descripción
H1	La “Seguridad técnica (ST)” influye positivamente en la “Privacidad de Datos (PD)” $ST > PD$
H2	La “Privacidad de Datos (PD)” influye positivamente en la “Responsabilidad de los Datos (RD)” $PD > RD$
H3	Los “Riesgo de Ciberseguridad (RC)” influyen positivamente en la “Seguridad Técnica (ST)” $RC > ST$
H4	Las “Normativas de Ciberseguridad (NC)” influye positivamente en el “Riesgo de Ciberseguridad (RC)” $NC > RC$
H5	Las “Normativas de Ciberseguridad (NC)” influye positivamente en la “Seguridad técnica (ST)” $NC > ST$

CAPÍTULO 5: VALIDACIÓN

5.1. Metodología y diseño de la investigación

5.1.1. Tipo y diseño de la investigación

La presente investigación se enmarca en un enfoque de tipo aplicada, donde se busca abordar un problema práctico y desarrollar una solución concreta. Para ello, se utiliza un diseño de investigación en la ciencia del diseño, el cual se caracteriza por su enfoque en responder ante un paradigma mediante la elaboración de un artefacto, con la finalidad de contribuir con un avance teórico como práctico del problema a investigar (Hevner et al., 2010).

Así mismo, el nivel o alcance de la investigación se basa en un estudio descriptivo, ya que se busca comprender y describir la situación actual de la ciberseguridad social en el contexto universitario, así como proponer estrategias y pautas de acción. Además, se utiliza un enfoque cuantitativo para recopilar y analizar cifras de datos (Hernández et al., 2014) relacionados con la gestión de la ciberseguridad social en las instituciones privadas de nivel superior.

5.1.2. Unidad de análisis

En el marco de la investigación, se ha definido que la unidad de análisis se basará en las áreas de tecnología de la información que cuentan las universidades ubicadas en el departamento de Lima, de tipo gestión privada. Esto implica que, al delimitar claramente la unidad de análisis en las áreas de tecnología de las universidades de Lima, se espera obtener información detallada que posibilite abordar las preguntas de investigación formuladas anteriormente y permita cumplir los objetivos establecidos en este estudio.

5.1.3. Población y muestra

La población de estudio en la presente investigación abarca a todas aquellas personas que se dedican a la gestión de tecnologías de la información y a la gestión de la ciberseguridad en instituciones educativas privadas de nivel superior ubicadas en el departamento de Lima, Perú. La inclusión de todas las instituciones, exclusivamente licenciadas y avaladas por la Superintendencia Nacional de Educación Superior Universitaria (SUNEDU), tiene como objetivo obtener una visión completa y

representativa de la gestión de la ciberseguridad social en el contexto educativo de Lima y facilitar la extrapolación de los resultados obtenidos.

Dentro de la investigación, el tamaño de la muestra será finito. De un total de 145 universidades listadas por la Superintendencia Nacional de Educación Superior Universitaria (SUNEDU) en el Perú, se considerarán únicamente 30 universidades privadas en Lima debido a que se encuentran activas y licenciadas por la Superintendencia Nacional de Educación Superior Universitaria (SUNEDU).

La muestra para este estudio de investigación es no probabilística, empleándose la técnica de muestreo por conveniencia, lo cual implica seleccionar los casos de manera accesible, sin aplicar un proceso de selección aleatorio. Por tal motivo, se tomarán en cuenta consideraciones prácticas y factores de conveniencia para determinar qué universidades o participantes formarán parte de la muestra (Hernández y Carpio, 2019) para su selección.

Por ello, se seleccionarán las universidades privadas que se encuentren en el departamento de Lima, pero que cuenten con áreas de tecnología de la información donde permitan la ejecución del instrumento, obteniendo una muestra total de 30 universidades privadas que cumplen con estos criterios.

5.1.4. Recolección de datos

La técnica de recolección de datos que será utilizada en este estudio consistirá en una variedad de actividades diseñadas para obtener la información necesaria y así evaluar y en consecuencia responder al problema de investigación planteado (Hurtado, 2000). En síntesis, se aplicará un cuestionario que será representado por un instrumento que permitirá la recolección de datos. Este instrumento se basará en seis dimensiones y dieciocho indicadores. Al final de la construcción del instrumento, este será evaluado bajo la escala de Likert.

En proceso de análisis se llevará a cabo mediante la clasificación, registro y codificación de los datos obtenidos a partir de la encuesta con escala de Likert. Todos los datos recopilados serán organizados y categorizados de acuerdo con las dimensiones y preguntas establecidas en el instrumento. Así mismo, cada respuesta tendrá asignada una categoría específica, lo que permitirá su posterior análisis. Durante el proceso de clasificación, se asignará un valor numérico a cada categoría para facilitar el análisis estadístico con la finalidad de cuantificar las respuestas.

Para comprobar la hipótesis, se emplearán técnicas estadísticas para evaluar la relación entre las variables y realizar inferencias sobre la población. Dado que la escala de Likert implica una variable ordinal, se utilizarán pruebas estadísticas no paramétricas, como la prueba de Friedman y la correlación de Spearman (Quispe et al., 2019). Estas pruebas permitirán identificar patrones y posibles relaciones entre las dimensiones evaluadas en la encuesta.

5.1.5. Procedimiento

Este estudio se realizó en una sola fase, abarcando todo el proceso de diseño, distribución, recopilación y análisis del cuestionario, el cual se desarrolló siguiendo los pasos detallados a continuación:

- Se utilizó el listado de las instituciones privadas de educación superior de Lima Metropolitana Licenciadas por Sunedu (<https://www.sunedu.gob.pe/lista-de-universidades-licenciadas/>).
- Se diseñó el cuestionario (Anexo E), el cual fue validado mediante el juicio de expertos (Anexo F).
- Se redactó una carta de solicitud dirigida a las áreas de tecnología de las instituciones educativas de nivel superior de Lima Metropolitana. Esta carta se remitió en formato digital mediante correo y vías de comunicación colectiva como LinkedIn, WhatsApp y Messenger (Anexo G).
- Se realizó una encuesta virtual utilizando Microsoft forms (<https://forms.office.com/r/UD8q6TtnpR>), dirigida a gerentes, jefes, directores, y/o responsables de las áreas de tecnología de las instituciones educativas de nivel superior de Lima Metropolitana, durante el periodo de agosto a noviembre de 2024.
- Se recopilaron las respuestas, sumando un total 33, de las cuales 3 fueron eliminadas por presentar información incongruente.
- Con 30 respuestas corroboradas, se procedió a ejecutar el análisis estadístico correspondiente.
- Finalmente, se obtuvo la apreciación y/o perspectiva de los encuestados sobre los constructos de la ciberseguridad que influyen en la gestión de la ciberseguridad social dentro de las instituciones privadas de educación superior de Lima Metropolitana.

5.1.6. Confiabilidad de datos

La presente investigación se validará estadísticamente las relaciones del framework SCERA (ver Figura 8) mediante el modelado de ecuaciones estructurales, obteniendo así un análisis de confiabilidad y validación del framework propuesto a través de la técnica de mínimos cuadrados parciales (Partial Least Squares Structural Equation Modelling, PLS-SEM). En detalle, el análisis comprende cuatro etapas: a) la Fiabilidad Individual de los ítems, b) la Fiabilidad de los Constructos, que se evaluará a través del Alfa de Cronbach y la Fiabilidad Compuesta, c) la Validez Convergente, que indica la extensión en la que los distintos indicadores de un constructo se relacionan entre sí, donde para establecer la validez convergente se empleará la fiabilidad de los indicadores (cargas externas) y la varianza media extraída (AVE) y finalmente d) la Validez Discriminante, que se evalúa a través del criterio Fornell-Larcker y el ratio HTMT.

5.1.7. Análisis e interpretación de datos

En proceso de análisis se llevará a cabo mediante la clasificación, registro y codificación de los datos obtenidos a partir de la encuesta con escala de Likert. Todos los datos recopilados serán organizados y categorizados de acuerdo con las dimensiones y preguntas establecidas en el instrumento. Así mismo, cada respuesta tendrá asignada una categoría específica, lo que permitirá su posterior análisis. Durante el proceso de clasificación, se asignará un valor numérico a cada categoría para facilitar el análisis estadístico con la finalidad de cuantificar las respuestas.

Para comprobar la hipótesis, se emplearán técnicas estadísticas para evaluar la relación entre las variables y realizar inferencias sobre la población. Dado que la escala de Likert implica una variable ordinal, se utilizarán pruebas estadísticas no paramétricas, como la prueba de Friedman y la correlación de Spearman (Quispe et al., 2019). Estas pruebas permitirán identificar patrones y posibles relaciones entre las dimensiones evaluadas en la encuesta.

5.2. Resultados y Discusión

5.2.1 Análisis de los datos

Se elaboró un modelo de investigación para probar la relación entre 6 variables o constructo detalladas en la Tabla 6, donde se aplica la técnica estadística

multivariante denominada PLS-SEM, que se utiliza con frecuencia en diversas disciplinas de la investigación empresarial a través del software SMARTPLS, versión 4.0, proporcionado por Ringle, siendo elegida por ser una técnica adecuada para analizar los constructos del artefacto propuesto como lo ejecuta Henseler (2015), además de ser adecuada para analizar modelos con relaciones directas entre variables como lo indica Roldan (2012).

Tabla 6

Constructos considerados

ID	Descripción del constructo
RC	Riesgo de ciberseguridad
NC	Normativas de ciberseguridad
CC	Concientización de ciberseguridad
ST	Seguridad técnica
PD	Privacidad de los datos
RD	Responsabilidad de los datos

Fuente: Elaboración propia.

El estudio se basó en 30 universidades privadas de Lima Metropolitana mediante un muestreo de conveniencia no probabilístico, en el que la totalidad de los participantes aceptaron participar de manera voluntaria, como también lo evidencia Domínguez-Lara (2018). Este método de muestreo se justificó teniendo en cuenta las limitaciones de tiempo y recursos. Por lo tanto, al emplear un muestreo no probabilístico de conveniencia, se tuvo acceso a una muestra diversa de los líderes de las áreas de TI de las universidades privadas, lo que garantizó la fiabilidad de los resultados. Aunque este método de muestreo no garantiza la representatividad estadística del total de la población universitaria privada a nivel país, proporciona información valiosa y orientativa sobre las actitudes hacia la ciberseguridad social en el ámbito universitario. En cuanto a las características sociodemográficas (ver Tabla 7), se aprecia una mayor proporción de hombres (70%) que mujeres (30%) que participaron dentro del estudio, al igual que la edad de los participantes, donde se aprecia que un 43% oscilaba entre los 35 y los 44 años, lo que sugiere que se son líderes relativamente jóvenes.

Tabla 7

Perfil sociodemográfico de la muestra (n=30)

Item		N	%
Experiencia en sector educativo	Menos de 1 año	1	3
	De 1 a 5 años	9	30
	De 6 a 10 años	12	40
	De 11 a 20 años	5	17
	De 21 a 25 años	3	10
Experiencia laboral	De 1 a 5 años	5	17
	De 6 a 10 años	7	23
	De 11 a 20 años	12	40
	De 21 a 25 años	2	7
	De 26 a 30 años	3	10
Conoce sobre Ciberseguridad Social	Más de 30 años	1	3
	Si	11	37
	No	19	63

Fuente: Elaboración propia.

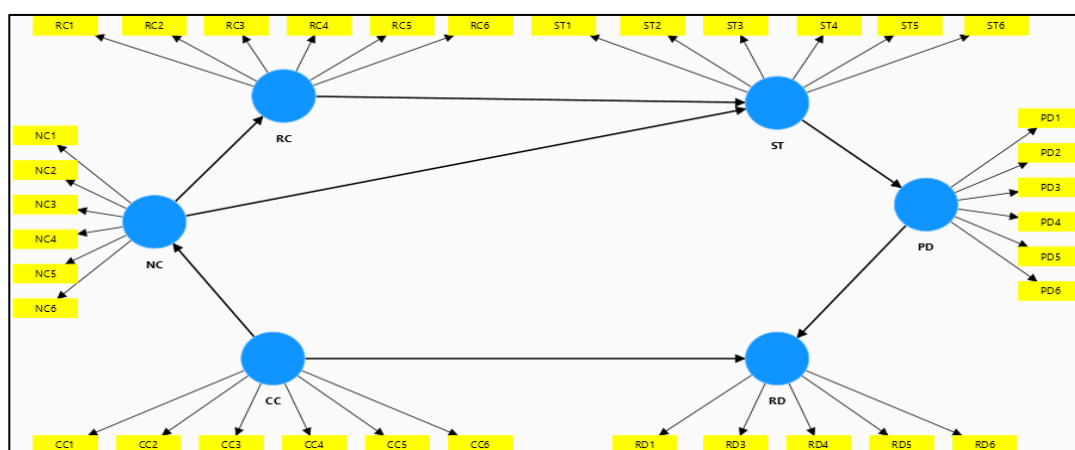
El análisis demográfico pone en manifiesto una distribución entre el nivel de estudios de los participantes, debido a que el 40% tiene un posgrado, el 43% ha culminado sus estudios universitarios y el 17% no culminó. Además, se revela que los participantes tenían experiencia previa en el sector de educación universitaria, evidenciando que un 40% tiene de 6 a 10 años de experiencia, el 17% tienen de 11 a 20 años y, finalmente, el 10% tiene entre 21 a 25 años de experiencia. Esto proporciona información relevante respecto al amplio dominio de los participantes en el sector educación superior en el Perú. Por último, es pertinente mencionar que el 63% de los participantes en el estudio no tiene conocimiento sobre lo que es la ciberseguridad social, siendo significativo, porque permite evidenciar que las algunas de las respuestas no pueden representar la situación actual sobre la ciberseguridad social del sector educativo. Todos los procedimientos aplicados en la encuesta fueron aprobados por las universidades seleccionadas para el estudio, dando así su consentimiento anónimo e informado.

5.2.2. Descripción del modelo en PLS-SEM

En la Figura 9 se muestra el modelo PLS-SEM dibujado en SMART-PLS, donde, en primer lugar, se importó el archivo .CSV que contiene los datos de las respuestas de los encuestados, luego se procedió a generar las 6 variables latentes (variables no observables) y se situaron los indicadores (variables observables) dentro de cada una de las variables correspondientes. Finalmente, se indicaron las 7 relaciones entre las variables latentes: $NC \rightarrow RC$, $NC \rightarrow ST$, $RC \rightarrow ST$, $ST \rightarrow PD$, $PD \rightarrow RD$, $CC \rightarrow NC$, y $CC \rightarrow RD$.

Figura 9.

Modelo de investigación a evaluar



Fuente: Elaboración propia.

Para obtener una validación del modelo, primero se debe determinar si las variables latentes o constructos empleados en el estudio sirven para definir y medir nuestras dimensiones. Para ello, en la siguiente sección, se mostrará la evaluación del modelo de medida

5.2.3. Evaluación del modelo de medida (Modelo exterior)

El análisis del modelo de medida se centra en evaluar el constructo y sus indicadores mediante cuatro etapas: a) la fiabilidad individual de los ítems, b) la fiabilidad de los constructos evaluados a través del Alfa de Cronbach y la Fiabilidad Compuesta, c) la validez convergente, el cual indica la extensión en la que los distintos indicadores de un constructo se relacionan entre sí, empleándose la Fiabilidad de los indicadores (cargas externas) y la varianza media extraída (AVE), finalmente, d) la

validez discriminante, que se evalúa a través del criterio Fornell-Larcker y el ratio HTMT.

Para determinar la consistencia interna: Alfa de Cronbach y Fiabilidad Compuesta, ambos indicadores toman valores entre 0 y 1. Mientras más se aproximen a 1, mayor es su nivel de fiabilidad. Por lo general, se aceptan valores entre 0.7 y 0.95. Valores menores a 0.7 indican falta de consistencia interna, mientras que valores superiores a 0.95 indican que todos los indicadores estarían midiendo el mismo fenómeno, y, por lo tanto, no es una medida válida del constructo, ya que se trataría de indicadores redundantes.

Para la validez convergente, se debe establecer fiabilidad del indicador de cada ítem, donde deberían de manifestar unas cargas externas extraídas superior a 0.708 y ser estadísticamente significativas, es decir, tener un valor de $p < 0.5$. En lo relativo a la Variable Media Extraída (AVE), esta debería tomar un valor $\geq$ a 0.5, lo que indicaría que, en promedio, el constructo explica el 50% más de la varianza de sus indicadores.

Finalmente, para validar la Validez Discriminante, el cual mide la extensión en la que los constructos son verdaderamente diferentes entre sí, se evalúa a través del criterio Fornell-Larcker, donde se compara la raíz cuadrada del AVE de cada constructo contra las correlaciones entre las variables latentes para establecer validez discriminante, donde la raíz cuadrada del AVE de cada constructo debe ser mayor que las correlaciones que este constructo mantenga con los demás constructos, mientras que el ratio HTMT debe ser menor que 0.85 y ser significativo, además, los intervalos de confianza no deben contener el 1 para determinar la validez discriminante.

5.2.4. Fiabilidad de los ítems

Como primer paso se analiza la fiabilidad compuesta de los ítems a través de sus cargas externas, definida como la relación que tiene el indicador con cada uno de sus constructos. En este caso, las cargas factoriales resultan ser superiores a 0,7 para la mayoría de los ítems, y nunca son inferiores a 0,4, límite que fue indicado por Hair (2011). Por lo tanto, queda un grupo de escalas con 36 ítems en el modelo propuesto como se aprecia a continuación en la Tabla 8.

Tabla 8*Modelo de medición de fiabilidad individual y de los constructos*

VARIABLES	RC	NC	CC	ST	PD	RD	Alfa de Cronbach
Riesgo de Ciberseguridad							0.927
RC1	0.797						
RC2	0.861						
RC3	0.814						
RC4	0.904						
RC5	0.899						
RC6	0.856						
Normativas de Ciberseguridad							0.921
NC1		0.892					
NC2		0.828					
NC3		0.853					
NC4		0.836					
NC5		0.864					
NC6		0.806					
Concientización de Ciberseguridad							0.925
CC1			0.865				
CC2			0.887				
CC3			0.867				
CC4			0.854				
CC5			0.770				
CC6			0.871				
Seguridad Técnica							0.911
ST1				0.871			
ST2				0.879			
ST3				0.918			
ST4				0.837			
ST5				0.707			
ST6				0.777			
Privacidad de Datos							0.885

PD1	0.787	
PD2	0.780	
PD3	0.816	
PD4	0.766	
PD5	0.856	
PD6	0.769	
Responsabilidad de Datos		0.929
RD1	0.886	
RD3	0.852	
RD4	0.901	
RD5	0.858	
RD6	0.916	

Fuente: Elaboración propia.

Cabe señalar que el ítem ST5 presenta una carga factorial de 0.707, ligeramente por debajo del umbral adoptado en esta tesis (0.708). Sin embargo, la diferencia es marginal (0.001) y, dado que el constructo Seguridad Técnica presenta una fiabilidad compuesta robusta ($CR = 0.911$) y un valor de $AVE = 0.696$, ambos superiores a los criterios mínimos recomendados, se decide mantener el ítem ST5 en el modelo para preservar la cobertura teórica del constructo.

5.2.5. Fiabilidad de los constructos

En segundo lugar, se examina la fiabilidad del constructo con el Alfa de Cronbach y el índice de fiabilidad compuesta (CR). Como se observa en la Tabla 8, en todos los casos el Alfa de Cronbach de las 6 variables latentes y la fiabilidad compuesta es >0.7 por lo cual queda comprobada la fiabilidad del constructo.

5.2.6. La validez convergente

En tercer lugar, se confirma la existencia de validez convergente mediante la Varianza Media Extraída (AVE, por sus siglas en inglés). Los resultados muestran un valor de fiabilidad compuesta (CR) que supera el valor crítico de 0,8 para todas las variables latentes como lo menciona Nunnally (1994) en su libro, y el valor AVE es superior a 0,5, detallado así que el constructo explica más del 50% de la varianza de

sus indicadores como lo detalla Fornell (1981), por lo que se verifica la fiabilidad y la validez convergente como se aprecia en la Tabla 9.

Tabla 9

Modelo de medición de validez convergente

Constructo	CR	AVE
Riesgo de Ciberseguridad	0.927	0.733
Normativas de Ciberseguridad	0.921	0.717
Concientización de Ciberseguridad	0.925	0.728
Seguridad Técnica	0.911	0.696
Privacidad de Datos	0.885	0.634
Responsabilidad de Datos	0.929	0.780

Fuente: Elaboración propia.

5.2.7. La validez discriminante

Por último, el análisis del modelo de medida consiste en la comprobación de la existencia de validez discriminante. Para confirmar la validez discriminante de los constructos del estudio, en primer lugar, se utilizó el criterio de Fornell y Larcker, que exige que la raíz cuadrada del AVE sea superior a la correlación entre constructos. Luego, se utilizó el enfoque de la razón de correlación heterotrait monotrait (HTMT - 90) propuesta por Henseler (2015), donde en la mayoría de los constructos, las pruebas de inferencia muestran que los intervalos de confianza no contienen el valor uno, lo que sugiere que dichas variables son empíricamente diferentes. Sin embargo, en el caso de Concientización de Ciberseguridad (CC) y Normativas de Ciberseguridad (NC), el valor HTMT alcanzó 1.003, excediendo el umbral recomendado (<0.85), mientras que en la matriz de Fornell-Larcker la correlación entre ambos constructos (0.927) superó la raíz cuadrada del AVE (0.853 y 0.847, respectivamente). Estos resultados evidencian que, si bien la mayoría de las escalas cumplen con los requisitos de validez discriminante, en el par CC–NC no se satisface plenamente, lo que puede deberse al solapamiento conceptual entre ambos factores y a la cercanía semántica de los ítems empleados, dejándolo como evidencia consignada en la Tabla 10.

Tabla 10*Validez discriminante*

Constructo	CC	NC	PD	RC	RD	ST
<i>Criterio Fornell and Larcker's (1981)</i>						
Concientización de Ciberseguridad	0.853					
Normativas de Ciberseguridad	0.927	0.847				
Privacidad de Datos	0.814	0.798	0.796			
Riesgo de Ciberseguridad	0.882	0.912	0.740	0.856		
Responsabilidad de Datos	0.857	0.827	0.860	0.829	0.883	
Seguridad Técnica	0.912	0.915	0.876	0.877	0.852	0.834
<i>Ratio Heterotrait-Monotrait HTMT</i>						
Concientización de Ciberseguridad						
Normativas de Ciberseguridad	1.003					
Privacidad de Datos	0.867	0.857				
Riesgo de Ciberseguridad	0.947	0.981	0.779			
Responsabilidad de Datos	0.921	0.888	0.917	0.886		
Seguridad Técnica	0.992	0.995	0.960	0.944	0.919	
Constructo	CC	NC	PD	RC	RD	ST

Fuente: Elaboración propia.

5.2.8. Evaluación del modelo estructural (Modelo exterior)

El modelo estructural se encarga de evaluar la relación entre variables latentes. Para determinar la significación estadística de los coeficientes «path», se utiliza la técnica “bootstrapping” con 5.000 submuestras como lo explica Hair en su investigación. Además, se presenta el tamaño del efecto (f^2) para las relaciones de nuestro modelo estructural siguiendo la recomendación que menciona Hair (2011) en su libro.

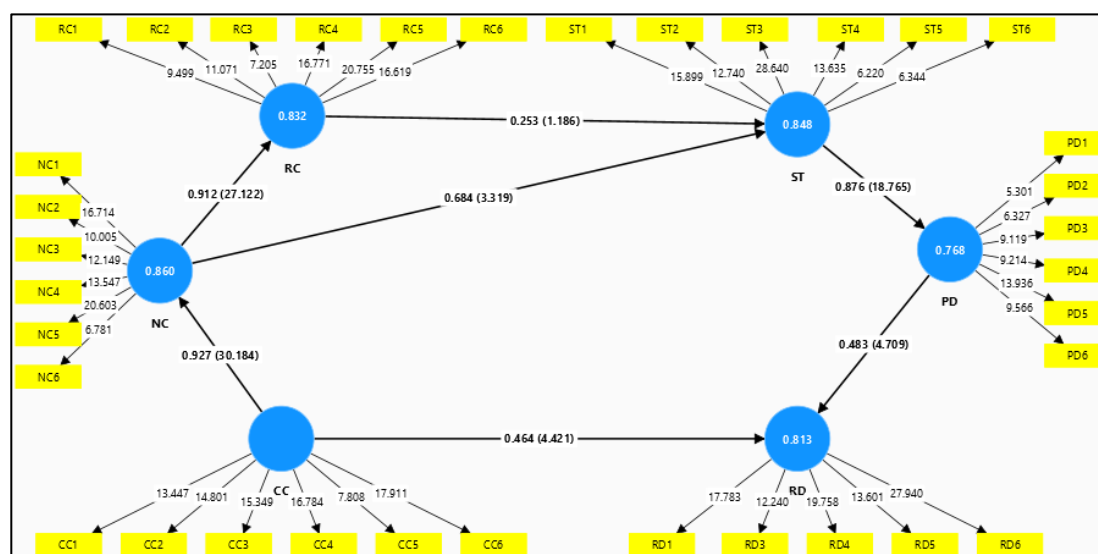
Como muestran la Tabla 11 y la Figura 10, los resultados contrastan las siguientes hipótesis de investigación:

- La hipótesis 1 indica una relación positiva para la Seguridad Técnica (ST) con la Privacidad de Datos (PD) (0.876***).
- En la hipótesis 2, se muestra también una relación positiva para la Privacidad de Datos (PD) con la Responsabilidad de los Datos (RD) (0.483***).
- Por el contrario, la hipótesis 3 (0.253) no se contrasta, evidenciando que el Riesgo de Ciberseguridad (RC) no se relaciona con la Seguridad Técnica (ST).
- En la hipótesis 4, la Normativas de Ciberseguridad (NC) se relacionan positivamente con el Riesgo de Ciberseguridad (RC) (0,912***).
- Así mismo, la hipótesis 5 muestra que las Normativas de Ciberseguridad (NC) se relacionan positivamente con la Seguridad Técnica (ST) (0,684***).
- También la hipótesis 6 evidencia que la Concientización de la Ciberseguridad (CC) se relaciona positivamente con las Normativas de Ciberseguridad (NC) (0,927***).
- Finalmente, la hipótesis 7 muestra una la relación positiva intermedia de la Concientización de la Ciberseguridad (CC) con la Responsabilidad de los Datos (RD) (0,464***).

Tabla 11*Resultados del modelo estructural*

Hipótesis	Coefficient es Path	t-value	p-value	Intervalo de Confianza	Decisión	f ²
H1: ST → PD	0.876***	18.765	0.000	[0.769;0.949]	Si	3.304
H2: PD → RD	0.483***	4.709	0.000	[0.280;0.691]	Si	0.421
H3: RC → ST	0.253ns	1.186	0.236	[-0.210;0.627]	No	0.071
H4: NC → RC	0.912	27.122	0.000	[0.307;1.121]	Si	4.957
H5: NC → ST	0.684	3.319	0.001	[0.307;1.121]	Si	0.517
H6: CC → NC	0.927	30.184	0.000	[0.848;0.967]	Si	6.133
H7: CC → RD	0.464	4.421	0.000	[0.238;0.658]	Si	0.390

Fuente: Elaboración propia.

Figura 10.*Resultado del análisis básico del Modelo**Fuente: Elaboración propia.*

Siguiendo a Cohen, en cuanto al tamaño del efecto sustantivo, H6, H4 y H1 muestran efectos significativos altos, especialmente la relación H6: Concientización de la Ciberseguridad (CC) y la Normativa de Ciberseguridad (NC) ($f^2 = 6.133$) y la relación H4: las Normativas de Seguridad (NC) y el Riesgo de Ciberseguridad (RC) ($f^2 = 4.957$). Además, H5, H7 y H2 muestran efectos significativamente medios, sin embargo, H3 no muestra relación entre ambas variables.

5.2.9. Framework final

El framework final, denominado **SCERA** (*Framework para la Gestión de la Ciberseguridad Social en Universidades Privadas*), se construye a partir de los resultados obtenidos en el modelo estructural validado estadísticamente (Figura 10) y la propuesta conceptual inicial (Figura 8). Este framework se estructura en torno a tres ejes principales: riesgo cibernético, normativas existentes y concientización del personal, los cuales, a partir del análisis estadístico y la validación mediante ecuaciones estructurales, evidenciaron una relación significativa con los componentes clave de la protección de datos: seguridad técnica, privacidad y responsabilidad. De esta manera, el modelo estructural validado estadísticamente sustenta teóricamente las relaciones entre los ejes de la investigación, mientras que el framework SCERA organiza dichos hallazgos en un marco práctico aplicable a las universidades. La

validación del modelo respalda la solidez del framework planteado y su alineación con el NIST CSF 2.0, proporcionando a las universidades privadas de educación superior una guía integral para gestionar la ciberseguridad social desde un enfoque educativo, normativo y de cultura organizacional.

5.2.10. Discusión

El objetivo del estudio fue verificar la relación positiva de 6 constructos (ver Tabla 2) mediante 7 hipótesis, lo cual se cumplió a excepción de la hipótesis (H3) donde se menciona la relación entre los Riesgos de Ciberseguridad y la Seguridad Técnica que no mostró significancia. Además, se determinó que 3 relaciones (hipótesis) propuestas eran consideradas altamente significativas (H6: CC $\rightarrow$ NC, H4: NC $\rightarrow$ RC, H1: ST $\rightarrow$ PD) y 3 relaciones eran consideradas medianamente significativas (H5: NC $\rightarrow$ ST, H7: CC $\rightarrow$ RD, H2: PD $\rightarrow$ RD).

El modelo propuesto buscó integrar factores críticos que influyen directamente en la ciberseguridad dentro de las universidades privadas desde un enfoque social. Los resultados indican que tanto los aspectos técnicos, normativos y de conciencia son jugadores principales en la creación de una gestión efectiva de la ciberseguridad social, corroborando, además, la necesidad de un enfoque interdisciplinario que vincula la cultura organizacional, la seguridad de la información y la gestión normativa.

Los resultados (positivos de H1) validan que la seguridad técnica es un activo crucial para mantener la privacidad de los datos, donde la aplicación de buenas prácticas se traduce directamente en una mayor protección, evidenciando que Nejari demuestra que el mal uso de las tecnologías producen brechas de ciberseguridad, además de alinearse con Oyewole, puesto que al aplicar una legislación global apoyada de buenas prácticas tecnológicas, las expectativas de privacidad que los usuarios exigen se darán de una manera mucho más efectiva.

Así mismo, (el soporte brindado a H2) se resalta la importancia de la privacidad de los datos para la promoción de la responsabilidad de los datos, sugiriendo que, al aplicar una adecuada protección, se refuerza la confianza en los usuarios finales como lo menciona Ogbuke, además, se mejora el cumplimiento general de las responsabilidades relacionadas al tratamiento de los datos a través de una influencia responsable y ética, impidiendo así una violación a la privacidad según Anshari,

dejando como índice principal que el ejecutar una gestión de la privacidad basada en la transparencia demuestra que se actúa con responsabilidad.

También, los hallazgos (poca influencia de H3) muestran que el riesgo de ciberseguridad no se relaciona con la seguridad técnica, evidenciando que los riesgos no son percibidos como influyentes para ejecutar mejoras técnicas, es aquí donde Shaikh menciona que la seguridad técnica puede ayudar en la mitigación de los riesgos, pero que esos riesgos también pueden ser ocasionados por el uso de tecnologías obsoletas, donde no se tenga un plan de implementación basado en la mejora continua. Así mismo, Durst resalta que frente las adversidades se deben incorporar mejoras, dando a entender que existe una posibilidad de exploración donde, además de los riesgos, se incluyan otras variables o constructos que puedan influir directamente en la gestión y la obtención de una la seguridad técnica resiliente.

Por otra parte, (una fuerte relación encontrada en H4) entre las normativas de ciberseguridad y el riesgo de ciberseguridad, se deja en evidencia que las políticas y regulaciones juegan un papel crucial en la mitigación de los riesgos cibernéticos, confirmando lo que Sharma afirma al mencionar que las regulaciones y el seguimiento de buenas prácticas ayudan a combatir amenazas cibernéticas, así se demuestra que un modelo o marco de trabajo sólido, como lo propone Abrahams, puede influir directamente en la percepción y la gestión de los riesgos.

Además, (en H5) las normativas de ciberseguridad sí se relacionan con la seguridad técnica, puesto que la adopción de marcos normativos no solo ayuda en gestionar los riesgos, sino también en la mejora de la infraestructura tecnológica. Autores como Kryshchanovych y Saeed concuerdan que, además de ganar mejoras técnicas, también se aumenta la percepción de seguridad digital en los usuarios que usan las tecnologías, demostrando que es esencial contar con una defensa efectiva y guiada por políticas que usen tecnologías recientes para proteger un ambiente cibernético.

La existencia de una fuerte relación entre la concientización de la ciberseguridad y las normativas de ciberseguridad (descritas en H6) demuestra el impacto positivo de una educación desde edades tempranas, tal como lo menciona Nwankpa, aumentando el conocimiento y la toma de conciencia. Por otra parte, también con los resultados se demuestra que la implementación de políticas y normas son resultado de una conciencia influenciada en la educación, relacionándose con lo

que sostiene Mittal respecto a que los esfuerzos de formación en ciberseguridad son esenciales para obtener leyes mucho más rigurosas.

Por último, (en H7) se evidencia cómo la relación entre la concientización de la ciberseguridad influye en la responsabilidad de los datos subrayando la importancia de que una buena formación integral, que puedan ejecutarse desde las aulas, tal como lo menciona Argyridou, pueden contribuir en la formación a largo plazo de futuros profesionales que sean responsables dentro de áreas de trabajo o en la misma sociedad. Asimismo, la influencia de la concientización de ciberseguridad sobre las normativas de ciberseguridad fue la relación que tenía un impacto más significativo en el conjunto del modelo, lo que demuestra la importancia de reforzar la conciencia de los involucrado para el correcto cumplimiento de las normas de ciberseguridad.

La concientización de la ciberseguridad se puso de manifiesto en estudios realizados, teniendo un efecto muy elevado y estadísticamente significativo tanto en las normas de ciberseguridad como en la responsabilidad de los datos (ver la Tabla 8). Por lo tanto, las universidades privadas participantes del estudio deben prestar especial atención a esta variable. Autores como Carley han señalado que este tipo de variables son los que más influyen en la ciberseguridad social. Además, la normativa de ciberseguridad es otra variable que tiene un impacto significativamente positivo sobre los riesgos de ciberseguridad y la seguridad técnica. En discusión y para poder reducir el impacto de los ataques de ciberseguridad social, las universidades privadas deberían invertir en programas que permitan el desarrollo de la concientización de su capital humano, además de establecer normativas para administrar su ciberseguridad. En este sentido, como lo menciona Wu, la concientización y las normativas son un instrumento que minimiza los riesgos de ciberataques sociales en las instituciones de educación superior privada.

CAPÍTULO 6: CONCLUSIONES

6.1. Conclusiones

6.1.1. Conclusión general

6.1.1.1. Objetivo general: Diseñar un marco de trabajo para asegurar la gestión de la ciberseguridad social en las instituciones privadas de educación superior que sufren pérdidas de datos.

Se ha diseñado un framework conceptual validado mediante un modelo conceptual (ver figura 8) para lograr el aseguramiento de una gestión de la ciberseguridad social. Este framework incluye 6 factores clave bajo 7 relaciones entre los constructos, lo que proporciona una estructura íntegra para facilitar la gestión de la ciberseguridad bajo amenazas sociales.

6.1.1.2. Hipótesis general: El marco de trabajo propuesto permitirá asegurar la gestión de la ciberseguridad social en las instituciones privadas de educación superior que sufren pérdidas de datos.

La validación estadística del modelo estructural confirmó que los ejes de riesgo cibernético, normativas existentes y concientización del personal tienen una relación significativa con los componentes de la protección de datos (seguridad técnica, privacidad y responsabilidad). Estos hallazgos sustentan la solidez del framework SCERA como marco de referencia integral. Asimismo, el alineamiento con el NIST CSF 2.0 refuerza la aplicabilidad práctica del framework, garantizando una guía confiable para las universidades en la gestión de la ciberseguridad social.

En consecuencia, la hipótesis general queda validada, al demostrar que el framework SCERA contribuye efectivamente a asegurar la gestión de la ciberseguridad social desde un enfoque organizacional, normativo y tecnológico.

6.1.2. Conclusiones específicas

6.1.2.1. Objetivo específico 1: Identificar los factores de la ciberseguridad social que influyen en la pérdida de datos en las instituciones privadas de educación superior.

Como se propuso en el capítulo 3, se ejecutó una revisión sistemática de la literatura considerando una metodología de 3 fases: a) Planificación, b) Desarrollo, y c) Análisis, donde se obtuvo como resultado un total de 15 factores relevantes que influyen en la ciberseguridad social utilizando como técnica la ingeniería social, como se pueden apreciar en la Figura 4. Del conjunto, se seleccionaron 6 constructos aplicables a la ciberseguridad social en base a su criterio de ocurrencia en la literatura.

6.1.2.2. Hipótesis específica 1: La identificación de los factores de la ciberseguridad social permitirá establecer las principales dimensiones que inciden en pérdidas de datos en las instituciones privadas de educación superior.

Se confirma la hipótesis en dos sustentos. Primero, en la Revisión Sistemática de la Literatura (RSL) se identificaron 63 autores quienes resaltaron 15 factores de riesgos relacionados con la ciberseguridad social utilizando como técnica la ingeniería social, los cuales se representan en la Figura 4, mostrando que constituyen amenazas críticas para la pérdida de datos. Segundo, el modelo validado estadísticamente demostró que el constructo riesgo cibernético, que integra estos factores, presenta cargas significativas y relaciones directas con la gestión de la seguridad técnica y privacidad de los datos.

6.1.2.3. Objetivo específico 2: Describir un conjunto de criterios que aseguren la gestión de la ciberseguridad social en las instituciones privadas de educación superior.

De la misma manera, en el capítulo 3, se hallaron criterios considerados como principales para asegurar una gestión de la ciberseguridad, resultando en marcos adoptados, modelos desarrollados y tecnologías aplicadas. Durante la revisión se destacaron 24 framework (ver Figura 5), 9 modelos (ver Figura 6), y más de 15 tecnologías (ver Figura 7) capaces de contribuir con la gestión de la ciberseguridad social. Sin embargo, bajo una comparación en el uso y aplicación de estos, se considera

que el más significativo es el NIST Cybersecurity Framework 2.0, por su orientación hacia la gestión de la ciberseguridad con el fin de proteger los activos tecnológicos y enfrentar las amenazas cibernéticas sea de índole digital o social.

6.1.2.4. Hipótesis específica 2: La descripción de los criterios servirá como base para la estructuración del marco de trabajo para la gestión de la ciberseguridad social en las instituciones privadas de educación superior.

La hipótesis se valida se la siguiente manera. Primero, en la Revisión Sistemática de la Literatura (RSL) se identificaron los principales framework aplicados en ciberseguridad social, presentados en la Figura 5, donde el NIST CSF destaca como el modelo más utilizado para definir criterios y guías de acción en la gestión de la seguridad. Esto evidencia que los criterios establecidos en marcos de referencia reconocidos constituyen índices clave para la formulación de estrategias. Segundo, los resultados del modelo validado estadísticamente mostraron que el constructo normativas existentes presenta un impacto significativo sobre la seguridad técnica y la privacidad de los datos, confirmando que la existencia y aplicación de criterios normativos fortalecen la gestión de la ciberseguridad social.

6.1.2.5. Objetivo específico 3: Diseñar un marco de trabajo para la gestión de la ciberseguridad social en las instituciones privadas de educación superior.

Mediante un favorable análisis estadístico, se validaron los 6 factores clave del modelo propuesto a través de sus relaciones internas, utilizando el modelado de ecuaciones estructurales y la técnica de mínimos cuadrados parciales. En primer lugar, se determinó la fiabilidad compuesta, con cargas factoriales superiores a 0,7 para la mayoría de los ítems y ninguna inferior a 0,4, lo que respalda la consistencia interna de los factores. En segundo lugar, se verificó la validez convergente, que presentó valores superiores a 0,5 en todos los casos, lo que indica que los constructos explican más del 50% de la varianza de sus indicadores. Finalmente, la validez discriminante ha sido verificada utilizando tanto el criterio de Fornell y Larcker como el ratio HTMT, observándose en general cumplimiento adecuado; sin embargo, se identificó que el par de constructos Concientización de Ciberseguridad y Normativas de Ciberseguridad no satisfizo plenamente este criterio, lo que sugiere un solapamiento conceptual entre ambos factores. Esta limitación, atribuible a la cercanía semántica de los ítems y al tamaño muestral, no invalida el modelo, pero sí representa un aspecto a considerar en

futuras investigaciones. Con ello se deja en evidencia que el framework cumple con los requisitos técnicos necesarios para ser considerado robusto, asegurando su utilidad para futuras investigaciones y aplicaciones prácticas.

6.1.2.6. Hipótesis específica 3: El marco de trabajo diseñado permite la gestión de la ciberseguridad social en las instituciones privadas de educación superior.

La hipótesis se respalda en la identificación de tecnologías emergentes aplicadas a la ciberseguridad descritas en la Figura 7, tales como Machine Learning, Inteligencia Artificial, Blockchain, Cloud Computing y técnicas avanzadas de encriptación. Estas tecnologías fortalecen la capacidad de las instituciones para detectar, responder y recuperarse ante incidentes de seguridad, aportando mecanismos de resiliencia frente a amenazas sociales y técnicas. El análisis de la literatura y los resultados del modelo validado evidencian que la incorporación de dichas tecnologías a un marco de trabajo no solo mejora la capacidad de prevención, sino que también asegura la continuidad y la integridad de la información en entornos universitarios.

6.2. Limitaciones

Durante el presente estudio se consideraron las siguientes limitaciones:

- **Alcance de la encuesta:** El instrumento propuesto se aplicó únicamente universidades privadas de Lima Metropolitana, pudiéndose extender hacia otras universidades del Perú o hacia otros sectores económicos o el gobierno.
- **Tamaño de la muestra:** Se enfocó únicamente en los responsables de la toma de decisiones de las áreas de tecnología de las universidades privadas, pudiéndose extender hacia otras especialidades dentro del área de tecnología que pudieran contribuir en un enriquecimiento de la data recolectada.
- **Enfoque del marco de referencia:** La principal base del framework muestra como punto de partida la adecuación del framework NIST v2.0, pudiéndose tomar como otras referencias otros framework que durante la revisión sistemática de literatura quedaron en evidencia.

6.3. Trabajos futuros

Con la finalidad de ampliar el marco de trabajo propuesto, se recomiendan las siguientes áreas de investigación:

- **Identificación de nuevos constructos:** Explorar nuevos conceptos relacionados a la ciberseguridad social, tales como la resiliencia digital comunitaria o la confianza digital en ecosistemas sociales.
- **Ampliación de la recolección de datos:** Desarrollar un instrumento aplicable en distintos sectores empresariales o en los distintos gobiernos con la finalidad de democratizar una buena práctica en la gestión de la ciberseguridad social.
- **Extensión del alcance:** Desarrollar un instrumento aplicable en distintos sectores empresariales o en los distintos gobiernos con la finalidad de democratizar una buena práctica en la gestión de la ciberseguridad social.
- **Desarrollo de nuevos modelos:** Explorar y definir los constructos reconocidos y utilizarlos dentro de otros framework de ciberseguridad con la finalidad de mostrar las validaciones a los distintos modelos que se pueden proponer.
- **Creación de una herramienta tecnológica:** Desarrollar una herramienta que permita automatizar la identificación ataques de ingeniería social mucho más sofisticado.

REFERENCIAS BIBLIOGRÁFICAS

- Aarón, M. A., Solano, A. D., Choles, P. E., Cuesta, R. (2018). Caracterización Socioeconómica de la Comunidad Indígena Wayuu de Manzana en Colombia: Un aporte desde la Ingeniería Social. *Información tecnológica*, 29(6), 3-12. <https://doi.org/10.4067/S0718-07642018000600003>
- Abdullayeva, F. (2023). Cyber resilience and cyber security issues of intelligent cloud computing systems. *Results in Control and Optimization*, 12, 100268. <https://doi.org/10.1016/j.rico.2023.100268>
- Abrahams, T. O., Ewuga, S. K., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Mastering compliance: A comprehensive review of regulatory frameworks in accounting and cybersecurity. *Computer Science & IT Research Journal*, 5(1). <https://doi.org/10.51594/csitrj.v5i1.709>
- Alallaq, N., Al-Khiza'ay, M., & Han, X. (2019). Group topic-author model for efficient discovery of latent social astroturfing groups in the tourism domain. *Cybersecurity*, 2(1), 1–11. <https://doi.org/10.1186/s42400-019-0029-8>
- AlDaajeh, S., Saleous, H., Alrabae, S., Barka, E., Breiting, F., & Choo, K.-K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, 119, 102754. <https://doi.org/10.1016/j.cose.2022.102754>
- Alieva, I., Moffitt, J., & Carley, K. M. (2022). How disinformation operations against Russian opposition leader Alexei Navalny influence the international audience on Twitter. *Social Network Analysis and Mining*, 12(1), 80. <https://doi.org/10.1007/s13278-022-00370-2>
- Alsmadi, I. (2019). *The NICE Cyber Security Framework: Cyber Security Intelligence and Analytics* (1st Edition). Springer International Publishing. <https://doi.org/10.1007/978-3-030-02360-7>
- AlSobeh, A. M. R., AlAzzam, I., Shatnawi, A. M. J., & Khasawneh, I. (2023). Cybersecurity awareness factors among adolescents in Jordan: Mediation effect of cyber scale and personal factors. *Online Journal of Communication and Media Technology*, 13(2), e202312. <https://doi.org/10.30935/ojcm/12942>
- Althobaiti, A., Jindal, A., Marnerides, A. K., & Roedig, U. (2021). Energy theft in smart grids: A survey on data-driven attack strategies and detection methods. *IEEE Access*, 9, 159,291–159,312. <https://doi.org/10.1109/ACCESS.2021.3051498>
- Amerini, I., Li, C. T., & Caldelli, R. (2019). Social network identification through image classification with CNN. *IEEE Access*, 7, 35264–35273. <https://doi.org/10.1109/ACCESS.2019.2905598>

- Amón-Salinas, J. P., & Zhindón-Mora, M. G. (2020). Modelo de Gobierno y Gestión de TI, basado en COBIT 2019 e ITIL 4, para la Universidad Católica de Cuenca. *Revista Científica FIPCAEC (Fomento de la investigación y publicación en Ciencias Administrativas, Económicas y Contables)*. ISSN : 2588-090X. *Polo de Capacitación, Investigación y Publicación (POCAIP)*, 5(16), 218-239. <https://doi.org/10.23857/fipcaec.v5i14.168>
- Anshari, M., Syafrudin, M., Fitriyani, N. L., & Razzaq, A. (2022). Ethical responsibility and sustainability (ERS) development in a metaverse business model. *Sustainability*, 14(23). <https://doi.org/10.3390/su142315805>
- Anyanwu, A., Olorunsogo, T., Abrahams, T. O., Akindote, O. J., & Reis, O. (2024). Data confidentiality and integrity: A review of accounting and cybersecurity controls in superannuation organizations. *Computer Science & IT Research Journal*, 5(1). <https://doi.org/10.51594/csitrj.v5i1.735>
- Argyridou, E., et al. (2023). Cyber hygiene methodology for raising cybersecurity and data privacy awareness in healthcare organizations: Concept study. *Journal of Medical Internet Research*, 25(1), e41294. <https://doi.org/10.2196/41294>
- Astakhova, L., & Medvedev, I. (2020). Scanning the resilience of an organization's employees to social engineering attacks using machine learning technologies. In *2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBREIT)* (pp. 606–610). IEEE. <https://doi.org/10.1109/USBREIT48449.2020.9117644>
- Awasthi, A., & Goel, N. (2022). Phishing website prediction using base and ensemble classifier techniques with cross-validation. *Cybersecurity*, 5(1), 1–23. <https://doi.org/10.1186/s42400-022-00123-1>
- Banathy, B. H. (1996). *Designing Social Systems in a Changing World* (1ra ed.). Springer New York, NY. <https://link.springer.com/book/10.1007/978-1-4757-9981-1>
- Batista Tellez, R. (2021). Enfoque transcultural de la ciberseguridad. Desafíos para el balance regional en América Latina. *UCIENCIA 2021*. <https://repositorio.uci.cu/jspui/handle/123456789/9695>
- Battaglioni, M., Rafaiani, G., Chiaraluce, F., & Baldi, M. (2022). MAGIC: A method for assessing cyber incidents occurrence. *IEEE Access*, 10, 73458–73473. <https://doi.org/10.1109/ACCESS.2022.3207832>
- Bayramova, A., Edwards, D. J., & Roberts, C. (2021). The role of blockchain technology in augmenting supply chain resilience to cybercrime. *Buildings*, 11(7), 283. <https://doi.org/10.3390/buildings11070283>
- Beltrán, A. (2024). Análisis de la educación en ciberseguridad: Situación actual, estrategias y retos (Ph.D. thesis). Universidad de Granada. Accessed: October 13, 2024.

- Bertalanffy, L. von. (2009). *General system theory: Foundations, development, applications* (Rev. ed., 17. paperback print). Braziller.
- Beskow, D. M., & Carley, K. M. (2019). Social cybersecurity: An emerging national security requirement. *Military Review*, 99(2), 117–126.
<https://www.armytimes.com>
- Beskow, D. M., & Carley, K. M. (2019). *Social Cybersecurity: An Emerging National Security Requirement*. Carnegie Mellon University Pittsburgh United States. <https://apps.dtic.mil/sti/citations/AD1108494>
- Bhamra, R. (2015). *Organisational Resilience: Concepts, Integration, and Practice*. CRC Press.
- Blane, J. T., Bellutta, D., & Carley, K. M. (2022). Social-cyber maneuvers during the COVID-19 vaccine initial rollout: Content analysis of tweets. *Journal of Medical Internet Research*, 24(3), e34040. <https://doi.org/10.2196/34040>
- Bondoc, C. E., & Malawit, T. G. (2020). Cybersecurity for higher education institutions: Adopting regulatory framework. *Global Journal of Engineering and Technology Advances*, 2(3), 016-021.
<https://doi.org/10.30574/gjeta.2020.2.3.0013>
- Buchanan, B. (2017). *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. (1ra ed.). Oxford University Press.
<https://doi.org/10.1093/acprof:oso/9780190665012.001.0001>
- Caiza, G., Llamuca, E. S., Garcia, C. A., Gallardo-Cardenas, F., Lanas, D., & Garcia, M. V. (2019). Industrial shop-floor integration based on AMQP protocol in an IoT environment.
- Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: The false promise of digital sovereignty. *European Security*, 31(3), 415–434.
<https://doi.org/10.1080/09662839.2022.2101885>
- Carías, J. F., Borges, M. R., Labaka, L., Arrizabalaga, S., & Hernantes, S. (2020). Systematic approach to cyber resilience operationalization in SMEs. *IEEE Access*, 8, 174,200–174,221. <https://doi.org/10.1109/ACCESS.2020.2972772>
- Carley, K. M. (2020). Social cybersecurity: An emerging science. *Computational and Mathematical Organization Theory*, 26(4), 365-381.
<https://doi.org/10.1007/s10588-020-09322-9>
- Carley, K. M., Cervone, G., Agarwal, N., & Liu, H. (2018). Social cyber-security. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 10899 LNCS, 389-394. Scopus. https://doi.org/10.1007/978-3-319-93372-6_42

- Carriegos, M. V., Castañeda, A. L. M., Trobajo, M., & De Zaballa, D. A. (2021). On aggregation and prediction of cybersecurity incident reports. *IEEE Access*, 9, 102636–102648. <https://doi.org/10.1109/ACCESS.2021.3107122>
- Carrillo-Mondéjar, J., Turtiainen, H., Costin, A., Martínez, J. L., & Suarez-Tangil, G. (2022). Hale-IoT: Hardening legacy Internet-of-Things devices by retrofitting defensive firmware modifications and implants. *IEEE Internet of Things Journal*. <https://doi.org/10.1109/JIOT.2022.3140748>
- Castano, F., Fernández, E. F., Alaiz-Rodríguez, R., & Alegre, E. (2023). Phikita: Phishing kit attacks dataset for phishing websites identification. *IEEE Access*. <https://doi.org/10.1109/ACCESS.2023.3207845>
- Centro Nacional de Planeamiento Estratégico. (2024). *Perú 2050: Actualización de las tendencias globales y regionales*. Accessed: October 20, 2024. <https://www.gob.pe/es/i/4985431>
- Cestero, J., Cuenca, L., & Ortiz, Á. (2018). Propuesta de un marco de referencia holístico de modelado de empresas. *Dirección y Organización*, 66, Art. 66. <https://doi.org/10.37610/dyo.v0i66.536>
- Chen, K.-C., Lin, S.-C., Hsiao, J.-H., Liu, C.-H., Molisch, A. F., & Fettweis, G. P. (2020). Wireless networked multirobot systems in smart factories. *Proceedings of the IEEE*, 109(4), 468–494. <https://doi.org/10.1109/JPROC.2020.2968761>
- Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of Social Engineering Attacks on Social Networks. *Procedia Computer Science*, 198, 656–661. <https://doi.org/10.1016/j.procs.2021.12.302>
- Chockalingam, S., Pieters, W., Teixeira, A., & Van Gelder, P. (2021). Bayesian network model to distinguish between intentional attacks and accidental technical failures: A case study of floodgates. *Cybersecurity*, 4(1), 1–19. <https://doi.org/10.1186/s42400-021-00086-6>
- Christopher, V., et al. (2021). Minority resampling boosted unsupervised learning with hyperdimensional computing for threat detection at the edge of the Internet of Things. *IEEE Access*, 9, 126646–126657. <https://doi.org/10.1109/ACCESS.2021.3080719>
- Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences* (2nd ed.). Routledge. <https://doi.org/10.4324/9780203771587>
- Corradini, I. (2020). *Building a cybersecurity culture in organizations: How to bridge the gap between people and digital technology*. Springer Nature, 284. <https://doi.org/10.1007/978-3-030-27829-3>
- Cruickshank, I. J., & Carley, K. M. (2020). Analysis of malware communities using multimodal features. *IEEE Access*, 8, 77435–77448. <https://doi.org/10.1109/ACCESS.2020.2992675>

- D'hooge, L., Wauters, T., Volckaert, B., & De Turck, F. (2019). Classification hardness for supervised learners on 20 years of intrusion detection data. *IEEE Access*, 7, 167,455–167,469. <https://doi.org/10.1109/ACCESS.2019.2934080>
- Das, S. (2016). Social cybersecurity: Understanding and leveraging social influence to increase security sensitivity. *It - Information Technology*, 58(5), 237-245. <https://doi.org/10.1515/itit-2016-0008>
- de Boer, M. H., Bakker, B. J., Boertjes, E., Wilmer, M., Raaijmakers, S., & van der Kleij, R. (2019). Text mining in cybersecurity: Exploring threats and opportunities. *Multimodal Technologies and Interaction*, 3(3), 62. <https://doi.org/10.3390/mti3030062>
- Doig Díaz, D. F., Mendoza Blanco, J. C., Mendoza Pasco, J. L., & Yañez Herrera, D. A. (2019). *Escenarios de aprendizaje competitivo a través de uso de elementos lúdicos para entrenamiento en ciberseguridad*. <https://repositorio.esan.edu.pe///handle/20.500.12640/1686>
- Domínguez, S. J. A., & Garrido, J. A. M. (2009). *La gestión de los sistemas de información en la empresa: Teoría y casos prácticos* (3ra ed.). Ediciones Pirámide.
- Dominguez-Lara, S., et al. (2018). Big five inventory en universitarios peruanos: Resultados preliminares de su validación. *Psykhé (Santiago)*, 27(2), 1–12. <https://doi.org/10.7764/psykhe.27.2.1052>
- Drury, B., Drury, S. M., Rahman, M. A., & Ullah, I. (2022). A social network of crime: A review of the use of social networks for crime and the detection of crime. *Online Social Networks and Media*, 30, 100211. <https://doi.org/10.1016/j.osnem.2022.100211>
- Duggineni, S. (2023). Impact of controls on data integrity and information systems. *Science and Technology*, 3(2), 29–35.
- Durand, H. (2018). A nonlinear systems framework for cyberattack prevention for chemical process control systems. *Mathematics*, 6(9), 169. <https://doi.org/10.3390/math6090169>
- Durst, S., Hinteregger, C., & Zieba, M. (2024). The effect of environmental turbulence on cybersecurity risk management and organizational resilience. *Computers & Security*, 137, 103591. <https://doi.org/10.1016/j.cose.2023.103591>
- Elmarady, A. A., & Rahouma, K. (2021). Studying cybersecurity in civil aviation, including developing and applying aviation cybersecurity risk assessment. *IEEE Access*, 9, 143,997–144,016. <https://doi.org/10.1109/ACCESS.2021.3051410>
- Erendor, M. E., & Yildirim, M. (2022). Cybersecurity awareness in online education: A case study analysis. *IEEE Access*, 10, 52319–52335. <https://doi.org/10.1109/ACCESS.2022.3171829>

- Escobar-Naranjo, J., Caiza, G., Ayala, P., Jordan, E., Garcia, C. A., & Garcia, M. V. (2023). Autonomous navigation of robots: Optimization with DQN. *Applied Sciences (Switzerland)*, 13(12), 7202. <https://doi.org/10.3390/app13127202>
- Eshetu, A. Y., Mohammed, E. A., & Salau, A. O. (2024). Cybersecurity vulnerabilities and solutions in Ethiopian university websites. *Journal of Big Data*, 11(1), 118. <https://doi.org/10.1186/s40537-024-00980-z>
- Forero, G., & Guillermo, L. F. (2020). *Ciberseguridad en las organizaciones, el personal potencial fuente de riesgo*. <http://repository.unipiloto.edu.co/handle/20.500.12277/9545>
- Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of Marketing Research*, 18(3), 382–388. <https://doi.org/10.2307/3150980>
- Freeman, L. C. (1978). Centrality in social networks conceptual clarification. *Social Networks*, 1(3), 215–239. [https://doi.org/10.1016/0378-8733\(78\)90021-7](https://doi.org/10.1016/0378-8733(78)90021-7)
- Furutani, S., Shibahara, T., Akiyama, M., & Aida, M. (2023). Interpreting graph-based Sybil detection methods as low-pass filtering. *IEEE Transactions on Information Forensics and Security*, 18, 1225–1236. <https://doi.org/10.1109/TIFS.2023.3208131>
- Gao, C., Zhang, X., & Liu, H. (2021). Data and knowledge-driven named entity recognition for cybersecurity. *Cybersecurity*, 4(1), 1–13. <https://doi.org/10.1186/s42400-021-00072-y>
- Gao, T., Yang, J., Peng, W., Jiang, L., Sun, Y., & Li, F. (2020). A content-based method for Sybil detection in online social networks via deep learning. *IEEE Access*, 8, 38753–38766. <https://doi.org/10.1109/ACCESS.2020.3033723>
- Garcia, C. A., et al. (2017). CPPS on low-cost devices for batch process under IEC-61499 and ISA-88 (pp. 855–860).
- Gavidia, J.-L., & Mariño, C.-J. (2023). Statistical model for production planning in a vehicle assembler applying lean manufacturing. *Lecture Notes in Networks and Systems*, 678, 494–507. https://doi.org/10.1007/978-3-030-91356-3_45
- George, D. A. S. (2024). Emerging trends in AI-driven cybersecurity: An in-depth analysis. *PUIRP*, 2(4). <https://doi.org/10.5281/zenodo.13333202>
- Gil Arango, J. E. (2020). *Marco de referencia para el diseño de estrategias competitivas, basadas en la creación de conocimiento para la innovación* [Master Thesis, Universidad Eafit]. <http://repository.eafit.edu.co/handle/10784/17405>
- González, D. L., & Pulido, S. S. (2021). *La ciberseguridad política clave dentro de las organizaciones*. <https://repository.usta.edu.co/handle/11634/37635>

- Gualpa, T., Ayala, P., Cáceres, J., Llango, E., & Garcia, M. (2022). Smart IoT watering platform based on orchestration: A case study. In M. V. Garcia, F. Fernández-Peña, & C. Gordón-Gallegos (Eds.), *Advances and Applications in Computer Science, Electronics, and Industrial Engineering* (pp. 191–204). Springer. https://doi.org/10.1007/978-3-030-97719-1_11
- Gualpa, T., Caiza, G., Ayala, P., Garcia, C. A., & Garcia, M. V. (2023). Smart i4.0-based irrigation system for optimization in water management: A case study. *IEEE Transactions on Emerging Topics in Computing*, 2023, 1–9. <https://doi.org/10.1109/ETFA54631.2023.10275443>
- Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, 19(2), 139–152. <https://doi.org/10.2753/MTP1069-6679190202>
- Hair, J., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2021). *A Primer on Partial Least Squares Structural Equation Modeling* (3rd ed.). Los Angeles.
- Hartel, P., Homoliak, I., & Reijdsbergen, D. (2019). An empirical study into the success of listed smart contracts in Ethereum. *IEEE Access*, 7, 177539–177555. <https://doi.org/10.1109/ACCESS.2019.2951706>
- Hasani, T., Rezania, D., Levallet, N., O'Reilly, N., & Mohammadi, M. (2023). Privacy enhancing technology adoption and its impact on SMEs' performance. *International Journal of Engineering Business Management*, 15. <https://doi.org/10.1177/18479790231172874>
- Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, 73, 102–113. <https://doi.org/10.1016/j.cose.2017.10.008>
- He, Z. (2022). When data protection norms meet digital health technology: China's regulatory approaches to health data protection. *Computer Law & Security Review*, 47, 105758. <https://doi.org/10.1016/j.clsr.2022.105758>
- Heeks, R., & Ospina, A. V. (2019). Conceptualising the link between information systems and resilience: A developing country field study. *Information Systems Journal*, 29(1), 70–96. <https://doi.org/10.1111/isj.12144>
- Henseler, J. (2015). Is the whole more than the sum of its parts? On the interplay of marketing and design research. University of Twente, Netherlands.
- Henseler, J. (2017). Bridging design and behavioral research with variance-based structural equation modeling. *Journal of Advertising*, 46(1), 178–192. <https://doi.org/10.1080/00913367.2017.1281780>
- Hernández, R., Fernández, C. y Baptista, P. (2014). *Metodología de la investigación*. México: Mc Graw Hill

- Hevner, A., & Chatterjee, S. (2010). *Design Research in Information Systems* (1st ed., Vol. 22). Springer New York, NY.
<https://link.springer.com/book/10.1007/978-1-4419-5653-8>
- Higgins, M., Teng, F., & Parisini, T. (2020). Stealthy MTD against unsupervised learning-based blind FDI attacks in power systems. *IEEE Transactions on Information Forensics and Security*, 16, 1275–1287.
<https://doi.org/10.1109/TIFS.2020.2979749>
- Hijji, M., & Alam, G. (2022). Cybersecurity awareness and training (CAT) framework for remote working employees. *Sensors*, 22(22).
<https://doi.org/10.3390/s22228663>
- Hong, L., & Hales, D. N. (2023). How blockchain manages supply chain risks: Evidence from Indian manufacturing companies. *The International Journal of Logistics Management*, 35(5), 1604–1627. <https://doi.org/10.1108/IJLM-05-2023-0178>
- Hong, W. C. H., Chi, C., Liu, J., Zhang, Y., Lei, V. N.-L., & Xu, X. (2023). The influence of social education level on cybersecurity awareness and behaviour: A comparative study of university students and working graduates. *Education and Information Technologies*, 28(1), 439–470. <https://doi.org/10.1007/s10639-022-11121-5>
- Hossain, N. U. I., Fazio, S. A., Lawrence, J.-M., Gonzalez, E. D. S., Jaradat, R., & Alvarado, M. S. (2022). Role of systems engineering attributes in enhancing supply chain resilience: Healthcare in the context of the COVID-19 pandemic. *Heliyon*, 8(6), e09815. <https://doi.org/10.1016/j.heliyon.2022.e09815>
- HR, M. G., MV, A., S, G. P., & S, V. (2020). Development of anti-phishing browser based on random forest and rule of extraction framework. *Cybersecurity*, 3(1), 1–14. <https://doi.org/10.1186/s42400-020-00059-1>
- Huang, Y., Huang, L., & Zhu, Q. (2022). Reinforcement learning for feedback-enabled cyber resilience. *Annual Review of Control*, 53, 273–295.
<https://doi.org/10.1016/j.arcontrol.2022.01.004>
- Huapaya, D., Marin, D., & Mauricio, D. (2021). TCO app: Telemonitoring and control of pediatric overweight and obesity. *Advances in Intelligent Systems and Computing*, 1307, 79–97. https://doi.org/10.1007/978-981-33-4565-2_6
- International Telecommunication Union (ITU). (2024). *Global cybersecurity index*. Accessed: October 13, 2024. <https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx>
- Iwaya, L. H., Babar, M. A., & Rashid, A. (2023). Privacy engineering in the wild: Understanding the practitioner's mindset, organizational aspects, and current practices. *IEEE Transactions on Software Engineering*, 49(9), 4324–4348.
<https://doi.org/10.1109/TSE.2023.3290237>

- Jaramillo Londoño, C. (1996). La ingeniería social: Un desafío investigativo. *Revista Universidad EAFIT*, 104, Art. 104.
- Joyce, C., Roman, F. L., Miller, B., Jeffries, J., & Miller, R. C. (2021). Emerging cybersecurity threats in radiation oncology. *Advances in Radiation Oncology*, 6(6), 100796. <https://doi.org/10.1016/j.adro.2021.100796>
- Katz, R., Jung, J., & Callorda, F. (2020). *El estado de la digitalización de América Latina frente a la pandemia del COVID-19*. CAF. <http://scioteca.caf.com/handle/123456789/1540>
- Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. *Information*, 12(10). <https://doi.org/10.3390/info12100417>
- Khairova, N., Mamyrbayev, O., Rizun, N., Razno, M., & Ybytayeva, G. (2023). A parallel corpus-based approach to the crime event extraction for low-resource languages. *IEEE Access*. <https://doi.org/10.1109/ACCESS.2023.3152365>
- Khidzir, N. Z., Ismail, A. R., Daud, K. A. M., Ghani, M. S. A. A., & Ibrahim, M. A. H. I. (2016). Critical Cybersecurity Risk Factors in Digital Social Media: Analysis of Information Security Requirements. *Lecture Notes on Information Theory*, 4(1), 18-24. <https://doi.org/10.18178/lnit.4.1.18-24>
- Kianpour, M., & Raza, S. (2024). Unmasking the hidden risk of cybersecurity regulations: More than malware. *International Cybersecurity Law Review*, 5(1), 169–212. <https://doi.org/10.1365/s43439-024-00111-7>
- Kim, Y., Kim, H. K., Kim, H., & Hong, J. B. (2020). Do many models make light work? Evaluating ensemble solutions for improved rumor detection. *IEEE Access*, 8, 150709–150724. <https://doi.org/10.1109/ACCESS.2020.3017839>
- Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering*. Technical report, EBSE Technical Report EBSE-2007-01.
- Knight, R., & Nurse, J. R. (2020). A framework for effective corporate communication after cybersecurity incidents. *Computers & Security*, 99, 102036. <https://doi.org/10.1016/j.cose.2020.102036>
- Kryshtanovych, M., Panfilova, T., Khomenko, A., Dziubenko, O., & Lukashuk, L. (2023). Optimization of state regulation in the field of safety and security of business: A local approach. *Business: Theory and Practice*, 24(2). <https://doi.org/10.3846/btp.2023.19563>
- Kumar, N. M., et al. (2020). Distributed energy resources and the application of AI, IoT, and blockchain in smart grids. *Energies*, 13(21), 5739. <https://doi.org/10.3390/en13215739>
- Laghari, S. U. A., Manickam, S., Al-Ani, A. K., Rehman, S. U., & Karuppayah, S. (2021). SECS/GEMSEC: A mechanism for detection and prevention of cyber-

- attacks on SECS/GEM communications in Industry 4.0 landscape. *IEEE Access*, 9, 154,380–154,394. <https://doi.org/10.1109/ACCESS.2021.3055270>
- Liu, B., Xie, S., Yang, Y., Wang, R., & Hong, Y. (2021). Privacy-preserving divisible double auction with a hybridized tee-blockchain system. *Cybersecurity*, 4(1), 1–14. <https://doi.org/10.1186/s42400-020-00066-2>
- Liu, P. (2020). Public-key encryption secure against related randomness attacks for improved end-to-end security of cloud/edge computing. *IEEE Access*, 8, 16750–16759. <https://doi.org/10.1109/ACCESS.2020.3001236>
- Liu, X., Deng, R. H., Wu, P., & Yang, Y. (2020). Lightning-fast and privacy-preserving outsourced computation in the cloud. *Cybersecurity*, 3(1), 1–21. <https://doi.org/10.1186/s42400-020-00057-3>
- Ma, C., Kong, X., Lan, Q., & Zhou, Z. (2019). The privacy protection mechanism of Hyperledger Fabric and its application in supply chain finance. *Cybersecurity*, 2(1), 1–9. <https://doi.org/10.1186/s42400-019-0012-3>
- Ma, Y. W., et al. (2022). Analysis and response strategy of cross-community rumors using mixed multilayer method for enterprise cyber warriors. *IEEE Access*, 10, 131386–131393. <https://doi.org/10.1109/ACCESS.2022.3142897>
- Madrigal, C. A., García, M. G., Zumbado, I. M., Murillo, T. M., González, M. R., & Ruiz, V. S. (2023). Un análisis del sistema educativo costarricense: Desafío crítico para la ciberseguridad del país. *Rhombus*, 3(2). Accessed: October
- Malavasi, M., Peters, G. W., Shevchenko, P. V., Trück, S., Jang, J., & Sofronov, G. (2022). Cyber risk frequency, severity and insurance viability. *Insurance: Mathematics and Economics*, 106, 90–114. <https://doi.org/10.1016/j.insmatheco.2022.05.003>
- Marinho, R., & Holanda, R. (2023). Automated emerging cyber threat identification and profiling based on natural language processing. *IEEE Access*. <https://doi.org/10.1109/ACCESS.2023.3121463>
- Martínez Díaz, C. A. (2020). *El nivel de desarrollo de la gestión de riesgo cibernético en las instituciones prestadoras de servicios de salud (IPS): Un análisis bajo el contexto de gobierno corporativo*. [Colegio de Estudios Superiores de Administración – CESA]. <https://repository.cesa.edu.co/handle/10726/2529>
- Mashatan, A., Sangari, M. S., & Dehghani, M. (2022). How perceptions of information privacy and security impact consumer trust in crypto-payment: An empirical study. *IEEE Access*, 10, 69441–69454. <https://doi.org/10.1109/ACCESS.2022.3148365>
- McAlaney, J., & Benson, V. (2020). Chapter 1: Cybersecurity as a social phenomenon. In V. Benson & J. McAlaney (Eds.), *Cyber Influence and*

- Cognitive Threats* (pp. 1–8). Academic Press. <https://doi.org/10.1016/B978-0-12-819204-7.00001-4>
- McIntosh, T., Watters, P., Kayes, A., Ng, A., & Chen, Y.-P. P. (2021). Enforcing situation-aware access control to build malware-resilient file systems. *Future Generation Computer Systems*, 115, 568–582. <https://doi.org/10.1016/j.future.2020.08.025>
- Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet of Things Journal*, 6(5), 8182–8201. <https://doi.org/10.1109/JIOT.2019.2900241>
- Mercado-Velázquez, A. A., Escamilla-Ambrosio, P. J., & Ortiz-Rodriguez, F. (2021). A moving target defense strategy for internet of things cybersecurity. *IEEE Access*, 9, 118,406–118,418. <https://doi.org/10.1109/ACCESS.2021.3053472>
- Ming, X., & Guo, J. (2018). Research on influence of cloud environment on traditional network security. *IOP Conference Series: Earth and Environmental Science*, 113(1), 012080. <https://doi.org/10.1088/1755-1315/113/1/012080>
- Minoli, D. (2008). *Enterprise Architecture A to Z: Frameworks, Business Process Modeling, SOA, and Infrastructure Technology*. CRC Press.
- Mittal, C. (2024). An empirical study on cybersecurity awareness, cybersecurity concern, and vulnerability to cyber-attacks. *Valley International Journal Digital Library*, 1144–1158. <https://doi.org/10.18535/ijssrm/v12i04.ec05>
- Moffitt, J., King, C., & Carley, K. M. (2021). Hunting conspiracy theories during the COVID-19 pandemic. *Social Media + Society*, 7(3), 20563051211043212. <https://doi.org/10.1177/20563051211043212>
- Mohan, A. M., Meskin, N., & Mehrjerdi, H. (2020). A comprehensive review of the cyber attacks and cyber-security on load frequency control of power systems. *Energies*, 13(15), 3860. <https://doi.org/10.3390/en13153860>
- Mulahuwaish, A., Qolomany, B., Gyorick, K., Bou Abdo, J., Aledhari, M., Qadir, J., Carley, K., & Al-Fuqaha, A. (2025). *A survey of social cybersecurity: Techniques for attack detection, evaluations, challenges, and future prospects*. *Computers in Human Behavior Reports*, 18, Article 100668. <https://doi.org/10.1016/j.chbr.2025.100668>
- Murdock, I., Carley, K. M., & Yagan, O. (2023). Identifying cross-platform user relationships in 2020 US election fraud and protest discussions. *Online Social Networks and Media*, 33, 100245. <https://doi.org/10.1016/j.osnem.2023.100245>
- Murillo, J. U., et al. (2024). Influencia de las tecnologías de la información y comunicación: Retos y potencialidades en la educación superior. *Revista San Gregorio*, 1(57), 170–185. <https://doi.org/10.36097/rsan.v1i57.2564>

- Mursi, K. T., Alahmadi, M. D., Alsubaei, F. S., & Alghamdi, A. S. (2022). Detecting Islamic radicalism Arabic tweets using natural language processing. *IEEE Access*, 10, 72526–72534. <https://doi.org/10.1109/ACCESS.2022.3182871>
- Narra, M., Umer, M., Sadiq, S., Karamti, H., Mohamed, A., Ashraf, I., et al. (2022). Selective feature sets based fake news detection for COVID-19 to manage infodemic. *IEEE Access*, 10, 98724–98736. <https://doi.org/10.1109/ACCESS.2022.3174245>
- Nejjari, N., Zkik, K., Hammouchi, H., Ghogho, M., & Benbrahim, H. (2024). Assessing data breach factors through modern crime theory: A structural equation modeling approach. *IEEE Access*, 12, 92198–92214. <https://doi.org/10.1109/ACCESS.2024.3423651>
- Nelson, J., & Gorichanaz, T. (2019). Trust as an ethical value in emerging technology governance: The case of drone regulation. *Technology in Society*, 59, 101131. <https://doi.org/10.1016/j.techsoc.2019.101131>
- Nespoli, P., Mármol, F. G., & Vidal, J. M. (2021). A bio-inspired reaction against cyberattacks: AIS-powered optimal countermeasures selection. *IEEE Access*, 9, 60971–60996. <https://doi.org/10.1109/ACCESS.2021.3083912>
- Ng, L. H. X., & Carley, K. M. (2022). Is my stance the same as your stance? A cross-validation study of stance detection datasets. *Information Processing & Management*, 59(6), 103070. <https://doi.org/10.1016/j.ipm.2022.103070>
- Nguyen, T., & Bhatia, S. (2020). Higher education social engineering attack scenario, awareness & training model. *Journal of The Colloquium for Information Systems Security Education*, 8(1).
- Nicholls, J., Kuppa, A., & Le-Khac, N. A. (2021). Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *IEEE Access*, 9, 163965–163986. <https://doi.org/10.1109/ACCESS.2021.3083719>
- Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric Theory*. McGraw-Hill Companies.
- Nwankpa, J. K., & Datta, P. M. (2023). Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers. *Computers & Security*, 130, 103266. <https://doi.org/10.1016/j.cose.2023.103266>
- Nwobodo, L. K., Nwaimo, C. S., & Adegbola, A. E. (2024). Enhancing cybersecurity protocols in the era of big data and advanced analytics. *GSC Advanced Research and Reviews*, 19(3). <https://doi.org/10.30574/gscarr.2024.19.3.0211>
- Ogbuke, N. J., Yusuf, Y. Y., Dharma, K., & Mercangoz, B. A. (2022). Big data supply chain analytics: Ethical, privacy, and security challenges posed to

- business, industries, and society. *Production Planning & Control*, 33(2-3), 123–137. <https://doi.org/10.1080/09537287.2020.1810764>
- Ojo-Gonzalez, K., Prosper-Heredia, R., Dominguez-Quintero, L., & Vargas-Lombardo, M. (2021). A model DevOps framework for SaaS in the cloud. *Advances in Intelligent Systems and Computing*, 1307, 37–51. https://doi.org/10.1007/978-3-030-62193-2_4
- Okutan, A., & Yang, S. J. (2019). ASSERT: Attack synthesis and separation with entropy redistribution towards predictive cyber defense. *Cybersecurity*, 2(1), 1–18. <https://doi.org/10.1186/s42400-019-0024-6>
- Olowononi, F. O., Rawat, D. B., & Liu, C. (2020). Resilient machine learning for networked cyber-physical systems: A survey for machine learning security to securing machine learning for CPS. *IEEE Communications Surveys & Tutorials*, 23(1), 524–552. <https://doi.org/10.1109/COMST.2020.2974786>
- Omolara, A. E., Jantan, A., Abiodun, O. I., Dada, K. V., Arshad, H., & Emmanuel, E. (2019). Adeception model robust to eavesdropping over communication for social network systems. *IEEE Access*, 7, 100881–100898. <https://doi.org/10.1109/ACCESS.2019.2933941>
- Orlikowski, W. J., & Gash, D. C. (1994). Technological frames: Making sense of information technology in organizations. *ACM Transactions on Information Systems*, 12(2), 174–207. <https://doi.org/10.1145/196734.196745>
- Ormachea Montes, J. F. (2020). Center for Higher National Studies- Postgraduate School. *Revista de Ciencia e Investigación en Defensa - CAEN*, 1(4), Art. 4.
- Ormachea, J. F. (2020). *Estrategias Integradas de Ciberseguridad para el Fortalecimiento de la Seguridad Nacional* [Centro de Altos Estudios Nacionales - Escuela de Posgrado]. <https://renati.sunedu.gob.pe/handle/sunedu/1336266>
- Oukemeni, S., Rifa-Pous, H., & Puig, J. M. M. (2019). IPAM: Information privacy assessment metric in microblogging online social networks. *IEEE Access*, 7, 114817–114836. <https://doi.org/10.1109/ACCESS.2019.2934600>
- Oyewole, A. T., Oguejiofor, B. B., Eneh, N. E., Akpuokwe, C. U., & Bakare, S. S. (2024). Data privacy laws and their impact on financial technology companies: A review. *Computer Science & IT Research Journal*, 5(3). <https://doi.org/10.51594/csitrj.v5i3.911>
- Pandey, A. B., Tripathi, A., & Vashist, P. C. (2022). A survey of cybersecurity trends, emerging technologies and threats. In *Cyber Security in Intelligent Computing and Communications* (pp. 19–33). Springer.
- Panorama en América Latina 2023*. (2023, agosto 23). [Blog]. Kaspersky Daily. <https://latam.kaspersky.com/blog/panorama-amenazas-latam-2023/26586/>

- Parkinson, S., & Khana, S. (2022). Identifying high-risk over-entitlement in access control policies using fuzzy logic. *Cybersecurity*, 5(1), 1–17. <https://doi.org/10.1186/s42400-022-00112-1>
- Peña-Casanova, M., & Anias-Calderón, C. (2020). Integración de marcos de referencia para gestión de Tecnologías de la Información. *Ingeniería Industrial*, 41(1). http://scielo.sld.cu/scielo.php?script=sci_abstract&pid=S1815-59362020000100011&lng=es&nrm=iso&tlng=pt
- Peralta, J. B., Donoso, X. V., Morales, N. C., & Aguilar, K. M. (2021). ¿Cómo se usan las tecnologías de la información y comunicación (TIC), y las redes sociales (RRSS) en la micro, pequeña y mediana empresa (MIPYMES)? Caso: Región de Arica y Parinacota, Chile. *Iberoamerican Business Journal*, 5(1), Art. 1. <https://doi.org/10.22451/5817.ibj2021.vol5.1.11050>
- Pincovscy, J. A., & Costa-Gondim, J. J. (2023). Methodology for cyber threat intelligence with sensor integration. *Lecture Notes in Networks and Systems*, 678, 14–28. https://doi.org/10.1007/978-3-031-30592-4_2
- Poma, A., & Vargas, R. (2019). Problemática en Ciberseguridad como protección de sistemas informáticos y redes sociales en el Perú y en el Mundo. *SCIENDO*, 22(4), Art. 4. <https://doi.org/10.17268/sciendo.2019.034>
- Popescu, T. M., Popescu, A. M., & Prostean, G. (2021). Leaders' perspectives on IoT security risk management strategies in surveyed organizations relative to IoTSRM2. *Applied Sciences*, 11(19), 9206. <https://doi.org/10.3390/app11199206>
- Pramod, T., Boroojeni, K. G., Amini, M. H., Sunitha, N., & Iyengar, S. (2019). Key pre-distribution scheme with join-leave support for SCADA systems. *International Journal of Critical Infrastructure Protection*, 24, 111–125. <https://doi.org/10.1016/j.ijcip.2019.01.004>
- Presidencia del Consejo de Ministros. (2023). Decreto Supremo N.º 085-2023-PCM: Decreto que regula disposiciones clave para la administración pública. Retrieved October 13, 2024, from <https://www.gob.pe/institucion/pcm/normas-legales/4471543-085-2023-pcm>
- Presidencia del Consejo de Ministros. (2024). Reglamento de la ley de gobierno digital: Documento regulatorio esencial para la transformación digital en Perú. Retrieved October 13, 2024, from <https://www.gob.pe/13326-reglamento-de-la-ley-de-gobierno-digital>
- Presidencia del Consejo de Ministros. (2024). Reporte sobre entidades que implementaron su equipo de respuestas ante incidentes de seguridad digital. Análisis sobre el estado de la ciberseguridad en entidades públicas peruanas. Retrieved October 13, 2024, from <https://www.gob.pe/es/i/2605569>
- Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. *Journal of the Academy of*

Marketing Science, 50(6), 1299–1323. <https://doi.org/10.1007/s11747-022-00845-y>

- Quispe, A., Calla, K. M., Yangali, J. S., Rodríguez, J. L., & Pumacayo, I. I. (2019). *Estadística no paramétrica aplicada a la investigación científica con software SPSS, MINITAB Y EXCEL* (1ra ed.). Editorial EIDEC. <https://editorialeidec.com/producto/estadistica-no-parametrica-aplicada-a-la-investigacion-cientifica-con-software-spss-minitab-y-excel/>
- Rahman, S., Hossain, N. U. I., Govindan, K., Nur, F., & Bappy, M. (2021). Assessing cyber resilience of additive manufacturing supply chain leveraging data fusion technique: A model to generate cyber resilience index of a supply chain. *CIRP Journal of Manufacturing Science and Technology*, 35, 911–928. <https://doi.org/10.1016/j.cirpj.2021.02.003>
- Ramezani, S., & Niemi, V. (2024). Cybersecurity education in universities: A comprehensive guide to curriculum development. *IEEE Access*, 12, 61741–61766. <https://doi.org/10.1109/ACCESS.2024.3392970>
- Razali, N. A. M., et al. (2023). Political security threat prediction framework using hybrid lexicon-based approach and machine learning technique. *IEEE Access*, 11, 17151–17164. <https://doi.org/10.1109/ACCESS.2023.3225765>
- Ren, J., et al. (2020). Complex social contagions on weighted networks considering adoption threshold heterogeneity. *IEEE Access*, 8, 61905–61914. <https://doi.org/10.1109/ACCESS.2020.2993461>
- Ringle, C. M., Wende, S., & Becker, J. M. (2024). *SmartPLS 3: Software for PLS-SEM*. Retrieved November 12, 2024, from <http://www.smartpls.com>
- Rodríguez, E., Santisteban, J., Morales, V., & Morales, J. (2024). Emerging technologies that ensure information resilience against social engineering attacks. In M. V. Garcia, C. Gordón-Gallegos, A. Salazar-Ramírez, & C. Nuñez (Eds.), *Proceedings of the International Conference on Computer Science, Electronics and Industrial Engineering (CSEI 2023)* (Vol. 797, pp. 133–145). Lecture Notes in Networks and Systems. Springer. https://doi.org/10.1007/978-3-031-70981-4_14
- Rodríguez, E., Santisteban, J., Morales, V., & Morales, J. (2024). Factors influencing frameworks for social cybersecurity management: A systematic literature review. In M. V. Garcia, C. Gordón-Gallegos, A. Salazar-Ramírez, & C. Nuñez (Eds.), *Proceedings of the International Conference on Computer Science, Electronics and Industrial Engineering (CSEI 2023)* (Vol. 797, pp. 119–131). Lecture Notes in Networks and Systems. Springer. https://doi.org/10.1007/978-3-031-70981-4_12
- Rojas, M., & Gilberto, J. (2022). *Influencia del covid 19 en el incremento de los ciberataques a nivel mundial*. <http://repository.unipiloto.edu.co/handle/20.500.12277/11574>

- Roldán, J. L., & Sánchez-Franco, M. J. (2012). Variance-based structural equation modeling: Guidelines for using partial least squares in information systems research. In *Research Methodologies, Innovations and Philosophies in Software Systems Engineering and Information Systems* (pp. 193–221). IGI Global. <https://doi.org/10.4018/978-1-4666-0179-6.ch010>
- Ross, J., Weill, P., & Robertson, D. (2006). *Enterprise Architecture as Strategy: Creating a Foundation for Business Execution* (1ra ed.). Harvard Business Review Press. <https://www.alibris.com/search/books/isbn/9781591398394>
- Rossi Lévano, G. (2021). La Seguridad y Defensa en la era de la Cuarta Revolución Industrial: Elementos para una propuesta de estrategia de política exterior para el fortalecimiento de las capacidades del Perú en materia de ciberdefensa y amenazas híbridas. *Repositorio Institucional - ADP*. <http://repositorio.adp.edu.pe/handle/ADP/170>
- Ruiz-Navarro, J. A., Santos-López, F. M., Portella-Delgado, J. M., & Santos-de-la Cruz, E. G. (2022). Computer vision technique to improve the color ratio in estimating the concentration of free chlorine. *Lecture Notes in Networks and Systems*, 433, 127–141. https://doi.org/10.1007/978-3-030-79567-9_11
- Ryan, P., Fokker, J., Healy, S., & Amann, A. (2022). Dynamics of targeted ransomware negotiation. *IEEE Access*, 10, 32836–32844. <https://doi.org/10.1109/ACCESS.2022.3174169>
- Saeed, S. (2023). A customer-centric view of e-commerce security and privacy. *Applied Sciences*, 13(2). <https://doi.org/10.3390/app13021020>
- Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for business resilience: Issues and recommendations. *Sensors*, 23(15). <https://doi.org/10.3390/s23156666>
- Salinas, A. P. (2022). *Modelo de ciberseguridad para cajas municipales en tiempos de transformación digital—Un nuevo enfoque* [Universidad Privada del Norte]. <https://renati.sunedu.gob.pe/handle/sunedu/3098504>
- Sanabria-Ardila, M., Navarro, L. D. B., Díaz-López, D., & Garzón-Alfonso, W. (2020). A semantic framework for the design of distributed reactive real-time languages and applications. *IEEE Access*, 8, 143862–143880. <https://doi.org/10.1109/ACCESS.2020.3011995>
- Sánchez-Paniagua, M., Fernández, E. F., Alegre, E., Al-Nabki, W., & Gonzalez-Castro, V. (2022). Phishing URL detection: A real-case scenario through login URLs. *IEEE Access*, 10, 42949–42960. <https://doi.org/10.1109/ACCESS.2022.3180539>
- Santana-Rodríguez, L., Pérez-Lorences, P., Abreu-Ledón, R., Santana-Rodríguez, L., Pérez-Lorences, P., & Abreu-Ledón, R. (2019). La gestión de Tecnologías de la Información: Análisis factorial confirmatorio. *Ingeniería Industrial*, 40(3), 272–284.

- Sebastian, G. (2023). A descriptive study on the metaverse: Cybersecurity risks, controls, and regulatory framework. *International Journal of Social and Political Cybersecurity*, 15(1), 1–14. <https://doi.org/10.4018/IJSPPC.315591>
- Security Report*. (s. f.). ESET - Seguridad Digital en Latinoamerica. Recuperado 11 de noviembre de 2022, de <https://www.eset.com/ve/security-report/>
- Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cybersecurity strategies. *International Journal of Computer Science and Information Security*, 14(1), 129–136. <https://www.ijcsis.org>
- Shah, M. U., Iqbal, F., Rehman, U., & Hung, P. C. K. (2023). A comparative assessment of human factors in cybersecurity: Implications for cyber governance. *IEEE Access*, 11, 87970–87984. <https://doi.org/10.1109/ACCESS.2023.3296580>
- Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, 124, 102974. <https://doi.org/10.1016/j.cose.2022.102974>
- Shaikh, F. A., & Siponen, M. (2024). Organizational learning from cybersecurity performance: Effects on cybersecurity investment decisions. *Information Systems Frontiers*, 26(3), 1109–1120. <https://doi.org/10.1007/s10796-023-10404-7>
- Sharma, P. (2024). Enforcing network security policies in the context of the NIST cybersecurity framework and its legal implications. *Network Security*, 2024(7). <https://doi.org/10.1016/j.netsec.2024.04.001>
- Skopik, F., & Pahi, T. (2020). Under false flag: Using technical artifacts for cyber attack attribution. *Cybersecurity*, 3(1), 1–20. <https://doi.org/10.1186/s42400-020-00048-4>
- Song, Z., Ma, H., Sun, S., Xin, Y., & Zhang, R. (2023). Rainbow: Reliable personally identifiable information retrieval across multi-cloud. *Cybersecurity*, 6(1), 19. <https://doi.org/10.1186/s42400-023-00131-7>
- Sriram, I. G. K. (2022). Security challenges of big data computing. *International Research Journal of Modern Engineering & Technology*. Retrieved from <https://www.irjmets.com/paperdetail.php?paperId=a72c9bc7917f48291e5088df405cb17c&title=SECURITY+CHALLENGES+OF+BIG+DATA+COMPUTING&authpr=Gopala+Krishna+Sriram>
- Straub, D. W., & Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, 22(4), 441. <https://doi.org/10.2307/249551>
- Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity behavior among government employees: The role of protection motivation theory and responsibility in mitigating cyberattacks. *Information*, 13(9). <https://doi.org/10.3390/info13090413>

- Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards: A review and comprehensive overview. *Electronics*, 11(14), 2181. <https://doi.org/10.3390/electronics11142181>
- Taherdoost, H. (2024). A critical review on cybersecurity awareness frameworks and training models. *Procedia Computer Science*, 235, 1649–1663. <https://doi.org/10.1016/j.procs.2024.04.156>
- Tajfel, H. (1974). Social identity and intergroup behaviour. *Social Science Information*, 13(2), 65-93. <https://doi.org/10.1177/053901847401300204>
- Terhörst, P., Fährmann, D., Damer, N., Kirchbuchner, F., & Kuijper, A. (2021). On soft biometric information stored in biometric face embeddings. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 3(4), 519–534. <https://doi.org/10.1109/TBIOM.2020.3034131>
- Thomson, R., & Pyke, A. (2025). *Social cybersecurity in 2023: a review of the 16th annual SBP-BRiMS conference*. *Computational and Mathematical Organization Theory*, 31, 105–108. <https://doi.org/10.1007/s10588-025-09400-w>
- Uddin, S. S. (2022). Importance of cyber education in the era of cyber war. *Pakistan Journal of Education and Research*, 5(2). <https://doi.org/10.52337/pjer.v5i2.530>
- Varma, G., Chauhan, R., & Singh, D. (2022). SARVE: Synthetic data and local differential privacy for private frequency estimation. *Cybersecurity*, 5(1), 26. <https://doi.org/10.1186/s42400-022-00087-2>
- Veliz, J. (2022, octubre 20). *Filtración de datos, PCM y ASBANC: ciberseguridad estatal | RPP Noticias* [Blog]. RPP Noticias - Niusgeek. <https://rpp.pe/tecnologia/mas-tecnologia/filtracion-de-datos-pcm-y-asbanc-ciberseguridad-estatal-noticia-1406543>
- Vielberth, M. (2019). Human-as-a-security-sensor for harvesting threat intelligence. *Cybersecurity*, 2(1), 1–15. <https://doi.org/10.1186/s42400-019-0040-0>
- Villa Mesa, S. (2018). *Impacto del riesgo cibernético en el segmento mipyme* [MasterThesis, Universidad EAFIT]. <http://repository.eafit.edu.co/handle/10784/12890>
- Villafuerte, N., Manzano, S., Ayala, P., & García, M. V. (2023). Artificial intelligence in virtual telemedicine triage: A respiratory infection diagnosis tool with electronic measuring device. *Future Internet*, 15(7). <https://doi.org/10.3390/fi15070227>
- Wang, Z., Sun, L., & Zhu, H. (2020). Defining social engineering in cybersecurity. *IEEE Access*, 8, 85,094–85,115. <https://doi.org/10.1109/ACCESS.2020.2997401>
- Wang, Z., Sun, L., & Zhu, H. (2020). Defining social engineering in cybersecurity. *IEEE Access*, 8, 85094–85115. <https://doi.org/10.1109/ACCESS.2020.2999704>

- Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE Access*, 9, 11895–11910. <https://doi.org/10.1109/ACCESS.2021.3058597>
- What the New 2019 Data Breach Report Means for Your Identity. (2020, noviembre 2). ITRC. <https://www.idtheftcenter.org/post/what-the-new-2019-data-breach-report-means-for-your-identity/>
- Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, 66, 102520. <https://doi.org/10.1016/j.ijinfomgt.2022.102520>
- Wu, X., Duan, R., & Ni, J. (2024). Unveiling security, privacy, and ethical concerns of ChatGPT. *Journal of Information and Intelligence*, 2(2), 102–115. <https://doi.org/10.1016/j.jiixd.2023.10.007>
- Wu, Y., Edwards, W. K., & Das, S. (2022). Sok: Social cybersecurity. In *2022 IEEE Symposium on Security and Privacy (SP)* (pp. 1863–1879). <https://doi.org/10.1109/SP46214.2022.9833757>
- Xian, X., Wu, T., Qiao, S., Wang, W., Liu, Y., & Han, N. (2020). Multi-view low-rank coding-based network data de-anonymization. *IEEE Access*, 8, 94575–94593. <https://doi.org/10.1109/ACCESS.2020.2991314>
- Xiong, X., Xie, C., Zhao, R., Li, Y., Ju, S., & Jin, M. (2019). A clickthrough rate prediction algorithm based on users' behaviors. *IEEE Access*, 7, 174782–174792. <https://doi.org/10.1109/ACCESS.2019.2950215>
- Yang, W., Li, D., & Liang, F. (2019). Sina Weibo bursty event detection method. *IEEE Access*, 7, 163160–163171. <https://doi.org/10.1109/ACCESS.2019.2955892>
- Yi, F., Jiang, B., Wang, L., & Wu, J. (2020). Cybersecurity named entity recognition using multi-modal ensemble learning. *IEEE Access*, 8, 63214–63224. <https://doi.org/10.1109/ACCESS.2020.2986372>
- Zambrano, P., et al. (2019). Technical mapping of the grooming anatomy using machine learning paradigms: An information security approach. *IEEE Access*, 7, 142129–142146. <https://doi.org/10.1109/ACCESS.2019.2944620>
- Zevallos, M. E. (2021). *Redes sociales y su incidencia en la vulneración del derecho a la intimidad en los habitantes de Trujillo, 2020* [Universidad César Vallejo]. <https://repositorio.ucv.edu.pe/handle/20.500.12692/69219>
- Zhang, J., & Zhang, Z. (2023). Ethics and governance of trustworthy medical artificial intelligence. *BMC Medical Informatics and Decision Making*, 23(1). <https://doi.org/10.1186/s12911-023-02103-9>

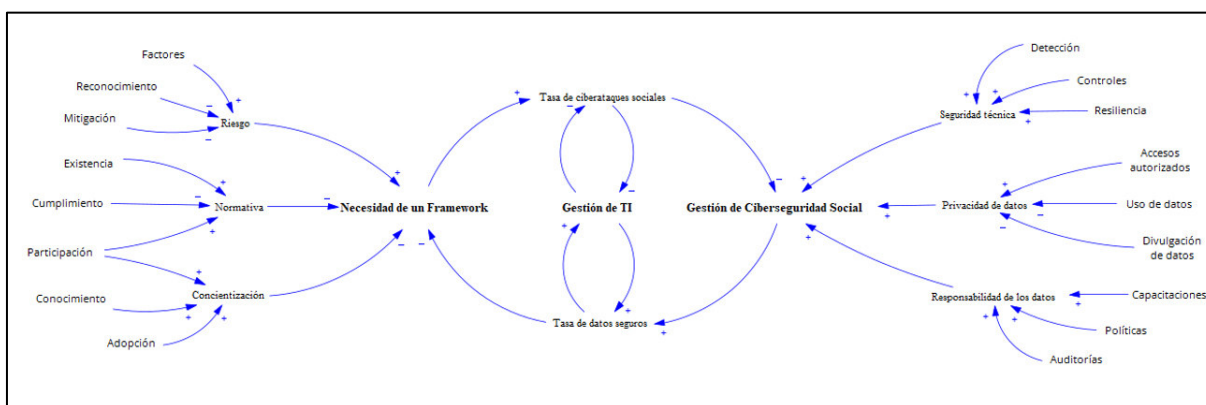
- Zhang, Y., Huo, W., Jian, K., Shi, J., Liu, L., Zou, Y., Zhang, C., & Liu, B. (2021). ESRFuzzer: An enhanced fuzzing framework for physical SOHO router devices to discover multi-type vulnerabilities. *Cybersecurity*, 4(1), 1–22. <https://doi.org/10.1186/s42400-021-00058-7>
- Zhou, C., Hu, B., Shi, Y., Tian, Y.-C., Li, X., & Zhao, Y. (2020). A unified architectural approach for cyberattack-resilient industrial control systems. *Proceedings of the IEEE*, 109(4), 517–541. <https://doi.org/10.1109/JPROC.2020.2979057>
- Zhou, Y., Zheng, C., Yang, A., & Wang, Y. (2025). *Social Cybersecurity in Conflict Zones: Quantitative Analysis of Narrative Manipulation on X*. In G. Yin, X. Liu, J. Su, & Y. Yang (Eds.), *Proceedings of the 14th International Conference on Computer Engineering and Networks (CENet 2024) (Lecture Notes in Electrical Engineering, Vol. 1387, pp. 365–373)*. Springer, Singapore. https://doi.org/10.1007/978-981-96-4245-8_32
- Zhu, L., Ma, Z., Huang, H., & Yan, M. (2021). Research on cybersecurity risk prevention and control of new infrastructure. *Journal of Physics: Conference Series*, 1856(1), 012034. <https://doi.org/10.1088/1742-6596/1856/1/012034>
- Zhu, X., Yang, Q., Tian, H., Ma, J., & Wang, W. (2019). Contagion of information on two-layered weighted complex networks. *IEEE Access*, 7, 155064–155074. <https://doi.org/10.1109/ACCESS.2019.2945467>
- Zulfahmi, M., Elsandi, A., Apriliansyah, A., Anggreainy, M. S., Iskandar, K., & Karim, S. (2023). Privacy protection strategies on social media. *Procedia Computer Science*, 216, 471–478. <https://doi.org/10.1016/j.procs.2023.01.064>

ANEXOS

ANEXO A MATRIZ TEÓRICA DEL PROBLEMA

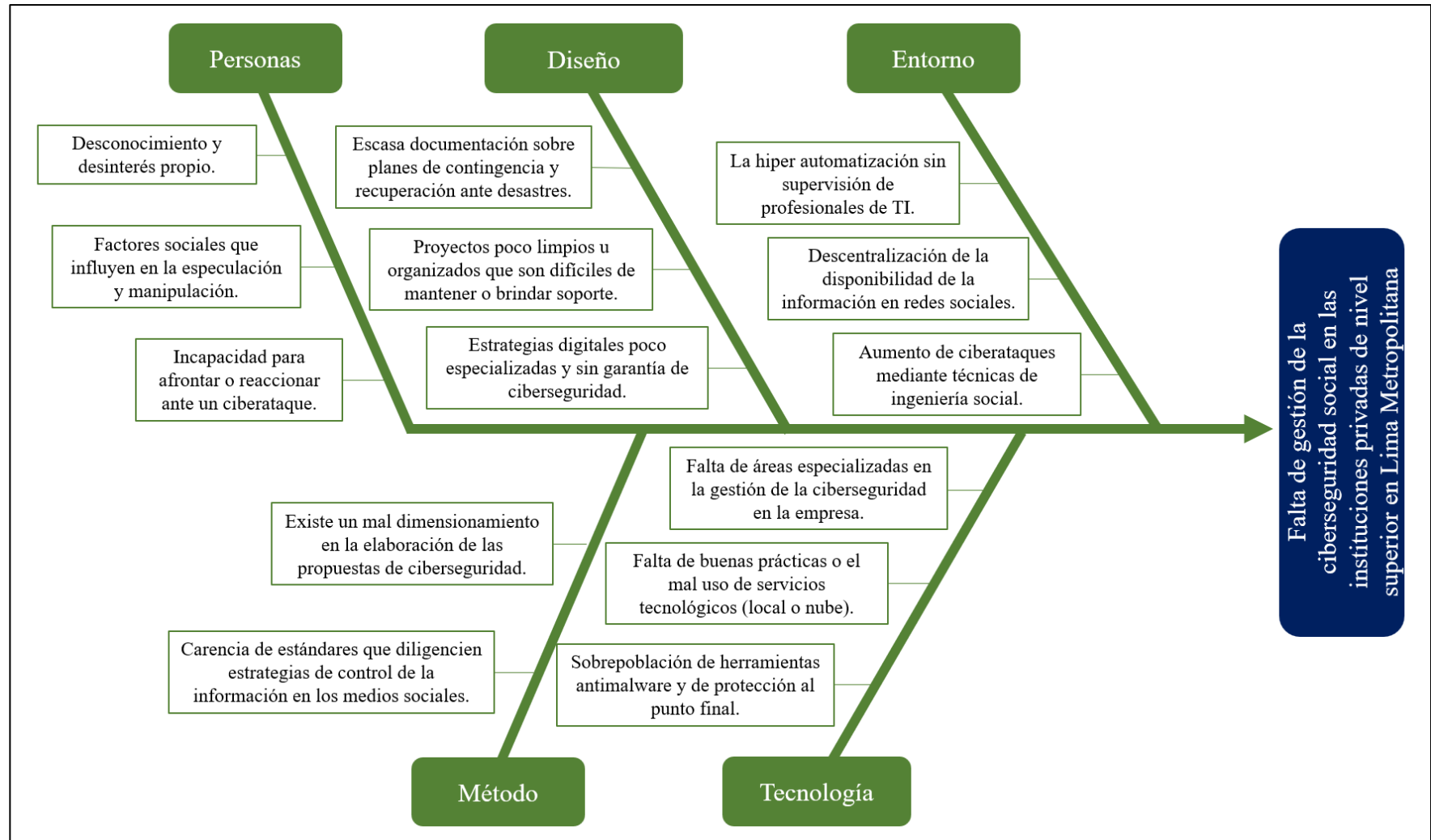
Bases teóricas					
T1: Teoría general de la disuasión	T2: Teoría de la identidad social	T3: Teoría de las redes sociales	T4: Teoría general de sistemas	T5: Marcos de referencia tecnológicos	
Conceptos generales					
C1: Ingeniería social	C2: Ciberseguridad	C3: Riesgo cibernético	C4: Gestión de TI	C5: Ciberseguridad social	C6: Marcos de referencia
Construcción del problema					
Deficiencia en la gestión de la ciberseguridad social					

ANEXO B DIAGRAMA CAUSAL DEL PROBLEMA



ANEXO C

DIAGRAMA CAUSA-EFECTO



ANEXO D

MATRIZ DE CONSISTENCIA

TÍTULO	FORMULACIÓN DEL PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES, DIMENSIONES E INDICADORES	METODOLOGÍA DE LA INVESTIGACIÓN
Un framework para la gestión de la ciberseguridad social en instituciones privadas de educación superior de Lima Metropolitana	PROBLEMA GENERAL	OBJETIVO GENERAL:	HIPÓTESIS PRINCIPAL:	Independiente (X) Marco de trabajo D1: Riesgo de ciberseguridad Factor de riesgo Reconocimiento del riesgo Mitigación del riesgo D2: Normativas de ciberseguridad Existencia normativa Cumplimiento normativo Participación normativa D3: Concientización de ciberseguridad Conocimiento de ciberseguridad Participación de ciberseguridad Adopción de ciberseguridad	Tipo de Investigación: Aplicada Diseño de Investigación: Diseño Nivel o alcance: Descriptivo Enfoque: Cuantitativo Método: Encuestas Instrumento: Cuestionario Unidad de análisis: Instituciones privadas de nivel superior de Lima
	PG: ¿Cómo el diseño de un nuevo marco de trabajo permite asegurar la gestión de la ciberseguridad social en las instituciones privadas de educación superior que sufren pérdidas de datos?	OG: Diseñar un marco de trabajo para asegurar la gestión de la ciberseguridad social en las instituciones privadas de educación superior que sufren pérdidas de datos.	HG: El marco de trabajo propuesto permitirá asegurar la gestión de la ciberseguridad social en las instituciones privadas de educación superior que sufren pérdidas de datos.		
	PROBLEMAS ESPECÍFICOS:	OBJETIVOS ESPECÍFICOS:	HIPÓTESIS ESPECÍFICAS:	Dependiente (Y) Gestión de la ciberseguridad social D1: Seguridad técnica Detección de incidentes Controles de seguridad Resiliencia D2: Privacidad de los datos Accesos autorizados Uso de los datos Divulgación de los datos D3: Responsabilidad de los datos Personal capacitado Políticas Auditorías	
	PE1: ¿Cuáles son los factores de la ciberseguridad social que influyen en la pérdida de datos en las instituciones privadas de educación superior? PE2: ¿Qué criterios deben considerarse para asegurar la gestión de la ciberseguridad social en las instituciones privadas de educación superior? PE3: ¿Cómo puede diseñarse un marco de trabajo para la gestión de la ciberseguridad social en las instituciones privadas de educación superior?	OE1: Identificar los factores de la ciberseguridad social que influyen en la pérdida de datos en las instituciones privadas de educación superior. OE2: Describir un conjunto de criterios que aseguren la gestión de la ciberseguridad social en las instituciones privadas de educación superior. OE3: Diseñar un marco de trabajo para la gestión de la ciberseguridad social en las instituciones privadas de educación superior.	HE1: La identificación de los factores de la ciberseguridad social permitirá establecer las principales dimensiones que inciden en pérdidas de datos en las instituciones privadas de educación superior. HE2: La descripción de los criterios servirá como base para la estructuración del marco de trabajo para la gestión de la ciberseguridad social en las instituciones privadas de educación superior. HE3: El marco de trabajo diseñado permite la gestión de la ciberseguridad social en las instituciones privadas de educación superior.		

ANEXO E CUESTIONARIO



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Facultad de Ingeniería de Sistemas e Informática
Unidad de Posgrado



CUESTIONARIO DIRIGIDO A LOS RESPONSABLES DE TI DE LAS UNIVERSIDADES PRIVADAS DE LIMA METROPOLITANA

Objetivo: Conocer su punto de vista con respecto al nuevo fenómeno denominado Ciberseguridad Social dentro de las Instituciones Privadas de Educación Superior de Lima Metropolitana, y está dirigida a los ejecutivos del segmento de Gerencia/Jefatura/Analista de Tecnología, Ciberseguridad o afines.

Antes de empezar:

- No escriba su nombre o de la institución en este cuestionario.
- Sus respuestas serán anónimas y serán utilizadas estrictamente para fines de la investigación.
- Es importante que responda a todas las preguntas.
- Poner sólo una respuesta.
- No hay respuestas correctas o capciosas.
- Su opinión es valiosa para el éxito de la investigación.

En primer lugar, se le pide que conteste las preguntas de la parte I, correspondientes a las características de los ejecutivos pertenecientes al área de Tecnología, Ciberseguridad o afines; la sección 2 refiere a los factores que influyen en la adopción de un marco de trabajo en la Ciberseguridad, la cual se encuentra dividida en 3 subsecciones: Riesgo, Normativa y Concientización; por último, la sección 3 refiere a los factores que influyen en la Gestión de la Ciberseguridad Social, la cual se encuentra dividida en 3 subsecciones: Seguridad Técnica, Privacidad de Datos y Responsabilidad de los Datos.

Responda la encuesta de acuerdo con su percepción y experiencia, marcando con ✓ o una X o rellenando el recuadro que más se acerque a su respuesta, considerando la escala del 1 como “Nunca” al 5 como “Siempre”.

Ejemplos: 12345 123X5 12345, donde:

Intención	Nunca	A veces	Normalmente	Casi siempre	Siempre
Valor	1	2	3	4	5

¡Muchas gracias por su colaboración!

Sección I: Características demográficas**1. Género:**

- ☐ Masculino
- ☐ Femenino

2. Grupo de edad:

- ☐ Menos de 18
- ☐ 18 - 24
- ☐ 25 – 34
- ☐ 35 – 44
- ☐ 45 – 54
- ☐ Encima de 55

3. ¿Cuál es el nivel máximo de estudio alcanzado por Usted?

- ☐ Técnica Incompleta
- ☐ Técnica Completa
- ☐ Universitaria Incompleta
- ☐ Universitaria Completa
- ☐ Posgrado

4. Indique el rango de años de experiencia en el sector educativo

- ☐ Menos de 1 año
- ☐ 01 – 05 años
- ☐ 06 – 10 años
- ☐ 11 – 20 años
- ☐ 21 - 25 años
- ☐ 26 – 30 años
- ☐ Encima de 30

5. Indique el rango de años de experiencia laboral (Considerando otros sectores)

- ☐ Menos de 1 año
- ☐ 01 – 05 años
- ☐ 06 – 10 años
- ☐ 11 – 20 años
- ☐ 21 - 25 años
- ☐ 26 – 30 años
- ☐ Encima de 30

6. Mencione la cantidad de tiempo que lleva laborando en la institución (en años o meses)**7. ¿Ha escuchado, leído o investigado sobre el término “Ciberseguridad Social”?**

- ☐ SI
- ☐ NO

8. Si la respuesta anterior es "SI", ¿Puede describirla o definirla a continuación?

Sección II: Factores que influyen en la adopción de un marco de trabajo en la Ciberseguridad

A continuación, se detalla una serie de preguntas para evaluar la necesidad de la implementación de un framework o marco de trabajo en las Instituciones Privadas de Educación Superior de Lima Metropolitana. Para evaluar la importancia que usted le atribuye a la influencia de los factores, en la escala de valoración marque según su apreciación:

Valoración: 1: Nunca / 2: A veces / 3: Normalmente / 4: Casi siempre / 5: Siempre.

Sub-Sección II-1: Con respecto a los Riesgos en la Ciberseguridad

- 1. ¿La institución identifica y evalúa regularmente los riesgos relacionados con la ciberseguridad?**

	1	2	3	4	5	
Nunca	☐	☐	☐	☐	☐	Siempre

- 2. ¿La institución aplica políticas y/o procedimientos claros para reconocer incidentes de ciberseguridad?**

	1	2	3	4	5	
Nunca	☐	☐	☐	☐	☐	Siempre

- 3. ¿Cree Ud. Que la institución informa o notifica los riesgos cibernéticos reconocidos a los involucrados?**

	1	2	3	4	5	
Nunca	☐	☐	☐	☐	☐	Siempre

- 4. ¿La institución continúa un proceso formal para identificar los riesgos de ciberseguridad?**

	1	2	3	4	5	
Nunca	☐	☐	☐	☐	☐	Siempre

- 5. ¿Cree Ud. Que la institución implementa medidas de seguridad técnicas para mitigar los riesgos de ciberseguridad?**

	1	2	3	4	5	
Nunca	☐	☐	☐	☐	☐	Siempre

- 6. ¿La institución refuerza las medidas de mitigación para reducir los riesgos de seguridad cibernéticos en los ambientes de trabajo?**

	1	2	3	4	5	
Nunca	☐	☐	☐	☐	☐	Siempre

Sub-Sección II-2: Con respecto a las Normativas de Ciberseguridad

- 7. ¿La institución informa a su personal de la existencia de políticas o procedimientos que regulen la seguridad cibernética?**

	1	2	3	4	5	
Nunca	☐	☐	☐	☐	☐	Siempre

8. ¿Cree Ud. Que la institución cumple con las normativas y regulaciones vigentes relacionadas con la ciberseguridad?

1 2 3 4 5
Nunca ☐ ☐ ☐ ☐ ☐ Siempre

9. ¿Las funciones que realiza el área de tecnología de la institución se adhieren a las normativas o regulaciones relacionadas con la ciberseguridad?

1 2 3 4 5
Nunca ☐ ☐ ☐ ☐ ☐ Siempre

10. ¿La institución realiza auditorías o revisiones para verificar el cumplimiento de normativas o regulaciones relacionadas con la ciberseguridad?

1 2 3 4 5
Nunca ☐ ☐ ☐ ☐ ☐ Siempre

11. ¿La institución promueve la concientización y capacitación de los miembros del área de tecnología sobre las normativas o regulaciones relacionadas con la ciberseguridad?

1 2 3 4 5
Nunca ☐ ☐ ☐ ☐ ☐ Siempre

12. ¿La institución fomenta la participación activa de otras áreas en la creación y/o actualización de normas o políticas relacionadas con la ciberseguridad?

1 2 3 4 5
Nunca ☐ ☐ ☐ ☐ ☐ Siempre

Sub-Sección II-3: Con respecto a la Concientización de la Ciberseguridad

13. ¿Cree Ud. Que el área de tecnología de la institución tiene el conocimiento de las principales amenazas cibernéticas?

1 2 3 4 5
Nunca ☐ ☐ ☐ ☐ ☐ Siempre

14. ¿Cree Ud. Que la institución en general está familiarizada con las mejores prácticas de ciberseguridad?

1 2 3 4 5
Nunca ☐ ☐ ☐ ☐ ☐ Siempre

15. ¿En qué medida los miembros de la institución participan activamente en actividades de concientización y capacitación sobre ciberseguridad?

1 2 3 4 5
Nunca ☐ ☐ ☐ ☐ ☐ Siempre

16. ¿En qué medida los miembros de la institución comparten conocimientos y experiencias relacionadas con la ciberseguridad?

1 2 3 4 5
Nunca ☐ ☐ ☐ ☐ ☐ Siempre

17. ¿Cree Ud. Que aplica las prácticas de seguridad cibernética recomendadas en su trabajo a diario?

1 2 3 4 5
Nunca ☐ ☐ ☐ ☐ ☐ Siempre

18. ¿Con qué frecuencia la institución utiliza las herramientas y medidas de seguridad proporcionadas para protegerse de amenazas cibernéticas?

1 2 3 4 5
Nunca ☐ ☐ ☐ ☐ ☐ Siempre

Sección III: Factores que influyen en la Gestión de la Ciberseguridad Social

A continuación, se detalla una serie de preguntas para ver la influencia de la gestión de la ciberseguridad social en las Instituciones Privadas de Educación Superior de Lima Metropolitana. Para evaluar la importancia que usted le atribuye a la influencia de los factores, en la escala de valoración marque según su apreciación:

Valoración: 1: Nunca / 2: A veces / 3: Normalmente / 4: Casi siempre / 5: Siempre.

Sub-Sección III-1: Con respecto a la Seguridad Técnica

19. ¿En qué medida se implementan herramientas de detección de intrusiones para identificar posibles brechas de seguridad en los sistemas de información?

1 2 3 4 5
Nunca ☐ ☐ ☐ ☐ ☐ Siempre

20. ¿La institución administra sistemas de alerta temprana para identificar potenciales ataques cibernéticos?

1 2 3 4 5
Nunca ☐ ☐ ☐ ☐ ☐ Siempre

21. ¿Con qué frecuencia se realizan evaluaciones y monitoreo de seguridad para detectar posibles vulnerabilidades en los sistemas de información?

1 2 3 4 5
Nunca ☐ ☐ ☐ ☐ ☐ Siempre

22. ¿Con qué frecuencia se realizan auditorías y revisiones de seguridad para evaluar la eficacia de los controles implementados dentro de la institución?

1 2 3 4 5
Nunca ☐ ☐ ☐ ☐ ☐ Siempre

23. ¿La institución reacciona con respaldos y planes de recuperación de datos ante la existencia de algún incidente o desastre?

1 2 3 4 5

Nunca ☐ ☐ ☐ ☐ ☐ Siempre

24. ¿Cree Ud. Que la institución realiza pruebas periódicas y simulacros de respuesta frente a posibles amenazas cibernéticas?

1 2 3 4 5

Nunca ☐ ☐ ☐ ☐ ☐ Siempre

Sub-Sección III-2: Con respecto a la Privacidad de Datos

25. ¿Cree Ud. Que el área de tecnología de la institución limita el acceso de control de sistemas basados en roles o privilegios?

1 2 3 4 5

Nunca ☐ ☐ ☐ ☐ ☐ Siempre

26. ¿En la institución se implementan controles de acceso para garantizar que solo las personas autorizadas tengan acceso a la información?

1 2 3 4 5

Nunca ☐ ☐ ☐ ☐ ☐ Siempre

27. ¿Constantemente existen usuarios de negocio que revisan los datos de los sistemas informáticos por algún motivo?

1 2 3 4 5

Nunca ☐ ☐ ☐ ☐ ☐ Siempre

28. ¿Cree Ud. Que la institución realiza un seguimiento del uso de los datos personales y sensibles para asegurar que se utilicen exclusivamente para los fines autorizados?

1 2 3 4 5

Nunca ☐ ☐ ☐ ☐ ☐ Siempre

29. En mi institución, ¿Con qué frecuencia se implementan medidas para garantizar que los datos solo sean divulgados a personal autorizado?

1 2 3 4 5

Nunca ☐ ☐ ☐ ☐ ☐ Siempre

30. ¿En la institución se fomenta la responsabilidad y la ética en relación con la divulgación adecuada de datos?

1 2 3 4 5

Nunca ☐ ☐ ☐ ☐ ☐ Siempre

Sub-Sección III-3: Con respecto a la Responsabilidad de los Datos

31. ¿Cree Ud. Que el área de tecnología de la institución recibe capacitación regular sobre las mejores prácticas y normas de seguridad para proteger los datos confidenciales?

1 2 3 4 5

Nunca ☐ ☐ ☐ ☐ ☐ Siempre

32. ¿Cree Ud. Que los empleados en general de la institución valoran los temas de protección de datos y ciberseguridad?

1 2 3 4 5

Nunca O O O O O Siempre

33. ¿Considero que las políticas existentes en mi institución son efectivas para garantizar la protección de los datos?

1 2 3 4 5

Nunca O O O O O Siempre

34. ¿Cree Ud. Que las políticas de protección de datos implementadas en la institución son claras y comprensibles para el personal de tecnología?

1 2 3 4 5

Nunca O O O O O Siempre

35. ¿Las auditorías periódicas realizadas en mi institución ayudan a evaluar el cumplimiento de las políticas de protección de datos?

1 2 3 4 5

Nunca O O O O O Siempre

36. ¿Mi institución brinda el apoyo necesario para implementar las recomendaciones surgidas de las auditorías de protección de datos?

1 2 3 4 5

Nunca O O O O O Siempre

ANEXO F
FICHAS DE VALIDACIÓN DEL INSTRUMENTO
(JUICIO EXPERTOS)

FICHA DE VALIDACIÓN DE INSTRUMENTO JUICIO DE EXPERTOS

I. DATOS INFORMATIVOS

Apellido y Nombre del Informante	Especialidad del evaluador(a)	Cargo o Institución donde Labora	Nombre del Instrumento de Evaluación	Autor(a) del Instrumento
Valencia Vivas Gloria Maritza	Doctora en Ingeniería de Sistemas e Informática	Universidad de las Fuerzas Armadas – ESPE	Encuesta de framework para la gestión de la ciberseguridad social	Elton Nick Roy Rodríguez Dulanto
Título: Un Framework para la gestión de la Ciberseguridad Social en Instituciones Privadas de Educación Superior de Lima Metropolitana.				

II. ASPECTOS DE VALIDACIÓN

INDICADORES	CRITERIOS	Deficiente 0- 20%	Regular 21- 40%	Buena 41- 60%	Muy buena 61-80%	Excelente 81- 100%
1. CLARIDAD	Está formulado con lenguaje apropiado.					86%
2. OBJETIVIDAD	Está expresado en conductas observables.					85%
3. ACTUALIDAD	Adecuado al avance de la ciencia y la tecnología.					96%
4. ORGANIZACIÓN	Los ítems del instrumento reflejan organización lógica.					99%
5. SUFICIENCIA	La cantidad de las preguntas es idónea para lograr el objetivo planteado				75%	
6. INTENCIONALIDAD	Adecuado para valorar aspectos metodológicos.					85%
7. CONSISTENCIA	Basado en aspectos teórico-científicos.					96%
8. COHERENCIA	Entre variables, dimensiones e indicadores.					96%
9. METODOLOGÍA	La estrategia responde al propósito del diagnóstico.					96%
10. PERTINENCIA	El instrumento es funcional para el propósito de la investigación.					92%

III. OPINIÓN DE APLICACIÓN

Aplicable [X] Aplicable después de corregir [] No aplicable []

IV. PROMEDIO DE VALIDACIÓN: 90.6%

Guayaquil, 02 de Setiembre de 2024	1204327900	 FIRMADO ELECTRONICAMENTE POR: GLORIA MARITZA VALENCIA VIVAS	593995734060
Lugar y fecha	DNI	Firma del Experto	Teléfono

FICHA DE VALIDACIÓN DE INSTRUMENTO JUICIO DE EXPERTOS

I. DATOS INFORMATIVOS

Apellido y Nombre del Informante	Especialidad del evaluador(a)	Cargo o Institución donde Labora	Nombre del Instrumento de Evaluación	Autor(a) del Instrumento
Castañeda Vargas Pedro Segundo	Ingeniero de Sistemas	DIGILINK S.A.C.	Ficha de Validación de Instrumento Juicio de Expertos	Elton Nick Roy Rodríguez Dulanto
Título: Un Framework para la gestión de la Ciberseguridad Social en Instituciones Privadas de Educación Superior de Lima Metropolitana.				

II. ASPECTOS DE VALIDACIÓN

INDICADORES	CRITERIOS	Deficiente 0- 20%	Regular 21- 40%	Buena 41- 60%	Muy buena 61-80%	Excelente 81- 100%
1. CLARIDAD	Está formulado con lenguaje apropiado.					X
2. OBJETIVIDAD	Está expresado en conductas observables.				X	
3. ACTUALIDAD	Adecuado al avance de la ciencia y la tecnología.					X
4. ORGANIZACIÓN	Los ítems del instrumento reflejan organización lógica.				X	
5. SUFICIENCIA	La cantidad de las preguntas es idónea para lograr el objetivo planteado				X	
6. INTENCIONALIDAD	Adecuado para valorar aspectos metodológicos.				X	
7. CONSISTENCIA	Basado en aspectos teórico científicos.				X	
8. COHERENCIA	Entre variables, dimensiones e indicadores.				X	
9. METODOLOGÍA	La estrategia responde al propósito del diagnóstico.				X	
10. PERTINENCIA	El instrumento es funcional para el propósito de la investigación.					X

III. OPINIÓN DE APLICACIÓN

Aplicable [X] Aplicable después de corregir [] No aplicable []

IV. PROMEDIO DE VALIDACIÓN: 87%

Lima, 16 de setiembre de 2024	10744358		998732355
Lugar y fecha	DNI	Firma del Experto	Teléfono

FICHA DE VALIDACIÓN DE INSTRUMENTO JUICIO DE EXPERTOS

I. DATOS INFORMATIVOS

Apellido y Nombre del Informante	Especialidad del evaluador(a)	Cargo o Institución donde Labora	Nombre del Instrumento de Evaluación	Autor(a) del Instrumento
Salas Arbaiza Cesar Enrique	Ingeniero	Docente	Encuesta	Elton Nick Roy Rodriguez Dulanto
Título: Un Framework para la gestión de la Ciberseguridad Social en Instituciones Privadas de Educación Superior de Lima Metropolitana.				

II. ASPECTOS DE VALIDACIÓN

INDICADORES	CRITERIOS	Deficiente 0- 20%	Regular 21- 40%	Buena 41- 60%	Muy buena 61-80%	Excelente 81- 100%
1. CLARIDAD	Está formulado con lenguaje apropiado.			X		
2. OBJETIVIDAD	Está expresado en conductas observables.		X			
3. ACTUALIDAD	Adecuado al avance de la ciencia y la tecnología.		X			
4. ORGANIZACIÓN	Los items del instrumento reflejan organización lógica.		X			
5. SUFICIENCIA	La cantidad de las preguntas es idónea para lograr el objetivo planteado			X		
6. INTENCIONALIDAD	Adecuado para valorar aspectos metodológicos.			X		
7. CONSISTENCIA	Basado en aspectos teórico científicos.		X			
8. COHERENCIA	Entre variables, dimensiones e indicadores.		X			
9. METODOLOGÍA	La estrategia responde al propósito del diagnóstico.			X		
10. PERTINENCIA	El instrumento es funcional para el propósito de la investigación.		X			

III. OPINIÓN DE APLICACIÓN

Aplicable [X]

Aplicable después de corregir []

No aplicable []

IV. PROMEDIO DE VALIDACIÓN: _13_

Lima, 09 de Setiembre de 2024	40038522		-
Lugar y fecha	DNI	Firma del Experto	Teléfono

ANEXO G

CARTA DE INVITACIÓN A LAS UNIVERSIDADES PRIVADAS



Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

VICEDECANATO DE INVESTIGACIÓN Y POSGRADO

Lima, 23 de junio del 2024

CARTA N° 01-FISI-VDIP-2024

Señor (a): Director de tecnología

ASUNTO: DISTRIBUIR CARTA DIRIGIDA A JEFES DE SISTEMAS O JEFES DE CIBERSEGURIDAD O EL QUE HAGA SUS VECES EN LAS INSTITUCIONES PRIVADAS DE EDUCACIÓN SUPERIOR DE LIMA METROPOLITANA PARA QUE RESPONDAN UNA ENCUESTA.

De mi consideración:

Por medio de la presente reciba un cordial saludo y así mismo hacer de su conocimiento que en la Maestría de Ingeniería de Sistemas de la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional Mayor de San Marcos, se viene desarrollando una investigación relacionada a la Ciberseguridad, denominado *“Un Framework para la gestión de la Ciberseguridad Social en Instituciones Privadas de Educación Superior de Lima Metropolitana”*.

Como parte de esta investigación se está realizando una encuesta a los Jefes, Responsables o encargados de la Gerencia de Sistemas y/o Ciberseguridad, o el que haga sus veces, por lo que agradeceré, se le brinde las facilidades para realizar la encuesta al Ing. Elton Nick Roy Rodríguez Dulanto, identificado con DNI 76029540, quien viene desarrollando dicha investigación para optar su grado de Magister.

Para contestar dicha encuesta, ingrese al siguiente enlace: <https://forms.office.com/r/UD8q6TtnpR>

Cabe precisar que la información obtenida será de carácter confidencial, y los resultados de esta investigación serán compartidas con su institución. Estamos seguros que contribuirá a la mejora en la implementación de prácticas en la gestión de la ciberseguridad social en las instituciones superiores del sector privado de Lima Metropolitana.

Expresando mis sentimientos de respeto y consideración me despido de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente,



Dra. Nora Bertha La Serna Palomino
Vicedecana de Investigación y Posgrado

Firmado digitalmente por LA SERNA
PALOMINO Nora Bertha FAU
20148092282 soft
Motivo: Soy el autor del documento
Fecha: 23.06.2023 15:52:42 -05:00

ANEXO H

PRODUCCIÓN CIENTÍFICA SOBRE LA INVESTIGACIÓN

ANEXO H.1.

1ER CERTIFICADO DE PONENCIA EN EL CONGRESO

“CONGRES OF COMPUTER, ELECTRONIC, AND

INDUSTRIAL SCIENCE – CSEI23”



UNIVERSIDAD
TÉCNICA DE AMBATO



FACULTAD DE INGENIERÍA EN
SISTEMAS, ELECTRÓNICA E INDUSTRIAL






**CONFERENCE ON COMPUTER
SCIENCE, ELECTRONICS AND
INDUSTRIAL ENGINEERING**

THIS CERTIFICATE IS PROUDLY AWARDED

TO: RODRIGUEZ DULANTO ELTON

Paper title: **FACTORS INFLUENCING FRAMEWORKS FOR SOCIAL CYBERSECURITY MANAGEMENT. A SYSTEMATIC LITERATURE REVIEW**

for your excellent oral presentation at the conference and your significant contribution to the success of the “V Conference on Computer Science, Electronics and Industrial Engineering (CSEI2023)” which held virtually in Ambato, Ecuador, from November 6th to November 10th, 2023.


 Ing. Carlos Núñez Mg.
 Chair of the Conference


 MSc. Elsa Pilar Urrutia
 President of Organizing Committee






ANEXO H.2.

1ER ARTÍCULO CIENTÍFICO: “FACTORS INFLUENCING FRAMEWORKS FOR SOCIAL CYBERSECURITY MANAGEMENT. A SYSTEMATIC LITERATURE REVIEW”

Author Proof



Factors Influencing Frameworks for Social Cybersecurity Management. A Systematic Literature Review

Elton Rodriguez¹ , José Santisteban² , Vicente Morales³ ,
and Johana Morales⁴

¹ Universidad Nacional Mayor de San Marcos, Av. Germán Amézaga s/n, 15081
Lima, Peru

elton.rodriguez1@unmsm.edu.pe

² Universidad Privada Norbert Wiener, Av. Arequipa 440 con Jr. Larrabure y
Unanue 110. Urb. Santa Beatriz, Lima, Peru

jsantistebanp1@unmsm.edu.pe

³ Universidad Técnica de Ambato, Los Chasquis y Río Payamino, 180103 Ambato,
Ecuador

jvmorales99@uta.edu.ec

⁴ Universidad Técnica Particular de Loja, San Cayetano Alto y C. París, 110107
Loja, Ecuador

jemorales22@utpl.edu.ec

Abstract. Currently, cybersecurity is a growing concern in society where cyber threats and risks have become increasingly sophisticated and frequent throughout the digital landscape. The purpose of this study is to analyze the factors, models, frameworks, and technologies applied in cybersecurity management within the social approach. Through a systematic review of the literature and an appropriate search strategy, 70 papers obtained from specialized sources such as IEEE Xplore, ScienceDirect, SpringerLink and Web of Science have been analyzed. Furthermore, applying an exhaustive exploration, those aspects that have proven to be relevant to be applied in effective management of social cybersecurity have been identified. The conjunction, understanding and application of these aspects in a strategic manner seeks to strengthen the protection of individuals, organizations, and communities against digital threats. This study has been developed as a valuable source of knowledge to address cybersecurity challenges in modern society and provide a solid foundation for future protection and prevention strategies.

[\[AQ1\]](#)

[\[AQ2\]](#)

[\[AQ3\]](#)

Keywords: Social Cybersecurity · Factors · Model · Frameworks ·
Emerging Technologies

1 Introduction

Currently, the adoption of technological platforms has become a fundamental part of the communication of millions of people around the world, since these

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2024
M. V. Garcia et al. (Eds.): CSEI 2023, LNNS 797, pp. 1–18, 2024.
https://doi.org/10.1007/978-3-031-70981-4_12

ANEXO H.3.

2DO CERTIFICADO DE PONENCIA EN EL CONGRESO

“CONGRES OF COMPUTER, ELECTRONIC, AND

INDUSTRIAL SCIENCE – CSEI23”



UNIVERSIDAD
TÉCNICA DE AMBATO



FACULTAD DE INGENIERÍA EN
SISTEMAS, ELECTRÓNICA E INDUSTRIAL





**CONFERENCE ON COMPUTER
SCIENCE, ELECTRONICS AND
INDUSTRIAL ENGINEERING**

THIS CERTIFICATE IS PROUDLY AWARDED

TO: RODRIGUEZ DULANTO ELTON

Paper title: EMERGING TECHNOLOGIES THAT ENSURE INFORMATION RESILIENCE AGAINST SOCIAL ENGINEERING ATTACKS

for your excellent oral presentation at the conference and your significant contribution to the success of the “V Conference on Computer Science, Electronics and Industrial Engineering (CSEI2023)” which held virtually in Ambato, Ecuador, from November 6th to November 10th, 2023.



Ing. Carlos Núñez Mg.
Chair of the Conference



MSc. Elsa Pilar Urrutia Urrutia
President of Organizing Committee






ANEXO H.4.

2DO ARTÍCULO CIENTÍFICO: “EMERGING TECHNOLOGIES THAT ENSURE INFORMATION RESILIENCE AGAINST SOCIAL ENGINEERING ATTACKS”

Author Proof



Emerging Technologies that Ensure Information Resilience Against Social Engineering Attacks

Elton Rodriguez¹ , José Santisteban² , Vicente Morales³ ,
and Johana Morales⁴

¹ Universidad Nacional Mayor de San Marcos, Av. Germán Amézaga s/n,
15081 Lima, Peru

elton.rodriguez1@unmsm.edu.pe

² Universidad Privada Norbert Wiener, Av. Arequipa 440 con Jr. Larrabure y
Unanue 110. Urb. Santa Beatriz, Lima, Peru

jsantistebanp1@unmsm.edu.pe

³ Universidad Técnica de Ambato, Los Chasquis y Río Payamino, 180103 Ambato,
Ecuador

jvmorales99@uta.edu.ec

⁴ Universidad de las Fuerzas Armadas - ESPE, Av. Gral. Rumiñahui S/N,
171103 Sangolquí, Ecuador

Abstract. The increase in technologies leads to a great challenge for organizations, since the greater the adoption of new technologies involved, the greater the risk of suffering cyberattacks that damage the integrity and continuity of the business. The aim of this research is to analyze how emerging technologies can be used effectively to strengthen the resilience of information in organizations against cyberattacks based on social engineering. Through this work, we proceeded to evaluate the consequences that cyberattacks due to social engineering and their relationship with information systems can have through a literature review of scientific articles in databases such as ScienceDirect, IEEE Xplore and Scopus. The results found show that emerging technologies such as artificial intelligence, the internet of things and blockchain are the main players in cybersecurity. These technologies ensure the resilience of information by providing control over how the information that organizations must safeguard is accessed and processed by building cyber resilient information systems.

[AQ1](#)

[AQ2](#)

[AQ3](#)

Keywords: Emerging Technologies · Information Resilience · Social Engineering · Cybersecurity

1 Introduction

In the current era, the increasing adoption of technologies in organizations has posed significant challenges. While these technologies offer opportunities

ANEXO H.5.

**CARTA DE ACEPTACIÓN DEL ARTÍCULO CIENTÍFICO DE
CONTRIBUCIÓN: "SCERA: MODEL FOR THE MANAGEMENT
OF SOCIAL CYBERSECURITY IN PRIVATE UNIVERSITIES"**



Computación y Sistemas

AN INTERNATIONAL JOURNAL OF COMPUTING SCIENCE AND APPLICATIONS

ISSN 1405-5546

Mexico City, 9 December, 2024.

Apartado Postal 75-546
C.P. 07738 México, D.F.
Tel. (+52)-55-57-29-60-00
Ext. 56518, 56643
Fax Ext 56607
computacion-y-sistemas@cic.ipn.mx

<http://cys.cic.ipn.mx>

ACCEPTANCE OF ARTICLE

This is to confirm that

Elton Nick Roy Rodriguez Dulanto, José Santisteban

served as the reviewer of the paper

***"SCERA: Model for the Management of Social
Cybersecurity in Private Universities".***

during the double blind reviewing process for the journal
Computacion y Sistemas, on November 22, 2024.

Sincerely.



Ph. Grigori Sidorov
Editor in Chief

ANEXO H.6.

3ER ARTÍCULO CIENTÍFICO: “SCERA: MODEL FOR THE MANAGEMENT OF SOCIAL CYBERSECURITY IN PRIVATE UNIVERSITIES”

SCERA: Model for the Management of Social Cybersecurity in Private Universities

Elton Rodriguez¹ and José Santisteban¹

¹Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Lima, Perú

elton.rodriguez1@unmsm.edu.pe, jsantistebanp1@unmsm.edu.pe

Abstract.

Educational institutions in Peru have faced significant challenges in terms of data security. This is largely due to the predominance of cyberattacks using social techniques, reflecting a lack of implementation of controls and practices in cyber management. In this context, it is crucial to develop a model that improves the collective management of cyberattacks, with the aim of strengthening resilience and promoting continuous improvement in private higher education institutions. This study proposes a model based on six constructs identified within social security. To validate the seven resulting relationships between the constructs, this research was carried out that included the participation of 30 technology managers from various institutions, using the partial least squares technique (PLS-SEM). The results obtained showed that six of the relationships were successfully validated, while one relationship suggests a possible area for future research. Notably, the relationship between "cybersecurity awareness" and "cybersecurity regulations" stood out as the most validated, underscoring its potential use within the proposed model to improve regulatory practices and comprehensive security in the educational field.

Keywords. Model, cybersecurity, social cybersecurity, data privacy, education.

1 Introduction

Educational institutions have rapidly transformed through digital adoption, enhancing collaboration and connectivity among students, teachers, and administrative staff. As the reliance on digital assets increases, educating about cybersecurity and ethics in cyberspace becomes essential [34]. According to the International Telecommunication Union (ITU) in its 2024 Global Cybersecurity

Index report, there is a widespread deficiency in developing effective strategies for raising awareness and adopting cybersecurity practices. Peru shows only a fundamental commitment to cybersecurity [26], which presents ongoing challenges -particularly in the social context, where the behavior of university users plays a crucial role in preventing and mitigating cyber incidents.

Furthermore, the growing reliance on technology in universities has raised significant concerns about the awareness, apprehension, and prior knowledge regarding cybersecurity among university staff and students, often emphasizing the risk of victimization [7]. In this context, the emerging concept of "social cybersecurity" refers to strategies and policies aimed at reducing cyber risks through the awareness and proper behavior of university internal users [9]. This presents a challenge for private universities to create a model that incorporates these factors into their cybersecurity practices, especially in Peru, where the regulatory and technological landscapes are still evolving.

The Presidency of the Council of Ministers (PCM) has announced that Supreme Decree No. 085-2023-PCM, which approves the National Digital Transformation Policy for 2030, highlights that Peru is facing challenges related to the limited advancement of digital security and the lack of trust in digital systems within society [42]. Supreme Decree No. 029-2021-PCM establishes a digital security framework, defining the principles and components of the digital security model [43]. In February 2024, public universities, due to the lack of a digital security incident response team [44], are classified as critical infrastructures. Despite