



UNIVERSIDAD ANDINA

NÉSTOR CÁCERES VELÁSQUEZ

ESCUELA DE POSGRADO

PROGRAMA DE SEGUNDA ESPECIALIDAD PROFESIONAL



TRABAJO ACADÉMICO

**PROTEGIENDO NUESTRA INFORMACIÓN EN LA ERA DIGITAL EN
ESTUDIANTES DEL CUARTO GRADO DE LA INSTITUCIÓN
EDUCATIVA SAN LUIS GONZAGA ICA 2023**

PRESENTADO POR:

EDDY ROJAS CHANCO

**PARA OPTAR EL TÍTULO DE SEGUNDA ESPECIALIDAD PROFESIONAL EN
TECNOLOGÍA, COMPUTACIÓN E INFORMÁTICA EDUCATIVA**

JULIACA – PERÚ

2025



UNIVERSIDAD ANDINA

NÉSTOR CÁCERES VELÁSQUEZ

ESCUELA DE POSGRADO

PROGRAMA DE SEGUNDA ESPECIALIDAD PROFESIONAL

TRABAJO ACADÉMICO

**PROTEGIENDO NUESTRA INFORMACIÓN EN LA ERA DIGITAL EN
ESTUDIANTES DEL CUARTO GRADO DE LA INSTITUCIÓN
EDUCATIVA SAN LUIS GONZAGA ICA 2023**

PRESENTADO POR:

EDDY ROJAS CHANCO

**PARA OPTAR EL TÍTULO DE SEGUNDA ESPECIALIDAD PROFESIONAL EN
TECNOLOGÍA, COMPUTACIÓN E INFORMÁTICA EDUCATIVA**

APROBADO POR:

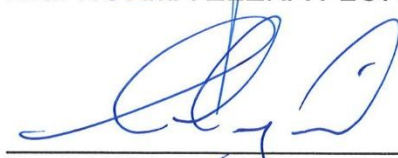
PRESIDENTE

:


Dra. NORMA ELENA FLORES VIZA

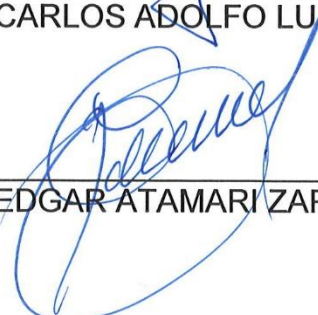
PRIMER MIEMBRO

:


Dr. CARLOS ADOLFO LUJAN URVIOLA

SEGUNDO MIEMBRO

:


Dr. EDGAR ATAMARI ZAPANA

LÍNEA DE INVESTIGACIÓN

:

GESTIÓN DE LA EDUCACIÓN - SEG22



TESIS UANCV

UNIVERSIDAD ANDINA

"NÉSTOR CÁCERES VELÁSQUEZ"

ESCUELA DE POSGRADO



VICERRECTORADO DE
INVESTIGACIÓN

"OFICINA DE INVESTIGACIÓN"



RESOLUCIÓN DIRECTORAL N° 157 - 2025-SEP-EPG/UANCV

Juliaca, 18 de diciembre del 2025

VISTO:

El Expediente N° 2025-C-9014, presentado por el (la) Egresado (a), **ROJAS CHANCO EDDY**, con DNI N° 21527546, con matrícula N° 21133F015, de la **SEGUNDA ESPECIALIDAD PROFESIONAL EN TECNOLOGÍA, COMPUTACIÓN E INFORMÁTICA EDUCATIVA**, de la **Escuela de Posgrado** de la Universidad Andina "Néstor Cáceres Velásquez" de la sede central Juliaca.

CONSIDERANDO:

Que, el egresado (a) **ROJAS CHANCO EDDY**, del Programa de **SEGUNDA ESPECIALIDAD PROFESIONAL EN TECNOLOGÍA, COMPUTACIÓN E INFORMÁTICA EDUCATIVA**, de la localidad Ica, de la **Escuela de Posgrado** de la Universidad Andina "Néstor Cáceres Velásquez" de Juliaca; Solicita sorteo de **Jurados y fecha para la Sustentación de Trabajo Académico**; habiendo cumplido con los requisitos para optar el Título de Segunda Especialidad Profesional;

Que, el inciso b) del Artículo N° 5 del Reglamento Específico de Titulación del Programa de Segunda Especialidad Profesional, establece la modalidad de Examen de Suficiencia y Sustentación de Trabajo Académico para optar el Título;

Que, los Artículos N° 12 al N° 21 del Reglamento Específico de Titulación del Programa de Segunda Especialidad Profesional, establecen los procedimientos para el referido Examen de Suficiencia y **Sustentación de Trabajo Académico**; y

En uso de las atribuciones conferidas a la Dirección en el inciso "J" del artículo 17 del Reglamento General de la Escuela de Posgrado, y el Art. 64 del Estatuto Universitario;

SE RESUELVE:

PRIMERO.- NOMBRAR a los **MIEMBROS DE JURADOS** que calificarán la Sustentación de Trabajo Académico del egresado (a): **ROJAS CHANCO EDDY**, con DNI N° 21527546, con matrícula N° 21133F015, del Programa de **SEGUNDA ESPECIALIDAD PROFESIONAL EN TECNOLOGÍA, COMPUTACIÓN E INFORMÁTICA EDUCATIVA**, de la localidad Ica, de la Escuela de Posgrado de la Universidad Andina "Néstor Cáceres Velásquez" de Juliaca; como se detalla en el Artículo Segundo de la presente Resolución, siendo los Jurados los siguientes Docentes:

Presidente	:	Dra. NORMA ELENA FLORES VIZA
Primer Miembro	:	Dr. CARLOS ADOLFO LUJAN URVIOLA
Segundo Miembro	:	Dr. EDGAR ATAMARI ZAPANA

SEGUNDO. - DETERMINAR que **LA SUSTENTACION DE TRABAJO ACADÉMICO** se llevará de acuerdo al siguiente detalle:

Fecha	:	Lunes, 22 de diciembre del 2025
Hora	:	09:00 a.m.
Lugar	:	Aula N° 207 – CC3 SEGUNDO PISO - UANCV

TERCERO. - AUTORIZAR la difusión de la presente Resolución a la Coordinación General del Programa de Segunda Especialidad Profesional e interesados.

Regístrese, comuníquese y archívese.



UNIVERSIDAD ANDINA NÉSTOR CÁCERES VELÁSQUEZ
ESCUELA DE POSGRADO

Dr. Javier Romulo Quispe Zapana
DIRECTOR (e)

Cc./Archiv.EPG (01)
Interesado (01)
Cargo (01)
JRQP(e)/aqj



PROTEGIENDO NUESTRA INFORMACIÓN EN EL ENTORNO DIGITAL EN ESTUDIANTES DEL CUARTO GRADO DE LA INSTITUCIÓN EDUCATIVA SAN LUIS GONZAGA ICA 2023

INFORME DE ORIGINALIDAD

23%

INDICE DE SIMILITUD

21%

FUENTES DE INTERNET

6%

PUBLICACIONES

9%

TRABAJOS DEL
ESTUDIANTE

FUENTES PRIMARIAS

1

www.coursehero.com

Fuente de Internet

4%

2

www.dykinson.com

Fuente de Internet

2%

3

Submitted to Universidad de Nebrija

Trabajo del estudiante

1%

4

Submitted to Universidad Internacional de la Rioja

Trabajo del estudiante

1%

5

Caballero Carlo, Nélida. "Nivel de autovaloración de hábitos de lectura en los alumnos de Educación Básica Alternativa 51029 "Sagrado Corazón de Jesús" provincia de Paucartambo, Cusco, 2023", Universidad Nacional del Altiplano de Puno (Peru)

Publicación

1%



Metadatos Complementarios

TRABAJO ACADÉMICO	
PROTEGIENDO NUESTRA INFORMACIÓN EN LA ERA DIGITAL EN ESTUDIANTES DEL CUARTO GRADO DE LA INSTITUCIÓN EDUCATIVA SAN LUIS GONZAGA ICA 2023	
Datos de autor	
Nombres y apellidos	EDDY ROJAS CHANCO
Tipo de documento de identidad	DNI
Número de documento de identidad	21527546
URL de ORCID	https://orcid.org/0009-0001-6683-3115
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	NORMA ELENA FLORES VIZA
Tipo de documento	DNI
Número de documento de identidad	29258552
URL de ORCID	https://orcid.org/0000-0003-3256-5391
Miembro del jurado 1	
Nombres y apellidos	CARLOS ADOLFO LUJAN URVIOLA
Tipo de documento	DNI
Número de documento de identidad	01213364
URL de ORCID	https://orcid.org/0000-0001-5596-3435
Miembro del jurado 2	
Nombres y apellidos	EDGAR ATAMARI ZAPANA
Tipo de documento	DNI
Número de documento de identidad	02264920
URL de ORCID	https://orcid.org/0000-0002-8064-4767



Datos de investigación	
Línea de investigación	GESTIÓN DE LA EDUCACIÓN - SEG22
Grupo de investigación	No aplica.
Agencia de financiamiento	Sin financiamiento
Ubicación geográfica de la investigación	País: Perú Departamento: Ica Provincia: Ica Distrito: Ica Coordenadas: Latitud: -12.5497331 Longitud: -74.548718 https://maps.app.goo.gl/89nrSNxbNset4wmQ7 
Año o rango de años en que se realizó la investigación	Diciembre 2024 – Diciembre 2025
URL de disciplinas OCDE	Ciencias de la educación https://purl.org/pe-repo/ocde/ford#5.03.00 Educación general (incluye capacitación, pedagogía) https://purl.org/pe-repo/ocde/ford#5.03.01



UNIVERSIDAD ANDINA NESTOR CÁCERES VELÁSQUEZ
ESCUELA DE POSGRADO

Dr. Jesús Mamari Mamani
DIRECTOR DE INVESTIGACIÓN - EPG



DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo EDDY ROJAS CHANCO, identificado con DNI

Nro. 21527546 en mi condición de egresado de:

☐ Escuela Profesional

☒ Programa de Segunda Especialidad,

☐ Programa de Maestría o Doctorado

S.E.P. EN TECNOLOGÍA, COMPUTACIÓN E INFORMÁTICA

informo que he elaborado el/la ☐ Tesis o ☐ Trabajo de Investigación, ☒ Trabajo Académico denominada:

PROTEGIENDO NUESTRA INFORMACIÓN EN LA ERA DIGITAL EN ESTUDIANTES DEL CUARTO GRADO DE LA INSTITUCIÓN EDUCATIVA SAN LUIS GONZAGA ICA 2023

Es un tema original.

Declaro que el presente trabajo de tesis es elaborado por mi persona y **no existe plagio/copia** de ninguna naturaleza, en especial de otro documento de investigación (tesis, revista, texto, congreso, o similar) presentado por persona natural o jurídica alguna ante instituciones académicas, profesionales, de investigación o similares, en el país o en el extranjero.

Dejo constancia que las citas de otros autores han sido debidamente identificadas en el trabajo de investigación, por lo que no asumiré como tuyas las opiniones vertidas por terceros, ya sea de fuentes encontradas en medios escritos, digitales o Internet.

Asimismo, ratifico que soy plenamente consciente de todo el contenido de la tesis y asumo la responsabilidad de cualquier error u omisión en el documento, así como de las connotaciones éticas y legales involucradas.

El incumplimiento de lo declarado da lugar a responsabilidad del declarante, en consecuencia; a través del presente documento asumo frente a terceros, la Universidad Andina Néstor Cáceres Velásquez y/o la Administración Pública toda responsabilidad que pueda derivarse por el trabajo final presentado. Lo señalado incluye responsabilidad pecuniaria incluido el pago de multas u otros por los daños y perjuicios que se ocasionen.

Juliaca 29 de DICIEMBRE del 2025

FIRMA (obligatoria)



Huella



DEDICATORIA

A aquellos cuyos conocimientos,
apoyo y aliento han sido la luz
que ha guiado mi camino



AGRADECIMIENTO

Mi más sincero agradecimiento a todas aquellas personas que han sido parte fundamental en la realización de este trabajo académico.



ÍNDICE GENERAL

DEDICATORIA.....	iii
AGRADECIMIENTO.....	iv
ÍNDICE GENERAL	v
ÍNDICES DE TABLAS	vii
ÍNDICES DE GRÁFICOS	viii
RESUMEN	ix
ABSTRACT	x
INTRODUCCIÓN	xi

CAPÍTULO I

ASPECTOS GENERALES DEL TRABAJO ACADÉMICO

1.1 Título.....	1
1.2 Descripción del problema.....	1
1.3 Justificación.....	2

CAPÍTULO II

OBJETIVOS

2.1. Objetivo general	4
2.1. Objetivos específicos	4

CAPÍTULO III

FUNDAMENTACIÓN TEÓRICA

3.1. Protegiendo información.....	5
3.1.1. Era digital	6
3.1.2. Conciencia sobre seguridad	7
3.1.3. Educación digital.....	8
3.2 Marco referencial.....	9



3.3. Marco Conceptual	26
-----------------------------	----

CAPÍTULO IV

PLANIFICACIÓN, EJECUCIÓN Y RESULTADOS PEDAGÓGICAS

4.1 METODOLOGÍA.....	30
4.1.1. Métodos aplicados a la investigación.....	30
4.1.2. Diseño de la investigación	30
4.1.3 Población	30
4.1.4 Muestreo	30
4.1.5 Técnicas instrumentos y fuentes	31
4.1.6 Técnicas	32
4.2 RESULTADOS	32
CONCLUSIONES.....	36
RECOMENDACIONES	38
REFERENCIAS.....	40
ANEXOS	43



ÍNDICES DE TABLAS

Tabla 1	29
Tabla 2	31
Tabla 3	33
Tabla 4	34



ÍNDICES DE GRÁFICOS

Figura 1	31
Figura 2	33
Figura 3	35



RESUMEN

En el estudio Protegiendo nuestra información en la era digital los estudiantes del cuarto, se abordó lo necesario de concienciar y educar en jóvenes educandos de la importancia de proteger su información personal en el mundo digital. la era digital, caracterizada por la interconexión global y la omnipresencia de dispositivos tecnológicos, plantea desafíos únicos en cuanto a la privacidad y la seguridad en información, el avance en el estudio está centrada sobre cómo desarrollar de estrategias educativas innovadoras para dotar a educandos de las bases como herramientas que acompañen el conocimientos necesario si proteger información digitales, se promovió la conciencia digital y se enseñaron buenas prácticas en el uso de la tecnología, con el objetivo empoderador para la toma en decisiones informáticas y seguras en línea la colaboración entre docentes, investigadores y padres de familia resultó fundamental las construcciones de culturas de seguridad digital en la comunidad educativa la educación en materia de proteger la información, se erigió como pilar con fundamentos en integra formación del estudiantado, con preparación que solucionen inconvenientes de la era digital con confianza y resiliencia, el estudio destacó la importancia de la educación como protección en materia de precisar datos y seguridad informática en la formación integral de los estudiantes al fomentar la conciencia digital desarrollando capacidades digitales, se contribuye a la construcción de una sociedad digitalmente segura y responsable, donde los jóvenes pueden desenvolverse en confianza y su responsabilidad en aplicaciones digitales

Palabras clave: Protegiendo, información, digital.



ABSTRACT

In the study Protecting our information in the digital age, the students of the fourth year addressed the need to raise awareness and educate young students of the importance of protecting their personal information in the digital world. The digital era, characterized by global interconnection and the omnipresence of technological devices, poses unique challenges in terms of privacy and information security. The progress in the study is focused on how to develop innovative educational strategies to provide learners with the bases as tools that accompany the necessary knowledge to protect digital information, digital awareness was promoted and good practices in the use of technology were taught, with the empowering objective for making computer and secure decisions online collaboration between teachers, researchers and parents, the construction of digital security cultures in the educational community was fundamental, education in matters of protecting information was established as a pillar based on comprehensive student training, with preparation to solve problems of the digital era with confidence and resilience, the study highlighted the importance of education as protection in terms of specifying data and computer security in the comprehensive training of students by promoting digital awareness by developing digital capabilities, contributing to the construction of a digitally safe and responsible society, where young people can develop confidence and responsibility in digital applications

Keywords: Protecting, information, digital.



INTRODUCCIÓN

El trabajo académico titulado "Protegiendo Nuestra Información en la Era Digital en Estudiantes del Cuarto Grado de la Institución Educativa San Luis Gonzaga, Ica" aborda la problemática actual de la seguridad digital, enfocándose en los desafíos que enfrentan los estudiantes de cuarto grado en la protección de su información personal. En un contexto donde la interconexión digital es omnipresente, este estudio se justifica por la necesidad de fomentar una cultura de conciencia sobre seguridad digital y desarrollar habilidades para proteger datos personales. La investigación se estructura en cuatro capítulos: el Capítulo I presenta los aspectos generales del trabajo académico, incluyendo la descripción del problema y su justificación; el Capítulo II detalla los objetivos, tanto generales como específicos, que buscan educar a los estudiantes sobre los riesgos en línea y capacitarlos en el uso de herramientas de protección; el Capítulo III ofrece una fundamentación teórica sobre la seguridad digital y la importancia de la educación en este ámbito; y el Capítulo IV describe la metodología empleada, que incluye un enfoque descriptivo y técnicas de recolección de datos a través de exámenes y registros. Los resultados indican un aumento significativo en la conciencia sobre los riesgos digitales entre los estudiantes, así como una mejora en sus prácticas de protección de datos. Las conclusiones destacan que la implementación de estrategias educativas ha sido efectiva para preparar a los estudiantes frente a las amenazas digitales, promoviendo una utilización responsable y ética de la tecnología. Este trabajo contribuye a establecer un marco para futuras investigaciones y prácticas educativas en el ámbito de la seguridad digital.



CAPÍTULO I

ASPECTOS GENERALES DEL TRABAJO ACADÉMICO

1.1 Título

Protegiendo Nuestra Información En La Era Digital En Estudiantes Del Cuarto Grado De La Institución Educativa San Luis Gonzaga Ica

1.2 Descripción del problema

En el contexto actual de la era digital, los estudiantes de cuarto grado de la Institución Educativa San Luis Gonzaga en Ica, Los estudiantes de cuarto grado enfrentan desafíos significativos en cuanto a la protección de su información personal en entornos virtuales, ya que la creciente interconexión digital y el uso generalizado de dispositivos tecnológicos los exponen a riesgos cibernéticos cada vez más complejos la falta de conciencia sobre la importancia de proteger la información en línea y la escasez de conocimientos sobre prácticas seguras en el uso de la tecnología plantean un problema fundamental en su formación. la exposición a amenazas como el robo de identidad, el acoso cibernético y la divulgación no autorizada de datos personales se ha vuelto una preocupación creciente en un entorno digital donde la privacidad y la seguridad son vulnerables, la necesidad de educar a estos estudiantes sobre la protección de su información en la era digital se vuelve imperativa para garantizar su seguridad y bienestar en línea, la falta de conocimientos sobre cómo gestionar y proteger



sus datos en entornos digitales puede exponerlos a consecuencias negativas que afecten su desarrollo personal, académico y social. la implementación de estrategias educativas innovadoras y la promoción de una cultura de seguridad cibernética en la comunidad educativa se presentan como medidas fundamentales para empoderar a estos jóvenes y prepararlos para enfrentar los desafíos de la era digital con confianza y responsabilidad, la educación en materia de protección de datos y seguridad informática debe ser considerada como un pilar fundamental en la formación integral de los estudiantes, ya que les permitirá desarrollar las habilidades y competencias necesarias para navegar de manera segura y responsable en el mundo digital al abordar de manera proactiva y efectiva la falta de conciencia y las prácticas inseguras en el manejo de la información digital, se puede garantizar que estos estudiantes estén mejor preparados para enfrentar los desafíos de la era digital y desarrollar una cultura de seguridad cibernética que los acompañe a lo largo de su vida.

1.3 Justificación

La justificación para el estudio "Protegiendo nuestra información en la era digital en estudiantes del cuarto grado de la Institución Educativa San Luis Gonzaga, Ica 2023" La importancia de abordar los desafíos que plantea la era digital en cuanto a la privacidad y seguridad de la información de los jóvenes estudiantes es evidente la interconexión global y la presencia generalizada de dispositivos tecnológicos han modificado nuestra interacción con la información, destacando la necesidad crucial de proteger los datos personales en el entorno digital, la justificación de este estudio se fundamenta en la necesidad de educar a los estudiantes de cuarto grado sobre la protección de su información en entornos digitales, la promoción de la conciencia digital y la adopción de buenas



prácticas en el uso de la tecnología son esenciales para capacitar a estos jóvenes y prepararlos para afrontar los retos de la era digital con confianza y responsabilidad, la educación en protección de datos y seguridad informática se erige como un pilar fundamental en la formación integral de los estudiantes, permitiéndoles adquirir las habilidades necesarias para navegar de forma segura y responsable en el mundo digital, al fomentar la conciencia digital y el desarrollo de competencias digitales, se contribuye a la creación de una sociedad digital segura y responsable, donde los jóvenes pueden desenvolverse con confianza y responsabilidad la justificación de este estudio también se basa en la necesidad de abordar la falta de conciencia y las prácticas inseguras en el manejo de la información digital por parte de los estudiantes de cuarto grado. la implementación de estrategias educativas innovadoras y la promoción de una cultura de seguridad cibernética en la comunidad educativa son medidas esenciales para garantizar la seguridad y el bienestar de estos jóvenes en línea



CAPÍTULO II

OBJETIVOS

2.1. Objetivo general

OG. Proteger nuestra información en la era digital en estudiantes del cuarto grado de la Institución Educativa San Luis Gonzaga ICA 2023

2.1. Objetivos específicos

OE1. Fomentar la Conciencia sobre Seguridad en la era digital en estudiantes y Educar a los estudiantes sobre los riesgos y amenazas en línea, promoviendo prácticas seguras en el manejo de información personal y la navegación en internet.

OE2. Desarrollar habilidades protegiendo nuestra información de Datos: Capacitar a los estudiantes en el uso de herramientas y estrategias para proteger sus datos personales y evitar el robo de información en entornos digitales.



CAPÍTULO III

FUNDAMENTACIÓN TEÓRICA

3.1. Protegiendo información.

Se refiere a la acción de salvaguardar y garantizar la seguridad de datos sensibles, evitando su filtración, robo, pérdida o uso indebido en el entorno digital, esta tarea implica la aplicación de medidas de seguridad informática, como el uso de contraseñas seguras, la encriptación de datos, la instalación de software antivirus y la adopción de prácticas responsables en el manejo de dispositivos y plataformas en línea el propósito de "protegiendo información" radica en resguardar los datos, manteniendo la confianza y la integridad de las personas y organizaciones que participan en el ámbito digital.

Lazo y Correa (2024). Presentan Un estudio sobre la importancia de proteger la información de los pacientes destaca que la creciente digitalización de los sistemas de salud ha aumentado la exposición de los datos personales de los pacientes a riesgos cibernéticos. Esto ha generado la necesidad de establecer estándares de seguridad adecuados para proteger la confidencialidad, integridad y disponibilidad de la información de salud. El artículo se basa en una revisión exhaustiva de la literatura y en entrevistas con expertos en ciberseguridad y sistemas informáticos, identificando estándares clave para la gestión de la seguridad de la información en el sector sanitario,



como el marco de referencia de la NIST para la gestión de la ciberseguridad y el estándar HIPAA para la protección de la privacidad y seguridad de los datos de salud. Los autores también presentan una metodología detallada para la implementación de estos estándares en los sistemas informáticos sanitarios, que incluye la identificación de riesgos, la evaluación de la vulnerabilidad de los sistemas, la implementación de controles de seguridad efectivos y la monitorización y evaluación continua de los sistemas para garantizar su seguridad y confiabilidad

3.1.1. Era digital

La "era digital" se refiere al período histórico actual, marcado por la transformación tecnológica y la generalización del uso de dispositivos y plataformas digitales, económicas y culturales, la era digital se caracteriza por la interconexión global y la disponibilidad de información y comunicación en tiempo real, gracias a la expansión de internet y la proliferación de dispositivos móviles y computadoras; esta era ha transformado los bienes y servicios, así como la forma en que se interactúa en las relaciones sociales y laborales; la era digital también ha presentado nuevos desafíos y riesgos en términos de seguridad, privacidad y ética, las estrategias y políticas que garanticen el uso responsable y seguro de las tecnologías digitales.

Caicedo Gonzalez, Contreras Murcia y Pino Diaz (2024). Destaca la importancia de la gestión del talento humano en un contexto digitalizado, identificando los desafíos y oportunidades que esto conlleva y ofreciendo orientación práctica para abordarlos de manera efectiva.

3.1.2. Conciencia sobre seguridad

El grado de atención y comprensión que una persona o grupo posee sobre los riesgos y amenazas relacionados con la seguridad, así como sobre las medidas y prácticas necesarias para prevenirlos y mitigarlos, desarrollar esta conciencia implica identificar y evaluar los riesgos, y adoptar comportamientos y hábitos seguros en diferentes contextos y situaciones, la conciencia sobre seguridad es especialmente relevante en el entorno digital, donde la exposición a riesgos y amenazas cibernéticas es cada vez mayor, y donde la protección de la privacidad requiere la adopción de medidas y prácticas de seguridad informática adecuadas, fomentar esta conciencia es fundamental para empoderar a los individuos y dotarlos de las herramientas necesarias para navegar de manera segura en el mundo digital, desarrollar una cultura de conciencia sobre seguridad implica que la prevención y gestión de riesgos sean una responsabilidad compartida entre individuos, organizaciones y comunidades todos los actores deben asumir un papel activo en la promoción de prácticas seguras y en la creación de entornos más seguros, tanto en el mundo físico como en el digital

Díaz Sandoval y Rojas Perleche (2023). En el artículo se resalta la importancia y la necesidad de implementar medidas de seguridad efectivas para resguardar los datos personales y sensibles. Los autores llevan a cabo un análisis exhaustivo de riesgos y vulnerabilidades en el sistema de información de la oficina, subrayando la relevancia de promover la conciencia sobre la seguridad de la información entre los empleados y la capacitación en las mejores prácticas de seguridad. Asimismo, se hace hincapié en la importancia de realizar auditorías periódicas para asegurar el cumplimiento de las normas de seguridad,



también enfatiza la importancia de llevar a cabo auditorías regulares para garantizar el cumplimiento de las normas de seguridad. Se incluye un análisis detallado de los riesgos y vulnerabilidades de la información en la oficina de informática y telecomunicaciones de la Municipalidad Distrital de San Juan Bautista, junto con recomendaciones para fortalecer la seguridad de la información en organizaciones públicas. Se destaca la relevancia de promover la conciencia y la capacitación en seguridad de la información, así como la necesidad de contar con políticas y procedimientos de seguridad claros y actualizados.

3.1.3. Educación digital

El aprendizaje que se apoya en tecnologías digitales y recursos en línea como herramientas y canales de comunicación y colaboración es fundamental en la educación actual el uso de dispositivos y plataformas digitales permite acceder, crear, gestionar y compartir información y conocimientos, así como desarrollar habilidades y competencias digitales necesarias para el presente y el futuro. la educación digital implica también la creación e implementación de estrategias y modelos educativos que aprovechen las oportunidades y beneficios de las tecnologías digitales, como la flexibilidad, la interactividad y la personalización del aprendizaje, para llevar a cabo una educación digital efectiva, es necesario adoptar enfoques y prácticas pedagógicas innovadoras que fomenten el pensamiento crítico, la creatividad, la colaboración y la participación activa de los estudiantes, se debe garantizar la equidad, la accesibilidad y la calidad de la educación en un entorno cada vez más digitalizado.

Escuderos, Restrepo y Rambal-Rivaldo (2024). En su artículo " publicado en la Revista de Investigación Educativa, El estudio analiza el impacto que tienen los entornos educativos digitales y presenciales en el compromiso académico de los estudiantes durante y después del confinamiento los investigadores llevan a cabo un análisis comparativo entre los perfiles de los estudiantes en estos dos contextos educativos, y los resultados muestran que el entorno digital puede ser un facilitador para lo académico, especialmente en situaciones de confinamiento, los autores identifican diferentes perfiles de compromiso académico en función del contexto educativo y el momento específico, destacan la necesidad de desarrollar estrategias didácticas específicas para cada contexto y perfil identificado para comprender mejor el impacto que tienen los entornos educativos en el compromiso académico de los estudiantes, sus hallazgos pueden ser útiles para la toma de decisiones en la planificación y diseño de estrategias educativas adaptadas a los contextos digitales y presenciales

3.2 Marco referencial

3.2.1 Riesgos en línea

Los "peligros digitales" se refieren a las amenazas y desafíos que enfrentan los usuarios de internet y las tecnologías digitales en relación con su seguridad, privacidad y bienestar estos peligros pueden variar en gravedad y naturaleza, y pueden incluir el acoso cibernético, la vigilancia, la divulgación de información personal y confidencial, el ciberterrorismo, la pornografía infantil y la exposición a contenido inapropiado o dañino los peligros digitales pueden afectar a individuos, organizaciones y comunidades, y pueden tener consecuencias negativas en términos de reputación, confianza, productividad y bienestar la gestión de estos peligros requiere la adopción de medidas y prácticas de



seguridad informática adecuadas, así como la promoción de una cultura de conciencia y responsabilidad en el uso de las tecnologías digitales la educación y la capacitación en materia de seguridad digital son fundamentales para prevenir y mitigar los peligros digitales, y para garantizar la protección de los derechos y la seguridad de los usuarios de internet y las tecnologías digitales es esencial fomentar una cultura de seguridad digital que incluya la conciencia sobre los riesgos, la adopción de prácticas seguras y la promoción de una responsabilidad compartida en la gestión de los peligros digitales.

Chambé-Morales y Sarmiento-Martínez (2024). El estudio presenta un análisis de los riesgos cibernéticos a los que se enfrenta la empresa familiar "colegio diego rivera" de tuxtla gutiérrez, chiapas. Su objetivo es identificar y evaluar los riesgos cibernéticos a los que está expuesta la organización, y proponer medidas efectivas para mitigarlos y controlarlos, los autores utilizan una metodología de evaluación de riesgos cibernéticos que incluye la identificación y clasificación de activos críticos, la evaluación de amenazas y vulnerabilidades, y la estimación de impactos y probabilidades los resultados del estudio revelan que la empresa enfrenta riesgos cibernéticos significativos, especialmente en relación con la protección de datos personales y la continuidad operativa en base a estos hallazgos, los autores proponen una serie de medidas de mitigación y control, como la implementación de políticas de seguridad, la capacitación del personal, la adopción de tecnologías de seguridad y la realización de auditorías periódicas destacan la importancia de fomentar una cultura de seguridad en toda la organización y la necesidad de involucrar a todos los miembros en la gestión de riesgos cibernéticos, este estudio representa una contribución valiosa al campo de la gestión de riesgos cibernéticos en empresas familiares proporciona



una metodología sólida y recomendaciones prácticas para abordar los desafíos de seguridad a los que se enfrentan este tipo de organizaciones en el entorno digital actual.

3.1.2 Amenazas en línea.

Las acciones o comportamientos intencionales y maliciosos que buscan dañar, interrumpir o comprometer la privacidad y los datos en línea representan amenazas cibernéticas estas amenazas pueden variar en gravedad y naturaleza e incluir el malware, el phishing, el ransomware, el spyware, los ataques de denegación de servicio (ddos), los ataques de día cero, el robo de credenciales y la suplantación de identidad estas amenazas pueden originarse tanto de individuos, organizaciones o estados, y tener como objetivo a personas, entidades u infraestructuras críticas, la gestión de estas amenazas en línea requiere la implementación de medidas y prácticas de seguridad informática adecuadas, como el uso de software antivirus, firewalls, encriptación, autenticación de dos factores y copias de seguridad es fundamental promover una cultura de conciencia y responsabilidad en el uso de las tecnologías digitales para hacer frente a estas amenazas la educación y la capacitación en seguridad digital son esenciales para prevenir y mitigar las amenazas en línea, protegiendo así a los usuarios de internet y las tecnologías digitales.

Barahona Paredes (2023). Examina detalladamente las dificultades y El estudio analiza los riesgos a los que se enfrenta el Sistema Académico SAI de una institución universitaria. el autor identifica una serie de problemas críticos y amenazas que impactan la seguridad y el funcionamiento eficiente de este sistema. barahona paredes resalta la importancia de abordar proactivamente estos problemas para garantizar la integridad, confidencialidad y disponibilidad



de la información académica, el autor sugiere la implementación de medidas preventivas y correctivas, como la actualización regular del software, la concienciación sobre seguridad informática entre los usuarios y el establecimiento de políticas de seguridad sólidas, este estudio proporciona una visión detallada de los desafíos en la gestión de la seguridad del sistema académico sai y ofrece recomendaciones prácticas para fortalecer la protección de los datos y la infraestructura informática en entornos universitarios las conclusiones y sugerencias de Barahona paredes son valiosas para mejorar la seguridad y eficacia de los sistemas académicos en el ámbito universitario sus hallazgos y propuestas pueden servir como guía para que otras instituciones educativas implementen medidas efectivas para salvaguardar sus sistemas de información críticos

3.1.3 Promoviendo prácticas de seguridad.

El artículo de Moya, J. G. (2023) titulado La relevancia de la seguridad informática en la educación digital: desafíos y propuestas, publicado en la revista Recimundo, resalta la creciente importancia de la seguridad informática en el entorno educativo digital el autor enfatiza que en la actualidad, la educación digital se ha vuelto fundamental en la vida de los estudiantes, lo que subraya la necesidad imperante de garantizar la seguridad de los datos y la privacidad de los usuarios, el texto aborda los desafíos que enfrentan los sistemas educativos digitales en términos de seguridad, como el ciberacoso, el robo de identidad y la divulgación de información persona, se proponen soluciones para abordar estas problemáticas, como la implementación de políticas de seguridad informática en los centros educativos y la formación tanto de docentes como de estudiantes en temas de seguridad digital, se destaca la importancia de la colaboración entre



los diversos actores involucrados en la educación digital, como las instituciones educativas, los entes gubernamentales y las empresas tecnológicas, para asegurar la protección de los usuarios este artículo representa una valiosa contribución al campo de la seguridad informática en la educación digital al ofrecer una visión clara de los desafíos y soluciones en este ámbito la investigación y el análisis realizados proporcionan una base sólida para la toma de decisiones informadas en materia de seguridad informática en la educación digital, resaltando la importancia de la colaboración y la formación en este ámbito

3.1.4 Información personal.

Los datos y Los datos personales se refieren a detalles que identifican de manera única a un individuo, como su nombre, dirección, número de teléfono, correo electrónico, número de identificación, información financiera, entre otros. Esta información es altamente sensible y confidencial, y su uso, divulgación o protección está regulada por leyes y normativas específicas en diferentes países y contextos la protección de la información personal es esencial para garantizar la privacidad, la integridad y la seguridad de las personas, especialmente en el mundo digital, donde la recopilación, el almacenamiento y el procesamiento de datos personales se han vuelto cada vez más comunes y sofisticados. En este entorno, es fundamental fomentar la conciencia y la responsabilidad en el manejo de esta información a través de la educación y la capacitación en materia de protección de datos personales. Esto permitirá prevenir posibles riesgos y amenazas en línea relacionada con el uso indebido o la divulgación no autorizada de datos personales

Garitaonandia, karrera-xuarros, jiménez-iglesias y larrañaga (2020)
menores conectados y riesgos online: contenidos inadecuados, uso inapropiado



de la información y excesiva exposición a internet" aborda la problemática de la seguridad en línea en la infancia y adolescencia los autores examinan los peligros a los que se enfrentan los menores que utilizan internet, como el acceso a contenidos inapropiados, la divulgación inadecuada de información personal y el uso excesivo de la red, se presentan diversas estrategias y herramientas para prevenir y mitigar estos riesgos, tales como la educación y sensibilización de los menores y sus familias, la configuración adecuada de dispositivos y redes, y la utilización de software y aplicaciones de control parental, el trabajo destaca la importancia de la colaboración entre diversas instituciones y actores involucrados en la protección de los menores en línea, como familias, escuelas, entidades gubernamentales y empresas tecnológicas. garitaonandia, karrera-xuarros, jiménez-iglesias y larrañaga (2020) ofrecen una visión actualizada y completa de los riesgos en línea a los que se enfrentan los menores, así como de las estrategias y herramientas disponibles para protegerlos su contribución resulta de gran interés para padres, educadores, profesionales de la seguridad en línea y responsables políticos.

3.1.5 Desarrollo de habilidades

El proceso de adquisición, mejora y refinamiento de conocimientos, destrezas y competencias que permiten a los individuos desempeñarse de manera efectiva y eficiente en diferentes contextos y situaciones, esto implica la identificación de las habilidades necesarias para alcanzar objetivos específicos, el diseño y la implementación de estrategias y actividades de aprendizaje, y la evaluación y el seguimiento del progreso y el desempeño el desarrollo de habilidades es fundamental para el crecimiento personal y profesional, y puede abarcar diferentes dominios y áreas, como las habilidades técnicas, las



habilidades sociales, las habilidades emocionales y las habilidades cognitivas en el entorno digital, el desarrollo de habilidades digitales es especialmente relevante, ya que permite a los usuarios aprovechar al máximo las posibilidades y ventajas de las tecnologías digitales, y garantizar su seguridad y protección en línea esto incluye habilidades como la navegación segura, la gestión de la información, la comunicación efectiva y la resolución de problemas en línea

Galardy y Silveira (2021). Publicado en la revista científica del Amazonas, los autores resaltan la importancia de la adquisición de habilidades tecnológicas en la educación primaria y su evolución histórica señalan que la incorporación de las tecnologías de la información y la comunicación (tic) en la educación primaria ha sido un proceso gradual y continuo, impulsado por el avance tecnológico y la necesidad de preparar a los estudiantes para un mundo cada vez más digitalizado, los autores revisan los diferentes hitos y etapas que han marcado la evolución de las habilidades infotecnológicas en la educación primaria, desde la introducción de las primeras herramientas tecnológicas en el aula hasta la actualidad, donde las tic son una herramienta fundamental en el proceso de enseñanza-aprendizaje también destacan la importancia de la formación de los docentes en el uso de las tic, ya que éstos desempeñan un papel clave en la adquisición de habilidades tecnológicas por parte de los estudiantes, en este sentido, abogan por la necesidad de incorporar la formación en tic en los planes de estudios de las facultades de educación y en los programas de formación continua de los docentes en definitiva, el artículo ofrece una visión amplia y actualizada de la evolución histórica de las habilidades infotecnológicas en la educación primaria, y subraya la importancia de la adquisición de estas habilidades en el proceso de enseñanza-aprendizaje

3.1.6 Protección de datos.

La protección de datos se refiere a las medidas y prácticas destinadas a garantizar la confidencialidad, integridad y disponibilidad de los datos y la información, especialmente en el entorno digital. esto implica la adopción de políticas y procedimientos de seguridad informática, como el uso de contraseñas seguras, la encriptación de datos, la realización de copias de seguridad y la restauración de información, la gestión adecuada de accesos y permisos, y la monitorización y el control de actividades sospechosas la protección de datos también conlleva el cumplimiento de las leyes y normativas específicas en materia de protección de datos, como el reglamento general de protección de datos (rgpd) de la unión europea, y la promoción de una cultura de conciencia y responsabilidad en el manejo de la información personal y sensible, la educación y la capacitación en protección de datos son fundamentales para fomentar la conciencia y la responsabilidad en el manejo de la información, y para prevenir posibles riesgos y amenazas en línea relacionados con el uso indebido o la divulgación no autorizada de datos

Calva Jiménez (2020) Aborda la temática de la protección de datos se enfoca en la protección de datos personales de niños y adolescentes en el entorno de internet, destacando los riesgos asociados y los mecanismos de protección disponibles se examina detalladamente la importancia de preservar la privacidad y seguridad de los datos de los jóvenes en el actual contexto digital, analizando los posibles riesgos que enfrentan en línea, como la exposición a contenidos inapropiados, el ciberacoso, la pérdida de privacidad y otros peligros asociados con el uso de internet, además, se exploran diversos mecanismos de protección, como la educación en seguridad digital, el uso de herramientas de



control parental, la configuración de la privacidad en redes sociales y la legislación vigente en protección de datos la investigación realizada resalta la importancia de concienciar a padres, educadores y jóvenes sobre la necesidad de proteger la información personal en línea y fomentar un uso seguro y responsable de la tecnología, se destaca la relevancia de implementar estrategias efectivas para mitigar los riesgos y garantizar la privacidad de los datos de los menores en el entorno digital, el estudio proporciona una visión integral y fundamentada sobre la protección de datos en la niñez y adolescencia en internet, ofreciendo recomendaciones prácticas y reflexiones importantes para promover un entorno digital seguro y protegido para los jóvenes

3.1.7 Uso de herramientas

La aplicación de instrumentos, recursos o aplicaciones específicas que facilitan la realización de tareas, la resolución de problemas o la consecución de objetivos en diversos contextos estas herramientas pueden ser de carácter físico, como herramientas manuales o maquinaria especializada, o de naturaleza digital, como software, aplicaciones en línea o plataformas tecnológicas el uso efectivo de herramientas implica la selección adecuada, el dominio de su funcionamiento y la aplicación eficaz de las mismas para optimizar procesos, mejorar la productividad y alcanzar resultados deseados de manera más eficiente en el ámbito educativo, el uso de herramientas tecnológicas puede potenciar el aprendizaje, la creatividad y la colaboración entre estudiantes y docentes, enriqueciendo así la experiencia educativa y fomentando el desarrollo de habilidades digitales la integración de estas herramientas en los procesos de enseñanza-aprendizaje permite a los estudiantes adquirir conocimientos y destrezas relevantes para desenvolverse en un mundo cada vez más digitalizado



Chuquitarco Lagla, LA (2024) La investigación de Chuquitarco Lagla sobre el uso de herramientas digitales en la cooperativa Ambato sede Latacunga, provincia de Cotopaxi, es una contribución valiosa al campo de la tecnología y la gestión empresarial, esta investigación proporciona una comprensión detallada de cómo las herramientas digitales pueden ser utilizadas para mejorar la eficiencia y eficacia en una cooperativa de crédito a través de una metodología rigurosa se examina el impacto de las herramientas digitales en la gestión de la cooperativa, incluyendo la automatización de procesos, la comunicación interna y externa, y la prestación de servicios financieros los hallazgos sugieren que el uso de herramientas digitales puede mejorar significativamente la eficiencia y eficacia de las operaciones de la cooperativa se destaca la importancia de la capacitación y el apoyo a los empleados en el uso de estas herramientas para garantizar una implementación exitosa. En general, la tesis de Chuquitarco Lagla es una importante contribución al campo de la tecnología y la gestión empresarial, y proporciona una base sólida para futuras investigaciones sobre el uso de herramientas digitales en cooperativas de crédito y otras organizaciones empresariales.

3.1.8 Estrategias de protección de datos.

A las acciones y medidas planificadas y sistemáticas que se implementan para garantizar la confidencialidad, integridad y disponibilidad de los datos y la información, especialmente en el entorno digital. estas estrategias pueden abarcar la adopción de políticas y procedimientos de seguridad informática, como el uso de contraseñas seguras, la encriptación de datos, la realización de copias de seguridad y su restauración, la gestión de accesos y permisos, así como la monitorización y el control de actividades sospechosas pueden



involucrar la formación y capacitación del personal en protección de datos, la implementación de sistemas de gestión de riesgos, y la evaluación y seguimiento del cumplimiento de normativas y leyes específicas en materia de protección de datos, son fundamentales para asegurar la seguridad y privacidad de la información personal y sensible, y para prevenir posibles riesgos y amenazas en línea la efectiva implementación de estas estrategias requiere la colaboración y el compromiso de todos los miembros de la organización, así como la actualización y adaptación continua de las medidas de seguridad en respuesta a las nuevas amenazas y desafíos en el entorno digital

Amador, MM (2024) En su artículo en un contexto de transformación digital", publicado en la revista Rhombus, ofrece una perspectiva relevante sobre la importancia de la protección de datos en un entorno de creciente transformación digital el artículo aborda la necesidad de garantizar la privacidad y seguridad de la información personal de los ciudadanos costarricenses en medio del acelerado proceso de digitalización que experimenta el país, el artículo proporciona un análisis exhaustivo de la situación actual de la protección de datos en costa rica, revisando el marco legal existente y las iniciativas gubernamentales en esta materia, también presenta recomendaciones para fortalecer la regulación y la aplicación de la ley, con el objetivo de garantizar un entorno digital seguro y respetuoso de los derechos de los ciudadanos, en definitiva, este trabajo publicado en Rhombus ofrece una perspectiva valiosa y oportuna sobre un tema de creciente relevancia en la era digital, contribuyendo a la discusión sobre la necesidad de proteger los datos personales y los derechos humanos en el contexto de la transformación digital que experimenta costa rica y otros países



de la región, la necesidad de abordar estos temas de manera integral y ética en la sociedad actual

3.1.9 Robo de información I

La acción ilegal de obtener, acceder o adquirir datos confidenciales, sensibles o privados de una persona, empresa u organización sin autorización este acto puede realizarse de diversas formas, como el acceso no autorizado a sistemas informáticos, el phishing, el malware, la interceptación de comunicaciones, entre otros métodos el robo de información puede tener graves consecuencias, como la violación de la privacidad, el robo de identidad, la pérdida de datos financieros, la exposición de secretos comerciales o industriales, y el daño a la reputación y la confianza de las personas u entidades afectadas, la prevención del robo de información requiere la implementación de medidas de seguridad informática robustas, como el uso de contraseñas seguras, la encriptación de datos, la autenticación de dos factores y la concienciación sobre prácticas seguras en línea, la educación y la sensibilización sobre los riesgos y las amenazas en línea son fundamentales para proteger la información y prevenir el robo de datos en el entorno digital es crucial que tanto individuos como organizaciones adopten un enfoque proactivo y se mantengan informados sobre las últimas tendencias y técnicas utilizadas por los ciberdelincuentes para robar información, con el fin de implementar las medidas de seguridad adecuadas y minimizar el riesgo de sufrir un incidente de robo de datos.

La tesis de Sánchez Acuña, WA (2024) El diseño de controles de seguridad informática para el sistema de información en la empresa proveedora de internet Telpronet de la ciudad de Ambato es una valiosa contribución al



ámbito de la seguridad informática y la gestión de sistemas de información. la tesis presenta un enfoque metodológico riguroso para el diseño de controles de seguridad informática en el contexto específico de una empresa proveedora de servicios de internet, con un estudio de caso centrado en Telpronet en la ciudad de Ambato. los aportes de la tesis abarcan la identificación de las vulnerabilidades y riesgos de seguridad más frecuentes en los sistemas de información de las empresas proveedoras de internet, así como la propuesta de controles de seguridad informática específicos para mitigar dichos riesgos., se resalta la importancia de la capacitación y la conciencia en seguridad informática entre los empleados de la empresa, junto con la necesidad de una gestión efectiva de los riesgos de seguridad informática en el contexto de las empresas proveedoras de internet, esta investigación ofrece una valiosa contribución al campo de la seguridad informática y la gestión de sistemas de información, siendo de utilidad para empresas proveedoras de internet y otras organizaciones que buscan fortalecer su seguridad informática y mejorar la gestión de riesgos en un entorno digital cada vez más complejo.

3.1.10 Entornos digitales.

Los entornos digitales hacen referencia a los espacios y ambientes virtuales en los que se llevan a cabo actividades y transacciones a través de dispositivos y tecnologías digitales estos entornos pueden ser de diversa índole, como redes sociales, plataformas de comercio electrónico, sitios web, aplicaciones móviles, entre otros ofrecen numerosas ventajas y oportunidades, como la comunicación y la colaboración en tiempo real, el acceso a información y conocimientos ilimitados, la personalización y la flexibilidad en el aprendizaje y el trabajo, entre otros aspectos positivos sin embargo, también conllevan riesgos



y desafíos, como el ciberacoso, el robo de información, la adicción a las tecnologías, la desinformación y la falta de privacidad y seguridad en línea. por tanto, es sencial promover el uso responsable y seguro de los entornos digitales, fomentar la alfabetización digital y la conciencia sobre los riesgos y amenazas en línea, y desarrollar habilidades y competencias digitales que capaciten a los usuarios para interactuar de manera efectiva y segura en estos entornos virtuales.

Huamán-Cuya, A., Moscoso-Paucarchuco, KM, Yupanqui-Villanueva, HR, Rojas-Hurtado, GF, & Zevallos-López, ZV (2024) en entornos pospandemia, específicamente en estudiantes universitarios, son de gran relevancia en el contexto actual de transformación digital acelerada el estudio examina detalladamente las competencias digitales de los estudiantes universitarios en un entorno pospandémico, resaltando la importancia de estas habilidades en un mundo cada vez más digitalizado los hallazgos revelan tanto las fortalezas como las áreas de mejora en las competencias digitales de los estudiantes, lo que proporciona información valiosa para el diseño de programas educativos que promuevan un desarrollo más completo de estas habilidades, el estudio enfatiza la necesidad de adaptar los enfoques educativos para integrar de manera efectiva las competencias digitales en el currículo universitario, preparando a los estudiantes para enfrentar los desafíos y aprovechar las oportunidades que ofrece el entorno digital actual se destaca la importancia de fomentar un aprendizaje continuo y una actualización constante de las competencias digitales para garantizar la empleabilidad y la adaptabilidad de los estudiantes en un mundo laboral en constante evolución asimismo, se subraya la relevancia de las competencias digitales en el contexto pospandemia y se ofrecen insights



significativos para la educación superior en la preparación de los estudiantes para un futuro digitalmente competente y exitoso.

3.1.11 Uso de tecnología y la ética

La interacción entre la aplicación de herramientas tecnológicas y el comportamiento ético en su utilización. Esto implica considerar no solo la eficacia y la conveniencia de la tecnología, sino también los principios morales y valores que guían su uso y sus implicaciones en la sociedad. La ética en el uso de la tecnología abarca aspectos como la privacidad, la transparencia, la equidad, la responsabilidad, la seguridad y el respeto a los derechos individuales y colectivos. Es fundamental que los usuarios y desarrolladores de tecnología consideren no solo el impacto positivo que puede tener su uso, sino también las posibles consecuencias negativas y los dilemas éticos que puedan surgir.

Promover un uso ético de la tecnología implica reflexionar sobre las implicaciones éticas de nuestras acciones digitales, tomar decisiones informadas y responsables, y contribuir a la construcción de un entorno tecnológico que respete los valores éticos fundamentales y promueva el bienestar de la sociedad en su conjunto.

Pino Ortega, Gómez Carmona y Moreno Contreras (2024) publicado en la ofrece una visión integral de los aspectos sociales, éticos y legales que rodean el desarrollo y uso de la tecnología en la sociedad los autores destacan la importancia de considerar estos aspectos en el diseño, implementación y evaluación de tecnologías emergentes, y subrayan la necesidad de una reflexión crítica sobre las consecuencias sociales y éticas de su uso, el artículo aborda la necesidad de establecer marcos legales claros y efectivos para garantizar la protección de los derechos humanos y la privacidad de los ciudadanos en el

contexto de la tecnología los autores también exploran los desafíos y oportunidades que presenta la tecnología en términos de equidad social, accesibilidad y participación ciudadana, y ofrecen recomendaciones prácticas para garantizar una integración responsable y sostenible de la tecnología en la sociedad el artículo proporciona una valiosa contribución al campo de los aspectos sociales, éticos y legales de la tecnología, y subraya la necesidad de una reflexión crítica y una acción responsable en el desarrollo y uso de la tecnología en la sociedad.

3.1.12 Dispositivos digitales

Son herramientas tecnológicas que procesan y almacenan información en formato digital, lo que permite a los usuarios interactuar y comunicarse en entornos digitales estos dispositivos pueden ser móviles, como teléfonos inteligentes y tabletas, o estacionarios, como computadoras y televisores inteligentes los dispositivos digitales ofrecen numerosas ventajas y oportunidades, como el acceso a información y conocimientos ilimitados, la comunicación y la colaboración en tiempo real, la personalización y la flexibilidad en el aprendizaje y el trabajo, entre otros aspectos positivos sin embargo, también presentan riesgos y desafíos, como la adicción a las tecnologías, la falta de privacidad y seguridad en línea, y el impacto en la salud y el bienestar de las personas, por lo tanto, es fundamental promover el uso responsable y seguro de los dispositivos digitales, fomentar la alfabetización digital y la conciencia sobre los riesgos y amenazas en línea, y desarrollar habilidades y competencias digitales que permitan a los usuarios interactuar de manera efectiva y segura con estos dispositivos es importante considerar los aspectos éticos y sociales del uso de los dispositivos digitales, como el impacto en la privacidad, la responsabilidad



y la equidad, y promover un uso ético y sostenible de estas herramientas tecnológicas.

Hanco Mescoco, Nueva Jersey y Palomino Salazar, VL (2024) presentan en su estudio "enseñanza a través de dispositivos digitales del cuarto grado de primaria Nuestra Señora del Rosario de Fátima–Chaclacayo 2022" una investigación sobre la implementación de dispositivos digitales en el proceso de enseñanza-aprendizaje en el cuarto grado de primaria de la institución nuestra señora del rosario de Fátima, ubicada en Chaclacayo, los autores describen el proceso metodológico seguido para la implementación de los dispositivos digitales, los recursos tecnológicos utilizados, y los resultados obtenidos en cuanto a la mejora en el rendimiento académico de los estudiantes, se presentan recomendaciones para la implementación de dispositivos digitales en el proceso de enseñanza-aprendizaje en otros contextos educativos; El estudio aporta evidencia sobre la efectividad de la implementación de dispositivos digitales en el proceso de enseñanza-aprendizaje en el nivel primario, y destaca la importancia de la capacitación y acompañamiento de los docentes en el uso de estas herramientas tecnológicas, los autores resaltan la necesidad de contar con recursos tecnológicos adecuados y conectividad estable para garantizar el éxito en la implementación de los dispositivos digitales en el proceso de enseñanza-aprendizaje, ofrece una valiosa contribución al campo de la integración de las tecnologías digitales en el proceso de enseñanza-aprendizaje, y destaca la importancia de la capacitación y acompañamiento de los docentes, así como la necesidad de contar con recursos tecnológicos adecuados y conectividad estable para garantizar el éxito en la implementación de los dispositivos digitales en el proceso de enseñanza-aprendizaje.

3.3. Marco Conceptual

3.3.1. Protegiendo.

Real Academia Española. (2024). hace referencia a una persona que recibe la protección de otra, ya sea como favorita o como ahijado apadrinado por otra persona esta palabra deriva del verbo "proteger" y se utiliza en el contexto de la relación entre dos personas en el ámbito académico.

3.3.2. Digital

Real Academia Española. (2024). Digital. Como aquello que está relacionado con los dedos o con los dígitos numéricos también se refiere a dispositivos o sistemas que crean, presentan, transportan o almacenan información mediante la combinación de bits, ya que se realizan o transmiten por medios digitales.

3.3.3. Seguridad

Real academia española. (2024). define seguridad como la "cualidad de seguro" y como el "servicio encargado de la seguridad de una persona, de una empresa, de un edificio, etc."

La seguridad activa se refiere a la seguridad que proporciona un conjunto de mecanismos, características o prestaciones de un vehículo cuya función es evitar o prevenir accidentes.

3.3.4. Desarrollo

Real academia española (2014) sobre el término "desarrollo" en el diccionario de la lengua española, se puede expresar de la siguiente manera, el concepto de "desarrollo" abarca la acción y el resultado de crecer o evolucionar, así como la relación entre los componentes de una bicicleta que determina la distancia recorrida con cada pedalada, se refiere a la progresión de una

economía hacia mejores estándares de vida ya la relación entre la potencia y la velocidad en un automóvil, influenciada por la disposición de los engranajes esta definición resalta la diversidad de significados que abarca el término "desarrollo" en distintos contextos, desde el crecimiento personal hasta la evolución económica y mecánica.

3.3.5. Entornos

Real academia española (2021) sobre el término "entorno" en el diccionario de la lengua española, se puede expresar de la siguiente manera, el término "entorno" se refiere al ambiente que rodea a algo, incluyendo las características que definen el lugar y la forma de ejecución de una aplicación informática, en matemáticas, se define como el conjunto de puntos cercanos a otro en artesanía, se menciona como el pliegue que se realiza en la ropa en el borde esta diversidad de significados resalta la importancia de comprender el entorno en diferentes contextos, desde el ámbito físico hasta el digital.

3.3.6. Privacidad

Real Academia Española (2024). Privacidad define la privacidad como la calidad de privado y el ámbito de la vida

. Dispositivos.

Los objetos o instrumentos que se utilizan para realizar una acción o tarea específica. En el contexto digital, los dispositivos se refieren a los equipos y dispositivos tecnológicos que se utilizan para acceder, procesar y gestionar información y datos digitales. Los dispositivos digitales pueden ser de diferentes tipos, como computadoras, teléfonos móviles, tabletas, relojes inteligentes, entre otros. Cada dispositivo digital tiene sus propias características, funcionalidades y limitaciones, y requiere la adopción de estrategias y prácticas específicas para



garantizar su eficacia y eficiencia. Los dispositivos digitales también requieren la consideración de aspectos éticos y sociales, como la accesibilidad, la privacidad, la seguridad y la sostenibilidad, y el compromiso con la mejora continua y la innovación en el diseño y la implementación de soluciones digitales. Los dispositivos digitales son esenciales para promover el aprendizaje, la colaboración y la participación en la era digital, y para satisfacer las necesidades y expectativas de los usuarios en un mundo cada vez más tecnológicamente avanzado.

En el contexto de la tecnología, un dispositivo es un objeto que ha sido diseñado para realizar una o más funciones específicas.

Real Academia Española (2024). En el contexto de la tecnología, un dispositivo es un objeto que ha sido diseñado para realizar una o más funciones específicas, como un teléfono móvil o una computadora los dispositivos pueden ser digitales o analógicos, y pueden ser controlados por software o hardware.



CAPÍTULO IV

PLANIFICACIÓN, EJECUCIÓN Y RESULTADOS PEDAGÓGICAS

Tabla 1

MES	ACTIVIDADES REALIZADAS	TIEMPO
INICIAL		
Marzo	Propuesta en reunión de docentes sobre protegiendo nuestra información en la era digital y aceptación de los temas para su aplicación.	3 Horas
INTERMEDIAS		
Abril	Aplicación de temas en los estudiantes la	12 Horas
FINALES		
Mayo	Evaluación y verificación de procedimientos de los educandos.	12 Horas

Nota: Elaboración propia.

4.1 METODOLOGÍA

4.1.1. Métodos aplicados a la investigación

En la investigación es un enfoque descriptivo implica examinar detalladamente un fenómeno, individuo o grupo sin modificar las variables, centrándose en recolectar información actual sin explorar las causas del comportamiento este método se basa en la observación y el registro de datos para presentar una representación precisa de lo que se está estudiando.

4.1.2. Diseño de la investigación

Un enfoque descriptivo en la investigación y la enseñanza se centra en proporcionar una descripción detallada y precisa de un fenómeno, individuo o grupo, sin intervenir en las variables que lo afectan. Este enfoque se basa en la recopilación de información actual y en la observación y el registro de datos, sin indagar en las causas subyacentes del comportamiento. El objetivo de un enfoque descriptivo es ofrecer una representación precisa y fiel de lo que se está analizando, sin hacer interpretaciones ni llegar a conclusiones definitivas. Este enfoque es útil en situaciones en las que se necesita obtener una visión general de una situación o fenómeno, o en las que se quiere establecer una base de datos sólida para futuras investigaciones. En la enseñanza, un enfoque descriptivo puede ser útil para presentar conceptos y teorías de una manera clara y objetiva, y para ayudar a los estudiantes a desarrollar habilidades de observación y análisis de datos.

4.1.3 Población

Son 2781 estudiantes

4.1.4 Muestreo

Por veracidad varones 30. Total 30

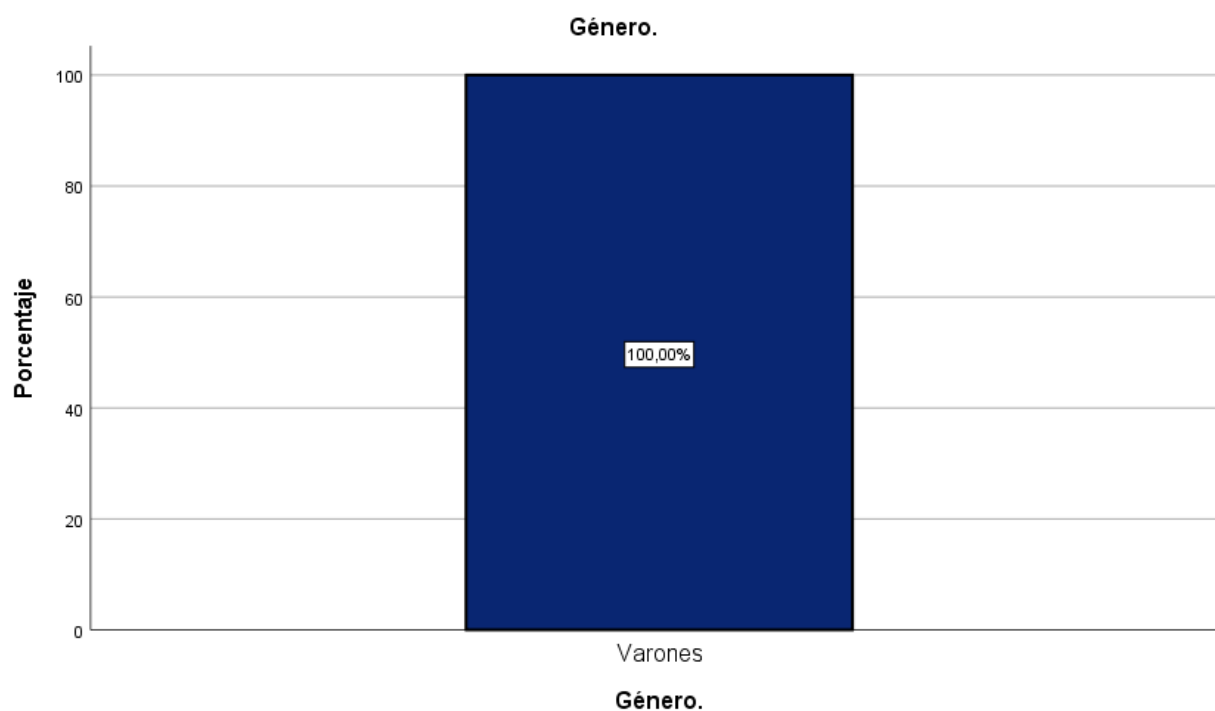
Tabla 2

Género.		
	Frecuencia	Porcentaje
Varones	30	100,0

Nota: Elaboración propia.

Interpretación de la tabla 2. La muestra estaba conformada en varones con una frecuencia de 30 y el porcentaje de 100 %

Figura 1



Nota: Elaboración propia.

Interpretación del gráfico 1. La muestra estaba conformada en varones con el porcentaje de 100%

4.1.5 Técnicas instrumentos y fuentes

Registro, exámenes, hojas de ruta.



4.1.6 Técnicas

El análisis de datos estadísticos implica la aplicación de herramientas y técnicas para procesar, interpretar y comunicar datos de manera significativa. Este proceso incluye el uso de software especializado, cálculos matemáticos, gráficos y tablas para resumir y examinar los datos recopilados. El objetivo principal es extraer conclusiones válidas a partir de los datos y presentar los resultados de forma clara y precisa. El análisis estadístico permite identificar patrones, tendencias y relaciones en los datos, así como evaluar la significancia de los hallazgos. Esta metodología es fundamental en la investigación y la toma de decisiones, ya que proporciona una base objetiva para comprender y comunicar la información contenida en los datos de manera rigurosa y confiable.

4.2 RESULTADOS

La presentación de resultados estadísticos se refiere a la exposición y explicación de los hallazgos numéricos obtenidos a través del análisis de datos. Esta etapa es crucial para la comunicación de los resultados de la investigación, ya que permite a los lectores u oyentes comprender y evaluar la información de manera clara y precisa. La presentación de resultados estadísticos puede incluir el uso de tablas, gráficos y medidas descriptivas, que ayudan a resumir y visualizar los datos de manera efectiva. La elección de los métodos de presentación depende del tipo de datos, el objetivo de la investigación y la audiencia a la que se dirige. El propósito de la presentación de resultados estadísticos es facilitar la comprensión y la interpretación de los hallazgos, y proporcionar una base sólida para la toma de decisiones y la formulación de recomendaciones.

Tabla 3

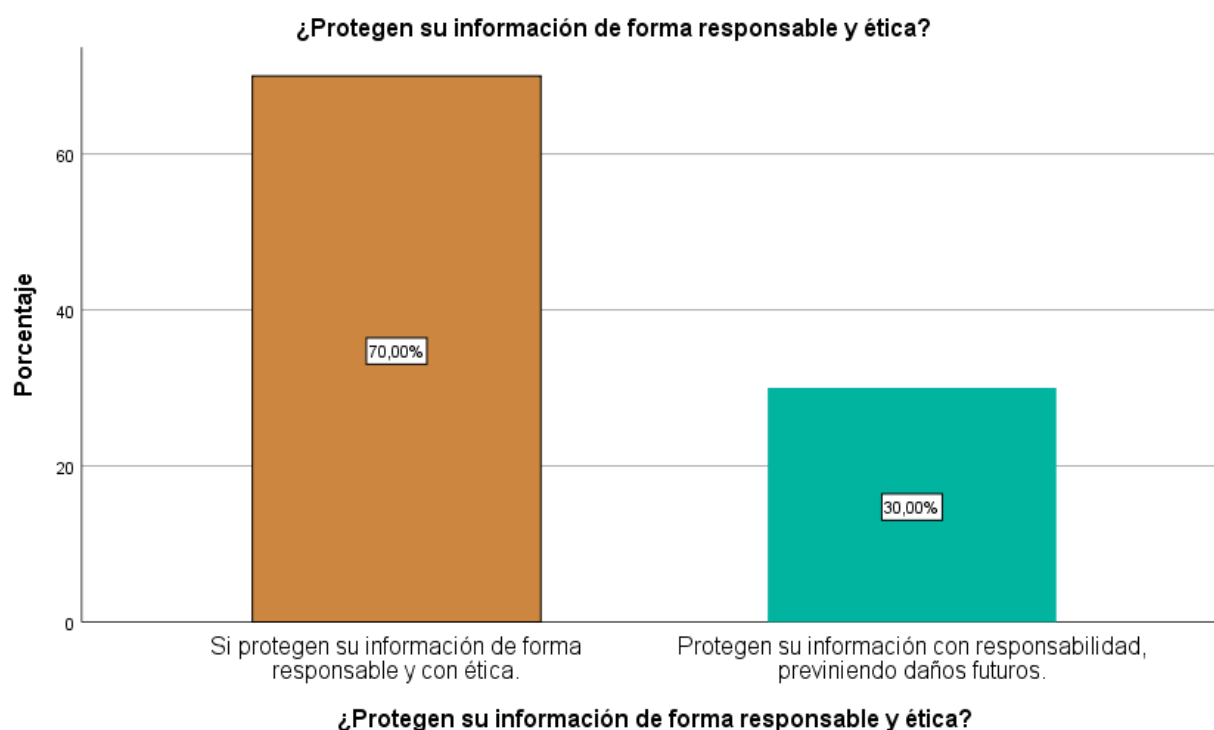
¿Protegen su información de forma responsable y ética?

	Frecuencia	Porcentaje
Si protegen su información de forma responsable y con ética.	21	70,0
Protegen su información con responsabilidad, previniendo daños futuros.	9	30,0
Total	30	100,0

Nota: Elaboración propia

Interpretando la tabla 3 en. Si protegen su información de forma responsable y con ética, con la frecuencia de 21 con el porcentaje de 70.0 por ciento y en Protegen su información con responsabilidad, previniendo daños futuros. Con frecuencia de 9 con el 30,0%, En total la frecuencia de 30 y el porcentaje de 100

Figura 2



Nota: Elaboración propia

Interpretando el gráfico 2. En si protegen su información de forma responsable y con ética, el porcentaje de 70.0 por ciento y en Protegen su información con responsabilidad, previniendo daños futuros con el 30,0%, En total el porcentaje es de 100

Tabla 4

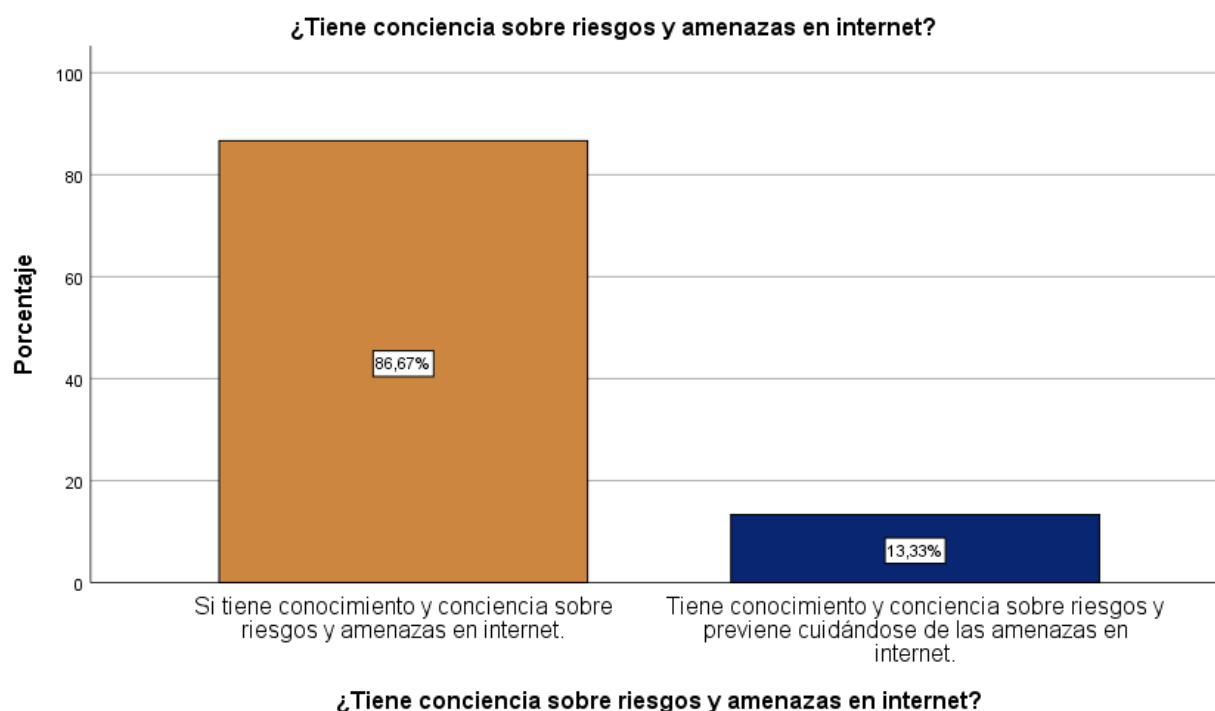
¿Tiene conciencia sobre riesgos y amenazas en internet?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Si tiene conocimiento y conciencia sobre riesgos y amenazas en internet.	26	86,7	86,7	86,7
	Tiene conocimiento y conciencia sobre riesgos y previene cuidándose de las amenazas en internet.	4	13,3	13,3	100,0
	Total	30	100,0	100,0	

Nota: Elaboración propia

Se interpreta la tabla 4 ¿Tiene conciencia sobre riesgos y amenazas en internet? la expresión oral con el ítem Si tiene conocimiento y conciencia sobre riesgos y amenazas en internet con frecuencia de 26 oral con el porcentaje de 86.7 y en Tiene conocimiento y conciencia sobre riesgos y previene cuidándose de las amenazas en internet con frecuencia de 4 con el porcentaje de 13,3% en total la frecuencia de 30 con el 100%

Figura 3



Nota: Elaboración propia.

Se interpreta el grafico 3 ¿Tiene conciencia sobre riesgos y amenazas en internet? la expresión oral con el ítem Si tiene conocimiento y conciencia sobre riesgos y amenazas en internet con el porcentaje de 86.7 y en Tiene conocimiento y conciencia sobre riesgos y previene cuidándose de las amenazas en internet con el porcentaje de 13,3% en total es 100%

RESULTADOS DE LAS ACTIVIDADES PEDAGÓGICAS

La elección de técnicas ha mejorado la expresión, ya que a través de gestos y la práctica, los estudiantes han demostrado una mejora significativa en su habilidad para expresarse de manera correcta.

CONCLUSIONES

PRIMERA: Los resultados fueron muy positivos, ya que se logró concientizar a los estudiantes sobre la importancia de proteger su información en esta era digital se les enseña a utilizar herramientas de seguridad, como contraseñas seguras y antivirus, y desactivar las funciones de localización cuando no se estén utilizando, se les inculcó el valor de la ética y la responsabilidad en el uso de la tecnología, respetando los derechos de autor y la propiedad intelectual.

SEGUNDA: La implementación de estrategias de concienciación sobre seguridad digital en la era digital en estudiantes ha demostrado ser una intervención efectiva para proteger a los estudiantes de los riesgos y amenazas en línea a través de la educación y la promoción de prácticas seguras en el manejo de información personal y la navegación en internet, se ha logrado un aumento en el conocimiento y la comprensión de los riesgos en línea entre los estudiantes, y un cambio en el comportamiento de los mismos al navegar en internet. Además, se ha promovido una cultura de responsabilidad y respeto en línea, al enfatizar la importancia de la privacidad y la seguridad en línea, y al promover prácticas éticas en el uso de internet.

TERCERA: La capacitación de los estudiantes en el desarrollo de habilidades de protección de información ha demostrado ser una intervención efectiva para proteger su información personal en entornos digitales a través de la enseñanza de herramientas y estrategias para proteger sus datos, se ha logrado un aumento en el



conocimiento y la comprensión de los riesgos en línea entre los estudiantes, y un cambio en el comportamiento de los mismos al navegar en internet., se ha promovido una cultura de responsabilidad y respeto.

RECOMENDACIONES

PRIMERA: Para continuar con el éxito de la iniciativa "Proteger la información en la era digital entre los estudiantes se recomienda, ampliar el programa a otros grados y niveles educativos, para asegurar que todos los estudiantes reciban educación en el uso seguro y responsable de la tecnología involucrar a los padres y tutores en el proceso de educación, a través de talleres y sesiones informativas, para asegurar que los estudiantes reciban apoyo y refuerzo en el hogar establecer alianzas con organizaciones y empresas tecnológicas, para obtener recursos y apoyo adicionales en la implementación del programa realice evaluaciones y seguimientos regulares del programa, para medir su impacto y hacer ajustes y mejoras según sea necesario.

SEGUNDA: Se recomienda implementar programas de educación sobre seguridad en la era digital en escuelas, desde el nivel primario hasta el superior, con el objetivo de capacitar a los estudiantes en el uso seguro y responsable de la tecnología, incorporar temas de seguridad digital en el currículo escolar, incluyendo la protección de datos personales, la navegación segura en internet, y el reconocimiento y prevención de riesgos y amenazas en línea fomentar la colaboración entre las escuelas, las familias y las comunidades, para crear una cultura de seguridad digital y promover prácticas seguras en el uso de la tecnología.

TERCERA: Implementar programas de capacitación en protección de datos en las escuelas, desde el nivel primario hasta el superior, con el



objetivo de enseñar a los estudiantes a proteger su información personal y evitar el robo de datos en entornos digitales incorporar temas de protección de datos en el currículo escolar, incluyendo el uso de herramientas y estrategias.

REFERENCIAS

- Amador, MM (2024). La protección de datos personales de los costarricenses y la relación con los humanos en un contexto de transformación digital. Rombo, 4(1), 55-76.
- Barahona Paredes, W. D. L. C. (2017). Análisis de los problemas y amenazas en el Sistema Académico SAI de la Universidad.
- Caicedo Gonzalez, P. A., Contreras Murcia, G. A., & (2024). Estándares de Ciberseguridad Aplicables a los Sistemas Informáticos Sanitarios para Proteger los Datos Personales. Digital Pu, 593.
- Calva Jiménez, S. X. (2020). Protección de datos de carácter personal en la niñez y adolescencia en internet: riesgos y mecanismos de protección. Tesis de licenciatura, [Nombre de la Universidad].
- Chambé-Morales, P. A., & Sarmiento-Martínez, E. Y. (2024). Estudio de riesgos cibernéticos, en la empresa Familiar 'Colegio Diego Rivera' de Tuxtla Gutiérrez, Chiapas. Revista de Investigación Educativa, 4.
- Chuquitarco Lagla, LA (2024). Uso de herramientas digitales en la Cooperativa Ambato sede Latacunga, Provincia de Cotopaxi (Tesis de licenciatura). Universidad Técnica de Cotopaxi (UTC), Latacunga, Ecuador.
- Díaz Sandoval, M. E. D. C., & Rojas Perleche, C. A. (2023). Análisis del nivel de seguridad de la información de la oficina de informática y telecomunicaciones de la municipalidad distrital de San Juan Bautista.
- El artículo de Moya, J. G. (2023) titulado "La importancia de la seguridad informática en la educación digital: retos y soluciones" publicado en la revista RECIMUNDO:



- Escuderos, A. M., Restrepo, D., & Rambal-Rivaldo, L. (2024). El rol del contexto educativo digital vs presencial en perfiles de engagement académico: Estudio comparativo durante y post confinamiento. *Revista de Investigación Educativa*, 4.
- Galardy y Silveira (2021) titulado "Evolución histórica del desarrollo de habilidades infotecnológicas en la educación primaria" aborda la importancia de la adquisición de habilidades tecnológicas en la educación primaria y su evolución histórica. El artículo fue publicado en la *Revista Científica Del Amazonas*, en su edición de agosto de 2021, en el volumen 4(8), páginas 49-58.
- Garitaonandia, C., Karrera-Xuarros, I., Jiménez-Iglesias, E., & Larrañaga, N. (2020). Menores conectados y riesgos online: contenidos inadecuados, uso inapropiado de la información y uso excesivo de internet.
- Hanco Mescoco, Nueva Jersey y Palomino Salazar, VL (2024). Enseñanza a través de dispositivos digitales del cuarto grado de primaria Nuestra Señora del Rosario de Fátima–Chaclacayo 2022.
- Huamán-Cuya, A., Moscoso-Paucarchuco, KM, Yupanqui-Villanueva, HR, Rojas-Hurtado, GF, & Zevallos-López, ZV (2024). Competencias digitales en entornos pospandemia: caso de estudiantes de nivel universitario. *Maestro y Sociedad*, 21(1), 100-108.
- Lazo, C. S., & Correa, B. Á. (2024). Estándares de Ciberseguridad Aplicables a los Sistemas Informáticos Sanitarios para Proteger los Datos Personales. *Digital Pu*, 593. <https://doi.org/10.1111/digpu.12345>



Pino Ortega, J., Gómez Carmona, CD, & Moreno Contreras, MI (2024). Aspectos Sociales, Éticos y Legales de la Tecnología. Maestro y Sociedad, 21(1), 100-108.

Real Academia Española (2021). Entorno . En Diccionario de la lengua española (24.^a ed., p. 678). Recuperado de [https://dle.rae.es/entorno?m=form\[5 \]](https://dle.rae.es/entorno?m=form[5])

Real Academia Española (2024). Dispositivo . En Diccionario de la lengua española. Recuperado de <https://dle.rae.es/dispositivo?m=form>

Real Academia Española (2024). Privacidad. En Diccionario de la lengua española. Recuperado de <https://dle.rae.es/privacidad?m=form>

Real Academia Española. (2014). Desarrollo. En Diccionario de la lengua española (23.^a ed.). Recuperado de <https://dle.rae.es/desarrollo?m=form>

Real Academia Española. (2024). Diccionario de la lengua española. Recuperado de <https://dle.rae.es/protegido?m=form>

Real Academia Española. (2024). digital. Diccionario de la lengua española. Recuperado de <https://dle.rae.es/digital?m=form>

Real Academia Española. (2024). Seguridad. En Diccionario de la lengua española. Recuperado de <https://dle.rae.es/seguridad?m=form>

Sánchez Acuña, WA (2024). Diseño de controles de seguridad informática para el sistema de información en la empresa proveedora de internet Telpronet de la ciudad de Ambato (Tesis de licenciatura). Universidad Técnica de Ambato, Facultad de Contabilidad y Auditoría, Carrera de Contabilidad y Auditoría.



ANEXOS





Unidad Didáctica: Fortaleciendo Hábitos Seguros en el Mundo Digital

1. Datos informativos

- **Área:** Tecnología e Informática
- **Grado:** Cuarto grado de Secundaria
- **Docente:** EDDY ROJAS CHANCO
- **Fecha:** Marzo - Mayo 2023
- **Institución:** Institución Educativa San Luis Gonzaga, ICA

2. Área de Formación

Tecnología e informática, centrada en ciudadanía digital y protección de datos personales.

3. Marco de competencias, capacidades y desempeños

Competencias	Capacidades	Desempeños
Gestiona de forma responsable su información personal en entornos virtuales.	Reconoce amenazas comunes como phishing o exposición de datos en redes sociales.	Identifica datos sensibles (nombre, dirección, fotos) que no deben compartirse en línea.
Desarrolla estrategias para navegar con privacidad y seguridad digital.	Crea contraseñas fuertes y ajusta la configuración de privacidad en aplicaciones básicas.	Aplica reglas para verificar sitios web confiables antes de ingresar datos.
Promueve entre pares el uso ético y protegido de herramientas digitales.	Diseña mensajes claros sobre riesgos digitales para campañas preventivas.	Colabora en grupo para elaborar guías visuales de seguridad en internet.

4. ¿Qué nos dará evidencia de aprendizaje?

Productos como pósters interactivos con reglas de protección digital y

simulaciones prácticas de escenarios riesgosos, donde los estudiantes demuestren toma de decisiones seguras. También elaboran el Decálogo de ciberseguridad.

5. Instrumento de evaluación

Rúbrica observacional que valora precisión en identificación de riesgos (1-4 puntos), creatividad en propuestas de protección (1-4) y participación colaborativa (1-4), junto con autoevaluación mediante listas de verificación personalizadas. También se utilizará el instrumento de evaluación lista de Cotejo con criterios claros y medibles.

6. Situación significativa

Los estudiantes de cuarto grado de la IE San Luis Gonzaga han notado que, en los últimos años, el avance tecnológico está transformando la forma en que interactuamos con la información, brindando innumerables beneficios pero también planteando desafíos significativos en cuanto a la seguridad y en la privacidad de usar datos, este contexto es fundamental concienciar a los educandos sobre la importancia de proteger su información en la era digital, envista que acceden diariamente a plataformas educativas y chats, pero enfrentan peligros como el robo de datos o contactos no deseados al compartir fotos o ubicaciones sin filtros. Frente a ello se plantean las siguientes preguntas ¿Qué es la protección de la información en la era digital? ¿Cómo el ciudadano protege su información personal utilizando los medios digitales? podemos evitar situaciones de riesgo digital? ¿Cómo fomentar conciencia sobre la seguridad en la era digital en el manejo de información y navegación en internet? ¿Qué sabes sobre los riesgos de compartir demasiada información en redes sociales?



Sesión de Aprendizaje: Detectando Peligros Ocultos en la Red Digital

I. Datos informativos

- **Área:** Tecnología e Informática
- **Grado:** Cuarto grado de Secundaria
- **Docente:** EDDY ROJAS CHANCO
- **Fecha laborable:** Miércoles , 29 de marzo de 2023
- **Duración:** 90 minutos
- **Propósito:** Los estudiantes reconocerán datos personales sensibles y practicarán decisiones seguras para evitar riesgos en internet e identifiquen y analicen riesgos digitales como el *phishing*, el *malware* y la ingeniería social, aplicando protocolos de seguridad para proteger su identidad y datos personales.
- **Protegiendo nuestra información en la era digital en estudiantes**

II. Aprendizajes esperados

Competencias	Capacidades	Desempeños/Indicadores
Gestiona responsablemente su información en espacios virtuales.	Identifica tipos de datos que no se deben compartir en línea.	Señale al menos tres ejemplos de información personal riesgosa como dirección o fotos familiares.
Aplicación de medidas básicas de protección digital.	Evalúa situaciones cotidianas de navegación web.	Clasifica mensajes sospechosos como phishing, el <i>malware</i> y la ingeniería social en escenarios simulados.

III. Criterios de evaluación

- Precisión al nombrar datos sensibles (alto: 3+ ejemplos correctos).

- Identifica correctamente elementos de fraude en un mensaje de texto o correo electrónico.
- Utiliza herramientas de escaneo de vulnerabilidades antes de interactuar con contenido web.
- Propone medidas de prevención frente a ataques de ingeniería social.

IV. Secuencia didáctica

1 inicio (20 minutos)

- **Motivación:** Mostrar capturas de pantalla de correos electrónicos falsos de bancos o premios de sorteos inexistentes. Muestra un video corto sobre un "superhéroe digital" que bloquea intrusos en línea, generando entusiasmo por convertirse en protectores de su información.
- **Recuperación de saberes previos:** Preguntar: "¿Qué reglas conoces para no decir tu nombre completo en juegos en línea?, ¿Cómo sabemos si un enlace es seguro antes de hacer clic?" o "¿Qué es lo peor que podría pasar si descargas un archivo desconocido?".
- **Conflicto cognitivo:** ¿Puede un sitio web que tiene "el candado verde" (HTTPS) ser un sitio de estafa?

DESARROLLO

(50

minutos)

En parejas, analizan tarjetas con escenarios (ej: "Un amigo virtual pide tu ubicación") y deciden: ¿compartir o bloquear? Rota estaciones para practicar contraseñas seguras y ajustes de privacidad en aplicaciones simuladas.

Breve explicación sobre la anatomía de un ataque:

- Phishing: Suplantación de identidad mediante URLs engañosas.
- Ingeniería Social: Manipulación psicológica para obtener claves.
- Malware oculto: Archivos ejecutables disfrazados de documentos (.pdf.exe)

Mediante la Practica realiza la Inspección de URLs: Usar herramientas como Google Transparency Report para verificar sitios sospechosos.



Cierre (20 minutos)

Grupo comparte y proponen una "regla de oro" para navegar seguro, reforzando el propósito con un compromiso visual en mural colectivo.

V. Recursos y Herramientas digitales

- Tarjetas impresas con escenarios riesgosos.
- Vídeo motivacional (proyector).
- Hojas para compromisos personales y marcadores.
- Computadoras o tabletas para simulación (opcional).
- Para análisis de amenazas: El portal de VirusTotal es esencial para analizar archivos sospechosos de forma gratuita.
- Guía de Seguridad: Los estudiantes pueden consultar la Guía de Ciberseguridad de la OSI para profundizar en protocolos de protección.

• EVALUACIÓN: LISTA DE COTEJO

TITULO	Detectando Peligros Ocultos en la Red Digital		
COMPETENCIA	Gestiona responsablemente su información en espacios virtuales.	Aplicación de medidas básicas de protección digital	
CATEGORIA	INDICADOR DE LOGRO	SI	NO
Inicio	Reconoce las diferencias entre virus, troyanos, ransomware y spyware.		
	Identifica señales de una posible infección riesgosa en un dispositivo (lentitud, ventanas emergentes, etc.).		
Desarrollo	Analiza correos y mensajes detectando indicadores de <i>phishing</i> (remitentes falsos, urgencia, enlaces dudosos).		
	Identifica perfiles falsos en redes sociales utilizando criterios de verificación de identidad.		
	. Verifica el uso de protocolos seguros (HTTPS y candado) antes de ingresar datos sensibles.		
	Evalúa la seguridad de una red Wi-Fi pública frente a una privada		
	Crea contraseñas seguras siguiendo criterios de complejidad y longitud.		
	Reconoce los riesgos de descargar software "pirata" o archivos de fuentes no oficiales		
Cierre	Propone medidas de respuesta ante un posible caso de ciberacoso o <i>grooming</i> .		
	Toma decisiones seguras y Propone medidas de prevención frente a ataques de ingeniería social		



Sesión de Aprendizaje N°2: Construyendo Escudos contra Amenazas en

Línea

I. Datos informativos

- **Área:** Tecnología e Informática
- **Grado:** Cuarto grado de Secundaria
- **Docente:** EDDY ROJAS CHANCO
- **Fecha laborable:** miércoles, 12 de abril de 2023
- **Duración:** 90 minutos
- **Propósito:** Los estudiantes identificarán amenazas digitales comunes y ensayarán prácticas seguras para manejar su información personal durante la navegación web.
- Fomentar la Conciencia sobre Seguridad en la era digital en estudiantes y Educar a los estudiantes sobre los riesgos y amenazas en línea, promoviendo prácticas seguras en el manejo de información personal y la navegación en internet.

II. Aprendizajes esperados

Competencias	Capacidades	Desempeños/Indicadores
Fomenta la conciencia sobre riesgos en entornos digitales.	Reconoce amenazas como phishing o exposición de datos.	Describe al menos dos riesgos en línea y explica cómo evitarlos en chats escolares.
Promueva hábitos seguros en el manejo de datos personales.	Configura protecciones básicas en dispositivos y aplicaciones.	Demuestra uso de contraseñas fuertes y verificación de sitios en simulaciones.

III. Criterios de evaluación

- Exactitud en reconocer amenazas (alto: identifica 4+ ejemplos con causas).
- Aplicación de prácticas seguras (alto: resuelve correctamente el 90% de escenarios prácticos).

IV. Secuencia didáctica

Inicio (15 minutos)

- Motivación: Proyecta un cómic animado de personajes que derrotan "ladrones digitales", inspirando a los estudiantes a adoptar roles de guardianes en su rutina en línea. Presentar un caso breve (o video) sobre un "secuestro de cuenta" de redes sociales por un enlace sospechoso.
- Saberes Previos: Lluvia de ideas con la pregunta: ¿Qué es lo más valioso que tienes en tu celular o computadora y cómo lo proteges? "¿Cómo proteges tu cuenta en apps de clase?" y anota ideas en tablero para vincularlas con estrategias avanzadas de seguridad
- Conflicto Cognitivo: ¿Es suficiente tener una contraseña difícil para estar 100% seguros? "¿Qué harías si un mensaje pide tu contraseña para un juego escolar?"

5. Desarrollo de aprendizaje (30 minutos)

En equipos, examinan casos reales (ej: email falso solicitando datos) y rotan por estaciones para practicar bloqueos, contraseñas seguras y filtros de contenido, priorizando decisiones protectoras.

También Identifican correctamente los diferentes tipos de amenazas en línea, durante la navegación en la web.

Cierre (10 minutos)

Cada equipo elabora un "escudo digital" en un poster interactivo (producto final: infografía, lista de consejos o configuración de perfiles)..

V. Recursos y materiales

- Cartas con casos de amenazas digitales.
- Proyector para cómic motivacional.
- Hojas, marcadores y tabletas para prácticas.
- Guías impresas de contraseñas seguras.

EVALUACIÓN: LISTA DE COTEJO

TÍTULO	Construyendo Escudos contra Amenazas en Línea		
COMPETENCIA	Fomenta la conciencia sobre riesgos en entornos digitales	Promueva hábitos seguros en el manejo de datos personales	
CATEGORIA	INDICADOR DE LOGRO	SI	NO
Inicio	Indaga sobre riesgos comunes (phishing, virus, malware). Proteges su cuenta en apps de la clase Anota ideas en tablero para vincularlas con estrategias avanzadas de seguridad		
	Ensaya prácticas seguras para manejar su información personal Fomenta Conciencia sobre Seguridad en la era digital.		.
Desarrollo	Identifica correctamente los diferentes tipos de amenazas en línea, durante la navegación en la web.		
	Propone medidas de seguridad robustas (contraseñas seguras)		.
	Participa activamente en la simulación o análisis de casos de riesgo. De email falso solicitando datos.		
	Utiliza herramientas digitales o material educativo de forma responsable		
Cierre	Elabora un "escudo digital" (producto final: infografía, lista de consejos o configuración de perfiles).		.
	Reflexiona sobre la importancia de la ética y la privacidad en la red.		
Actitud	Participa en equipo y muestra una actitud crítica frente a la información que recibe en internet		



Sesión de Aprendizaje N° 3: Construyendo Escudos contra Amenazas en

Línea y el uso seguro de herramienta digitales

I. Datos informativos

- **Área:** Tecnología e informática
- **Grado:** Cuarto grado de Secundaria
- **Docente:** EDDY ROJAS CHANCO
- **Fecha laborable:** miércoles, 12 de mayo de 2023
- **Duración:** 90 minutos
- **Propósito:** Los estudiantes Desarrollaran habilidades protegiendo nuestra información de Datos: Capacitar a los estudiantes en el uso de herramientas y estrategias de protección y sigan protocolos de seguridad para salvaguardar su información personal en la red.
- **II. Aprendizajes esperados**

Competencias	Capacidades	Desempeños/Indicadores
Fomenta la conciencia sobre riesgos en entornos digitales.	Reconoce amenazas como phishing o exposición de datos.	Describe al menos dos riesgos en línea y explica cómo evitarlos en chats escolares.
Promueva hábitos seguros en el manejo de datos personales.	Configura protecciones básicas en dispositivos y aplicaciones.	Demuestra uso de contraseñas fuertes y verificación de sitios en simulaciones.

III. Criterios de evaluación

- Exactitud en reconocer amenazas (alto: identifica 4+ ejemplos con causas).
- Aplicación de prácticas seguras (alto: resuelve correctamente el 90% de escenarios prácticos).

IV. Secuencia didáctica

1. Inicio (15 minutos)

Motivación: Iniciar con el caso real de un "ataque de phishing" reciente a una red social popular. Preguntar: *"¿Alguna vez han recibido un mensaje de un número desconocido pidiendo que hagan clic en un enlace para ganar un premio o evitar que bloqueen su cuenta?"*

Saberes Previos: Indaga: Lluvia de ideas sobre términos como *phishing*, *malware* y *huella digital*. "¿Cómo harías si un mensaje pide tu contraseña para un juego escolar?"

Conflicto Cognitivo: ¿Es suficiente tener un antivirus para estar 100% seguros en internet? "¿Cómo proteges tu cuenta en apps de clase?" y anota ideas en tablero para vincularlas con estrategias avanzadas de seguridad. "¿Qué harías si un mensaje pide tu contraseña para un juego escolar?"

2. DESARROLLO (50 minutos)

En equipos, examinan casos reales (ej: email falso solicitando datos) y rotan por estaciones para practicar bloqueos, contraseñas seguras y filtros de contenido, priorizando decisiones protectoras.

Uso de herramientas para verificar si sus correos han sido filtrados en bases de datos de hackers usando softwares protectores fiables

3. Cierre (20 minutos)

Cada equipo presenta un "escudo digital" con una norma clave, sellando el

aprendizaje con promesas grupales ilustradas en un póster compartido. Y elaboran el Decálogo de ciberseguridad.

V. Recursos y materiales

- Cartas con casos de amenazas digitales.
- Proyector para cómic motivacional.
- Hojas, marcadores y tabletas para prácticas.
- Guías impresas de contraseñas seguras.

RÚBRICA DE EVALUACIÓN

Criterio	Alto (4 puntos)	Medio (3 puntos)	Bajo (2 puntos)	Insuficiente (1 pt)
Reconoce amenazas	Identifica 4+ riesgos con ejemplos precisos.	Identificar 3 riesgos correctamente.	Identifica 2 con imprecisiones.	Identifica 1 o ninguno.
Aplica prácticas seguras	Resuelva todos los casos con acciones protectoras.	Resuelve el 75% de los casos.	Resuelve el 50% de los casos.	Resuelve menos del 50%.
Elabora el decálogo de ciberseguridad	Desarrolla habilidades y participa en forma segura	Desarrolla habilidades y participa regularmente	Desarrolla habilidades y participa esporádicamente	No participa
Colabora en equipo	Lidera aportes y respeta las ideas ajenas.	Aporta regularmente.	Aporta esporádicamente.	No colabora.



ANEXO 1 FORMULARIO DE AUTORIZACIÓN

AUTORIZACIÓN PARA LA INCORPORACIÓN DE LOS TRABAJOS DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL UANCV

Formato digital ☒

Fecha de entrega: 29 - 12 - 2025

1. Datos del autor (es):

Nombres y Apellidos: EDDY ROJAS CHANCO

Dirección: Urb. La Palma Lote : L-7 -ICA

DNI/Carné de Extranjería/Pasaporte N°: 21527546

Teléfono: 943 070 955 email: edrocha20@gmail.com

Nombres y Apellidos: _____

Dirección: _____

DNI/Carné de Extranjería/Pasaporte N°: _____

Teléfono: _____ email: _____

Facultad y/o Escuela de Posgrado: _____ ESCUELA DE POSGRADO

Escuela Profesional o Mención: _____ PROGRAMA DE SEGUNDA ESPECIALIDAD PROFESIONAL

Título o Grado Académico a optar: _____ EN TECNOLOGÍA, COMPUTACIÓN E INFORMÁTICA

Asesor: _____

Esta obra se encuentra dentro de las siguientes denominaciones:

Trabajo de Investigación ☐

Tesis ☒

Trabajo de Suficiencia Profesional ☐

Trabajo Académico ☐

Título: PROTEGIENDO NUESTRA INFORMACIÓN EN LA ERA DIGITAL EN ESTUDIANTES DEL CUARTO GRADO DE LA INSTITUCIÓN EDUCATIVA SAN LUIS GONZAGA ICA 2023

Palabras claves, (3 a 5 términos): Protegiendo, información, digital.

¿Esta obra se desarrolló en la UANCV ^{1, 2}?

1

¹ Indicar si su producción intelectual ha empleado recursos tales como, instalaciones, laboratorios, insumos, equipos, bases de datos, asesoría técnica por parte del personal de la UANCV, financiamiento, entre otros relacionados.

² Si su producción intelectual se desarrolló en la UANCV totalmente o parcialmente, deberá autorizar el depósito en el Repositorio de manera obligatoria.



2. Referencia de tesis:

☐ Bachiller ☐ Título ☒ 2da Especialidad ☐ Maestría ☐ Doctorado

3. Licencias:

a) Licencia estándar:

Bajo los siguientes términos, autorizo el depósito de mi tesis en el Repositorio Digital de la UANCV.

Con la autorización de depósito de mi producción intelectual, otorgo a la Universidad Andina "Néstor Cáceres Velásquez" una licencia no exclusiva para reproducir, distribuir, comunicar al público, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público mi producción intelectual (incluido el resumen), en formato físico o digital, en cualquier medio, conocido o por conocerse, a través de los diversos servicios por la Universidad, creados o por crearse, tales como el Repositorio Digital de tesis UANCV, colección de producción intelectual, entre otros, en el Perú y en el extranjero por el tiempo y veces que considere necesarias, y libres de remuneraciones.

En virtud de dicha licencia, la Universidad Andina "Néstor Cáceres Velásquez" podrá reproducir mi producción intelectual en cualquier tipo de soporte y en más de un ejemplar, sin modificar su contenido, solo con propósitos de seguridad, respaldo y preservación.

Declaro que la producción intelectual es una creación de mi autoría y exclusiva titularidad, coautoría con titularidad compartida, y me encuentro facultado a conceder la presente licencia y, asimismo, garantizo que dicha producción intelectual no infringe derechos de autor de terceras personas.

La Universidad Andina "Néstor Cáceres Velásquez" consignará el nombre del y/o los autor(es) de la producción intelectual, y no le hará ninguna modificación más que la permitida en la licencia.

Autorizo su publicación (marque con una X)

- ☒ Sí, autorizo que se deposite inmediatamente.
- ☐ Sí, autorizo que se deposite a partir de la fecha (d/m/a): _____
- ☐ No autorizo.

b) Licencia CREATIVE COMMONS 4.0 INTERNACIONAL:

Si usted concede una licencia CREATIVE COMMONS sobre su producción intelectual, mantiene la titularidad de los derechos de autor de esta y, a la vez, permite que otras personas puedan reproducirla, comunicarla al público y distribuir ejemplares de esta, bajo las condiciones siguientes:

¿Quiere permitir usos comerciales de su producción intelectual?

Sí: significa que usted permite la reproducción, distribución y comunicación pública de la producción intelectual incluso con fines comerciales.

No: significa que usted permite la reproducción, y comunicación pública de la producción intelectual, pero sin fines comerciales.

- ☐ Sí autorizo
- ☒ No autorizo



Jurisdicción de su Licencia

Todas las licencias CREATIVE COMMONS son de ámbito mundial, sin embargo, usted puede elegir entre la opción “internacional” o una adaptada a su jurisdicción, como para el caso peruano.

La opción “internacional” emplea el lenguaje y la terminología de los tratados internacionales; en cambio, la adaptada a su jurisdicción, recoge las particularidades de la legislación peruana.

En consecuencia, **la opción “internacional” goza de una mayor eficacia a nivel mundial, gracias a que tiene jurisdicción neutral.** Mientras que la opción adaptada a la jurisdicción del Perú goza de una mayor eficacia ante los tribunales peruanos.

☐

Internacional

☒

Nacional

Línea de investigación: GESTIÓN DE LA EDUCACIÓN - SEG22

Firma de Autor



huella digital

29 - 12 - 2025

Fecha