



Universidad Nacional José Faustino Sánchez Carrión

**Facultad de Derecho y Ciencias Políticas
Escuela Profesional de Derecho y Ciencias Políticas**

Determinación de criterios sobre aplicabilidad de ciberseguridad basada en la cultura de autoprotección ciudadana para lograr mitigar delitos informáticos (Huacho, 2025)

**Tesis
Para optar el Título Profesional de Abogado**

**Autor
Christopher Cherrepano Chinchay**

**Asesor
Dr. Juan Miguel Juárez Martínez**



**Huacho – Perú
2026**



Reconocimiento – No Comercial – Sin Derivadas- Sin Restricciones adicionales

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

Reconocimiento: Debe otorgar el crédito correspondiente, proporcionar un enlace a la licencia e indicar si se realizaron cambios. Puede hacerlo de cualquier manera razonable, pero no de ninguna manera que sugiera que el licenciante lo respalda a usted o su uso. **No Comercial:** No puede utilizar el material con fines comerciales. **Sin Derivadas:** Si remezcla, transforma o construye sobre el material, no puede distribuir el material modificado. **Sin restricciones adicionales:** No puede aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros de hacer cualquier cosa que permita la licencia.



UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

LICENCIADA

(Resolución de Consejo Directivo N° 012-2020-SUNEDU/CD de fecha 27/01/2020)

Facultad de Derecho y Ciencias Políticas

Escuela Profesional de Derecho y Ciencias Políticas

METADATOS

DATOS DEL AUTOR		
APELLIDOS Y NOMBRES	DNI	FECHA DE SUSTENTACIÓN
Cherrepano Chinchay Christopher	71464574	07 / Setiembre / 2026
DATOS DEL ASESOR		
APELLIDOS Y NOMBRES	DNI	CÓDIGO DE ORCID
Dr. Juárez Martínez Juan Miguel	16754186	https://orcid.org/0000-0001-8959-1270
DATOS DE LOS MIEMBROS DEL JURADO		
APELLIDOS Y NOMBRES	DNI	CÓDIGO DE ORCID
Dr. Rojas Alvarado Alberto	08953616	https://orcid.org/0000-0002-6822-8402
Mag. Meza Aguirre Maria Rosario	17859377	https://orcid.org/0000-0003-3736-5903
Mag. Mendoza Huerta Leonid Ronald	41184635	https://orcid.org/0000-0001-8189-2642

Christopher Cherrepano Chinchay

Determinación de criterios sobre aplicabilidad de ciberseguridad basada en la cultura de autoprotección ciudad...

 TESIS PREGRADO DERECHO Y CIENCIAS POLITICAS

 REVISION DE TESIS PREGRADO 2026

 Facultad de Derecho y Ciencias Políticas

Detalles del documento

Identificador de la entrega

tm:oid::1:3619518346

Fecha de entrega

29 jul 2026, 8:16 p.m. GMT-5

Fecha de descarga

29 jul 2026, 8:42 p.m. GMT-5

Nombre del archivo

3_Tesis_CHERREPANO_CHINCHAY_CHRISTOPHER_-_2026.pdf

Tamaño del archivo

1.6 MB

151 páginas

36.193 palabras

229.015 caracteres



Página 2 de 167 - Descripción general de integridad

Identificador de la entrega tm:oid::1:3619518346

20% Similitud general

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

Fuentes principales

18%  Fuentes de Internet

7%  Publicaciones

12%  Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

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

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

DEDICATORIA

Con todo mi amor y gratitud a mis padres, quienes con su ejemplo, sacrificio y cariño infinito han sido la guía en mi vida, que siempre creyeron en mí y me apoyaron incondicionalmente, les debo todo lo que soy. Este logro es tan suyo como mío.

AGRADECIMIENTO

A Dios por darme la fortaleza, la salud y la sabiduría para culminar esta etapa tan importante de mi vida.

A mis padres, por su amor incondicional, su confianza en mí y por ser mi mayor fuente de inspiración y motivación en todo momento.

A mi asesor de tesis, cuyo conocimiento y paciencia me guiaron durante este proceso, brindándome las herramientas necesarias para superar los desafíos

ÍNDICE

Dedicatoria	V
Agradecimiento	VI
Índice.....	VII
Índice de Tablas	XI
Índice de Figuras	XIII
Resumen	XVI
Abstract	XVII
Introducción	XVIII
Capítulo I : PLANTEAMIENTO DEL PROBLEMA	21
1.1 Descripción de la realidad problemática	21
1.2 Formulación del problema.....	22
1.2.1 Problema general	22
1.2.2 Problemas específicos.....	22
1.3 Objetivos de la investigación.....	22
1.3.1 Objetivo general	22
1.3.2 Objetivos específicos.....	22
1.4 Justificación de la investigación	23
1.4.1 Justificación Teórica.....	23
1.4.2 Justificación Social	23
1.4.3 Justificación Práctica	24
1.4.4 Justificación Legal.....	24
1.4.5 Justificación Metodológica.....	24
1.5 Delimitaciones del estudio.....	24
1.6 Viabilidad del estudio	25
Capítulo II : MARCO TEÓRICO	26
2.1 Antecedentes de la investigación.....	26
2.1.1 Investigaciones internacionales	26
2.1.2 Investigaciones nacionales	28
2.2 Bases teóricas	30
2.2.1 Ciberseguridad.....	30
2.2.2 Ciberseguridad humana: el componente conductual y su entrenamiento.....	33
2.2.3 Delitos informáticos	37
2.2.4 Cultura de seguridad (cultura de autoprotección ciudadana)	45
2.2.5 Factor humano (como principal vulnerabilidad - objetivo vulnerable).....	52
2.2.6 Derecho informático, derechos digitales y comportamiento preventivo	63
2.2.7 Criterios de aplicabilidad en la cultura de autoprotección	66

2.2.8 Criterios operativos para el diseño e implementación de un modelo de ciberseguridad fundamentado en la cultura de autoprotección ciudadana, con el fin de reducir la incidencia de delitos informáticos	69
2.3 Definiciones de términos básicos	71
2.4 Hipótesis de la investigación	73
2.4.1 Hipótesis general	73
2.4.2 Hipótesis específicas.....	73
2.5 Las variables	74
2.6 Operacionalización de las variables	74
Capítulo III : METODOLOGÍA.....	76
3.1 Diseño metodológico.....	76
3.2 Tipo de investigación.....	77
3.3 Nivel de la investigación	77
3.4 Diseño de la investigación.....	78
3.5 Enfoque de la investigación.....	78
3.6 Estilo de la investigación.....	79
3.7 Población y muestra.....	79
3.7.1 Población	79
3.7.2 Muestra	80
3.8 Técnicas de recolección de datos.....	81
3.8.1 Técnicas de recolección de datos a emplear	81
3.8.2 Descripción de los instrumentos.....	81
3.8.3 Recolección de datos	82
3.8.4 Codificación.....	82
3.8.5 Tabulación	82
3.8.6 Registro de datos	83
3.8.7 Presentación de datos.....	83
3.9 Técnicas para el procesamiento de la información.....	83
Capítulo IV : RESULTADOS	84
4.1 Análisis de resultados	84
4.2 Contrastación de hipótesis	133
Capítulo V : DISCUSIÓN.....	134
Capítulo VI : CONCLUSIONES Y RECOMENDACIONES.....	137
6.1 Conclusiones.....	137
6.1.1 Primera conclusión	137
6.1.2 Segunda conclusión	137
6.1.3 Tercera conclusión.....	137
6.1.4 Cuarta conclusión	137

6.1.5 Quinta conclusión	138
6.2 Recomendaciones	138
6.2.1 Primera recomendación	138
6.2.2 Segunda recomendación	138
6.2.3 Tercera recomendación.....	138
6.2.4 Cuarta recomendación	138
6.2.5 Quinta recomendación.....	139
Capítulo VII : REFERENCIAS	140
ANEXO (MATRIZ DE CONSISTENCIA)	152

ÍNDICE DE TABLAS

Tabla 1. Sexo	84
Tabla 2. Grupo etario.....	84
Tabla 3. Experiencia con accesos no autorizados de terceras personas a los dispositivos o sistemas informáticos personales.....	85
Tabla 4. Problemas de seguridad en sistemas informáticos personales en el último año....	86
Tabla 5. Pérdida o alteración de información personal por ataques informáticos.....	87
Tabla 6. Revisiones propias regulares de seguridad en los sistemas informáticos personales	88
Tabla 7. Frecuencia de actualización del software de seguridad personal	89
Tabla 8. Uso de contraseñas personales seguras y únicas en cuentas en línea.....	90
Tabla 9. Frecuencia de realización de copias de seguridad de datos importantes personales	91
Tabla 10. Información sobre amenazas cibernéticas actuales	92
Tabla 11. Experiencia respecto al fraude informático relacionado con datos personales ...	93
Tabla 12. Experiencia de robo o uso no autorizado de datos personales	94
Tabla 13. Ha visualizado o conoce casos de intentos de suplantación de identidad digital	95
Tabla 14. Medidas activas de protección de datos informáticos personales	96
Tabla 15. Revisión de la configuración de privacidad en redes sociales	97
Tabla 16. Preocupación por el uso indebido de datos personales en línea.....	98
Tabla 17. Frecuencia de compartir información personal sensible en línea.....	99
Tabla 18. Verificación de la autenticidad de las fuentes antes de compartir información en línea	100
Tabla 19. Implementación de medidas eficaces por parte de las autoridades locales para proteger los derechos digitales	101
Tabla 20. Garantía de protección adecuada a través de las leyes actuales sobre derechos digitales.....	102
Tabla 21. Participación ciudadana en iniciativas gubernamentales para fortalecer la protección de derechos digitales.....	103
Tabla 22. Confianza en las herramientas tecnológicas como medio para prevenir vulneraciones digitales	104
Tabla 23. Información constante sobre las leyes que protegen los derechos digitales.....	105
Tabla 24. Frecuencia con la que las leyes actuales son efectivas para proteger los derechos en línea.....	106

Tabla 25. Frecuencia con la que ha sentido que sus derechos digitales han sido vulnerados	107
Tabla 26. Frecuencia con la que las autoridades deberían hacer más para educar a la población sobre sus derechos digitales	108
Tabla 27. Conocimiento de medidas de seguridad necesarias para prevenir ataques cibernéticos.....	109
Tabla 28. Identificación de posibles vulneraciones a los derechos digitales personales ...	110
Tabla 29. Recepción de información educativa sobre ciberseguridad y derechos digitales por parte de las autoridades.....	111
Tabla 30. Acceso a formación en ciberseguridad y protección de derechos digitales	112
Tabla 31. Participación en talleres o cursos sobre seguridad en línea como estrategia preventiva	113
Tabla 32. Importancia de la educación sobre seguridad en línea para reducir los delitos informáticos	114
Tabla 33. Uso de recursos en línea como medio para aprender sobre seguridad digital ...	115
Tabla 34. Inclusión de la educación sobre derechos digitales en los currículos escolares	116
Tabla 35. Preocupación por el acceso no autorizado a información personal en línea	117
Tabla 36. Uso de mecanismos que garanticen la confidencialidad de la información personal	118
Tabla 37. Experiencia de divulgación no autorizada de información confidencial.....	119
Tabla 38. Confianza en las plataformas digitales para proteger la confidencialidad de los datos.....	120
Tabla 39. Sensación de seguridad al compartir información personal en entornos digitales	121
Tabla 40. Implementación de medidas para proteger la confidencialidad de la información en redes sociales	122
Tabla 41. Revisión regular de las políticas de privacidad de las aplicaciones utilizadas ..	123
Tabla 42. Frecuencia con la que se experimenta divulgación no autorizada de información personal.....	124
Tabla 43. Preocupación por la modificación no autorizada de información digital.....	125
Tabla 44. Implementación de medidas para proteger la integridad de la información personal en línea.....	126
Tabla 45. Detección de cambios no autorizados en datos personales o profesionales	127
Tabla 46. Confianza en las plataformas digitales para mantener la integridad de la información.....	128

Tabla 47. Verificación de la exactitud de la información recibida en línea	129
Tabla 48. Identificación de información incorrecta o manipulada en cuentas o dispositivos digitales.....	130
Tabla 49. Aseguramiento de que la información compartida en línea sea veraz	131
Tabla 50. Dificultad para detectar la manipulación de datos en entornos digitales	132

ÍNDICE DE FIGURAS

Figura 1. Sexo.....	84
Figura 2. Grupo etario	84
Figura 3. Experiencia con accesos no autorizados de terceras personas a los dispositivos o sistemas informáticos personales.....	85
Figura 4. Problemas de seguridad en sistemas informáticos personales en el último año ..	86
Figura 5. Pérdida o alteración de información personal por ataques informáticos	87
Figura 6. Revisiones propias regulares de seguridad en los sistemas informáticos personales	88
Figura 7. Frecuencia de actualización del software de seguridad personal.....	89
Figura 8. Uso de contraseñas personales seguras y únicas en cuentas en línea	90
Figura 9. Frecuencia de realización de copias de seguridad de datos importantes personales	91
Figura 10. Información sobre amenazas cibernéticas actuales.....	92
Figura 11. Experiencia respecto al fraude informático relacionado con datos personales..	93
Figura 12. Experiencia de robo o uso no autorizado de datos personales	94
Figura 13. Ha visualizado o conoce casos de intentos de suplantación de identidad digital	95
Figura 14. Medidas activas de protección de datos informáticos personales	96
Figura 15. Revisión de la configuración de privacidad en redes sociales	97
Figura 16. Preocupación por el uso indebido de datos personales en línea.....	98
Figura 17. Frecuencia de compartir información personal sensible en línea	99
Figura 18. Verificación de la autenticidad de las fuentes antes de compartir información en línea	100
Figura 19. Implementación de medidas eficaces por parte de las autoridades locales para proteger los derechos digitales	101
Figura 20. Garantía de protección adecuada a través de las leyes actuales sobre derechos digitales.....	102
Figura 21. Participación ciudadana en iniciativas gubernamentales para fortalecer la protección de derechos digitales.....	103
Figura 22. Confianza en las herramientas tecnológicas como medio para prevenir vulneraciones digitales	104
Figura 23. Información constante sobre las leyes que protegen los derechos digitales	105

Figura 24. Frecuencia con la que las leyes actuales son efectivas para proteger los derechos en línea.....	106
Figura 25. Frecuencia con la que ha sentido que sus derechos digitales han sido vulnerados	107
Figura 26. Frecuencia con la que las autoridades deberían hacer más para educar a la población sobre sus derechos digitales	108
Figura 27. Conocimiento de medidas de seguridad necesarias para prevenir ataques cibernéticos.....	109
Figura 28. Identificación de posibles vulneraciones a los derechos digitales personales .	110
Figura 29. Recepción de información educativa sobre ciberseguridad y derechos digitales por parte de las autoridades	111
Figura 30. Acceso a formación en ciberseguridad y protección de derechos digitales	112
Figura 31. Participación en talleres o cursos sobre seguridad en línea como estrategia preventiva	113
Figura 32. Importancia de la educación sobre seguridad en línea para reducir los delitos informáticos.....	114
Figura 33. Uso de recursos en línea como medio para aprender sobre seguridad digital..	115
Figura 34. Inclusión de la educación sobre derechos digitales en los currículos escolares	116
Figura 35. Preocupación por el acceso no autorizado a información personal en línea	117
Figura 36. Uso de mecanismos que garanticen la confidencialidad de la información personal	118
Figura 37. Experiencia de divulgación no autorizada de información confidencial	119
Figura 38. Confianza en las plataformas digitales para proteger la confidencialidad de los datos.....	120
Figura 39. Sensación de seguridad al compartir información personal en entornos digitales	121
Figura 40. Implementación de medidas para proteger la confidencialidad de la información en redes sociales	122
Figura 41. Revisión regular de las políticas de privacidad de las aplicaciones utilizadas	123
Figura 42. Frecuencia con la que se experimenta divulgación no autorizada de información personal.....	124
Figura 43. Preocupación por la modificación no autorizada de información digital	125
Figura 44. Implementación de medidas para proteger la integridad de la información personal en línea	126
Figura 45. Detección de cambios no autorizados en datos personales o profesionales.....	127

Figura 46. Confianza en las plataformas digitales para mantener la integridad de la información.....	128
Figura 47. Verificación de la exactitud de la información recibida en línea.....	129
Figura 48. Identificación de información incorrecta o manipulada en cuentas o dispositivos digitales.....	130
Figura 49. Aseguramiento de que la información compartida en línea sea veraz	131
Figura 50. Dificultad para detectar la manipulación de datos en entornos digitales	132

RESUMEN

La presente investigación aborda la crítica problemática del incremento de delitos informáticos frente a la evidente vulnerabilidad del factor humano en los entornos digitales contemporáneos. El problema central radica en la ausencia de una cultura de autoprotección consolidada en los ciudadanos de Huacho, lo que facilita que los ciberdelincuentes exploten sesgos cognitivos y carencias preventivas. En este sentido, el objetivo general del estudio es determinar los criterios operativos para el diseño e implementación de un modelo de ciberseguridad fundamentado en la cultura de autoprotección ciudadana, con el fin de reducir la incidencia de delitos informáticos en la ciudad de Huacho durante el año 2025.

Metodológicamente, el estudio se apoyó en un enfoque pertinente para la recolección y análisis de datos, tomando como población a los 435 estudiantes del Instituto de Idiomas de la Universidad Nacional José Faustino Sánchez Carrión (UNJFSC). Los resultados obtenidos a través de las encuestas evidencian una preocupante paradoja conductual: si bien la población demuestra habilidades técnicas básicas para la navegación y el uso de plataformas digitales, presenta severas deficiencias cognitivas y conductuales para identificar y neutralizar amenazas complejas, operando bajo un fuerte “sesgo de optimismo” y “fatiga de seguridad”. Se concluye que el analfabetismo digital preventivo es el principal facilitador del cibercrimen local, y que un modelo de ciberseguridad exitoso debe cimentarse obligatoriamente en tres ejes: accesibilidad cognitiva, sostenibilidad práctica y proporcionalidad económica. Al transformar al ciudadano de un “objetivo vulnerable” a una “línea de defensa activa”, se logra una mitigación real de las amenazas.

***Palabras clave:* Ciberseguridad, autoprotección ciudadana, delitos informáticos, prevención digital, factor humano.**

ABSTRACT

This research addresses the critical problem of the increase in cybercrime in the face of the evident vulnerability of the human factor in contemporary digital environments. The central problem lies in the absence of a consolidated self-protection culture among the citizens of Huacho, which facilitates the exploitation of cognitive biases and preventative deficiencies by cybercriminals. In this sense, the overall objective of the study is to determine the operational criteria for the design and implementation of a cybersecurity model based on a culture of citizen self-protection, in order to reduce the incidence of cybercrime in the city of Huacho by 2025. Methodologically, the study relied on a relevant approach for data collection and analysis, using as its population the 435 students of the Language Institute of the José Faustino Sánchez Carrión National University (UNJFSC). The results obtained through the surveys reveal a worrying behavioral paradox: while the population demonstrates basic technical skills for navigating and using digital platforms, it exhibits severe cognitive and behavioral deficiencies in identifying and neutralizing complex threats, operating under a strong “optimism bias” and “security fatigue.” It is concluded that preventive digital illiteracy is the main facilitator of local cybercrime, and that a successful cybersecurity model must be based on three pillars: cognitive accessibility, practical sustainability, and economic proportionality. By transforming citizens from “vulnerable targets” into “active lines of defense,” real threat mitigation is achieved.

Keywords: *Cybersecurity, citizen self-protection, cybercrime, digital prevention, human factor.*

INTRODUCCIÓN

La transformación digital contemporánea ha dejado de ser una simple transición tecnológica para erigirse como el eje estructural de las interacciones humanas, económicas y administrativas a nivel global. Si bien la hiperconectividad ha dinamizado el desarrollo de las sociedades, también ha institucionalizado un ecosistema de riesgos asimétricos, donde la sofisticación de las amenazas cibernéticas evoluciona con una celeridad abrumadoramente mayor a las capacidades de defensa del usuario promedio. Históricamente, la seguridad de la información delegaba su eficacia a la robustez de las barreras tecnológicas (como firewalls y algoritmos criptográficos); sin embargo, la doctrina moderna en ciberseguridad y la criminología digital reconocen unánimemente que el “factor humano” constituye el eslabón más vulnerable de la cadena de protección. En la actualidad, las modalidades delictivas de mayor impacto económico no centran sus esfuerzos en vulnerar códigos de programación complejos, sino en explotar sesgos cognitivos, descuidos y carencias preventivas de los ciudadanos mediante técnicas de ingeniería social.

A nivel internacional, la ciberdelincuencia se ha consolidado como una problemática de alto impacto social y económico, impulsada por modalidades como el phishing, el fraude informático, la suplantación de identidad, el ransomware y la ingeniería social. Estas conductas aprovechan la confianza de los usuarios, la inmediatez de la comunicación digital y la baja percepción del riesgo para lograr sus fines ilícitos. En países con desarrollo tecnológico desigual, el crecimiento del acceso a internet no siempre ha ido acompañado de una formación equivalente en seguridad digital, lo que incrementa la exposición de la población a ataques y engaños cada vez más sofisticados. Bajo esta perspectiva, la prevención no puede depender únicamente de sistemas de defensa institucionales, sino también de la capacidad de los ciudadanos para reconocer señales de alerta, adoptar hábitos seguros y responder adecuadamente ante situaciones de riesgo.

En el contexto latinoamericano, y específicamente en el Perú, este panorama resulta particularmente desafiante debido a la persistente brecha digital y a la insuficiente madurez de las políticas públicas orientadas a la alfabetización tecnológica. El Estado peruano, en su esfuerzo por hacer frente a esta criminalidad emergente, promulgó la Ley N° 30096, Ley de Delitos Informáticos, estableciendo un marco normativo para sancionar conductas como el fraude informático, la suplantación de identidad y el acceso ilícito. No obstante, la naturaleza del aparato de justicia penal es eminentemente reactiva; se activa de manera exclusiva cuando el daño patrimonial, psicológico o moral ya ha sido consumado.

Las estadísticas nacionales reflejan la crisis de este modelo puramente punitivo: un incremento sostenido de denuncias por ciberdelitos que terminan, en su gran mayoría, saturando el sistema fiscal debido a la falta de mecanismos de prevención desde la base ciudadana.

Esta desconexión entre la norma legal y la realidad conductual se agudiza drásticamente en escenarios locales en plena expansión comercial, como es el caso de la ciudad de Huacho. Al consolidarse como un nodo administrativo y económico, la población huachana ha integrado masivamente herramientas como la banca móvil, las billeteras digitales y el comercio electrónico en su dinámica diaria. Lamentablemente, este acelerado crecimiento transaccional no ha sido acompañado por el desarrollo de una cultura de seguridad. Los habitantes operan bajo un fuerte “sesgo de optimismo” y una carencia de higiene digital, convirtiéndose en blancos perfectos para redes de estafadores que operan a distancia. La percepción de lejanía con las unidades especializadas de investigación en Lima incrementa la sensación de vulnerabilidad e impunidad.

Frente a esta problemática, surge la imperiosa necesidad de cambiar el paradigma tradicional: el ciudadano debe dejar de ser catalogado como un “objetivo vulnerable” y transformarse en la primera línea de defensa activa del ecosistema digital. Es aquí donde la presente investigación encuentra su justificación teórica, social y legal. El derecho, actuando de forma aislada, ha demostrado ser insuficiente si no converge con controles sociales eficientes y hábitos preventivos tangibles. Por ello, se postula que la verdadera eficacia para mitigar el cibercrimen radica en operativizar el espíritu de la normativa a través de la autoprotección.

Bajo esta premisa, el objetivo principal del presente estudio es determinar los criterios operativos para el diseño e implementación de un modelo de ciberseguridad fundamentado en la cultura de autoprotección ciudadana, orientado a reducir la incidencia de delitos informáticos en la ciudad de Huacho durante el año 2025. Metodológicamente, la investigación focaliza su análisis en la comunidad estudiantil del Instituto de Idiomas de la Universidad Nacional José Faustino Sánchez Carrión (UNJFSC). Esta elección poblacional no solo permite un abordaje estructurado, sino que busca desmitificar la premisa de que el analfabetismo digital preventivo es exclusivo de las poblaciones de la tercera edad, evidenciando que los jóvenes y adultos contemporáneos (pese a su inmersión tecnológica) carecen de criterios defensivos reales.

A través del análisis de las dimensiones cognitivas, actitudinales y conductuales de la población, esta tesis aspira a proporcionar un marco de aplicabilidad real. Se busca dotar a las instituciones locales de herramientas y criterios basados en la accesibilidad cognitiva, la sostenibilidad práctica y la proporcionalidad económica, logrando así que la ciberseguridad trascienda los manuales técnicos y se convierta en un hábito cotidiano, resiliente y capaz de frenar la criminalidad informática desde su origen.

Capítulo I : PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción de la realidad problemática

La transformación digital contemporánea ha dejado de ser una simple transición tecnológica para convertirse en el eje estructural de las interacciones humanas, económicas y administrativas. En ese proceso, la expansión del uso de internet, redes sociales, banca móvil y servicios digitales ha incrementado la exposición de los ciudadanos a riesgos informáticos que evolucionan con mayor rapidez que sus capacidades de defensa. En ese marco, la ciberseguridad ya no puede entenderse únicamente como protección técnica, sino como un sistema integral que articula prácticas, tecnologías, procesos y comportamientos orientados a resguardar redes, dispositivos, programas y datos frente a accesos no autorizados y daños intencionales. Asimismo, la evidencia documentada permite sostener que el factor humano constituye el eslabón más vulnerable de la cadena de protección, debido a que muchas de las amenazas no se concretan por fallas tecnológicas, sino por descuidos, conductas inseguras y falta de cultura preventiva en los usuarios.

A nivel internacional, el cibercrimen se ha consolidado como una forma de criminalidad de alto impacto que aprovecha la confianza del usuario y la asimetría entre la sofisticación del atacante y la vulnerabilidad del ciudadano común. Modalidades como el phishing, el ransomware y la ingeniería social se han perfeccionado para explotar la confianza, la urgencia y la baja percepción del riesgo en entornos virtuales. En esa misma línea, las diferencias en la madurez de la ciberseguridad entre regiones también dependen de la desigualdad en el desarrollo y uso de internet, lo que coloca a los países en vías de desarrollo en una posición especialmente vulnerable si no equilibran el acceso tecnológico con la capacitación ciudadana.

En el contexto nacional, la problemática se intensifica porque, aunque el Perú cuenta con un marco normativo específico para enfrentar los delitos informáticos, la respuesta estatal continúa siendo predominantemente reactiva. La Ley N.º 30096 tipifica conductas como el fraude informático, el acceso ilícito y la interceptación de datos; sin embargo, su aplicación se produce cuando el daño ya ha ocurrido. Pese a los esfuerzos normativos, persiste una desconexión entre el conocimiento teórico y la práctica preventiva, situación que demuestra que la alfabetización digital en el país todavía es insuficiente frente al ritmo con el que evolucionan las amenazas digitales.

Esta realidad se agudiza en ámbitos locales como la ciudad de Huacho, provincia de Huaura. La población ha integrado de manera masiva el uso de la banca móvil, el comercio electrónico y las redes sociales en su vida cotidiana; no obstante, ese crecimiento digital no ha sido acompañado por el desarrollo de criterios de autoprotección. Por ende, los ciudadanos enfrentan una vulnerabilidad sistémica debido a la ausencia de hábitos como la verificación de fuentes, el uso de autenticación multifactor y la gestión crítica de los datos personales.

Además, la distancia geográfica y operativa respecto a unidades especializadas incrementa la percepción de impunidad y desamparo frente a estos delitos. Por ello, surge la necesidad imperativa de determinar criterios operativos de aplicabilidad de la ciberseguridad que no dependan solo de herramientas técnicas, sino que se fundamenten en una cultura de autoprotección ciudadana capaz de mitigar la incidencia delictiva en Huacho.

1.2 Formulación del problema

1.2.1 Problema general único

¿Cuáles son los criterios operativos para diseñar e implementar un modelo de ciberseguridad basado en la cultura de autoprotección ciudadana que permita reducir la incidencia de delitos informáticos en Huacho en el año 2025?

1.2.2 Problemas específicos

En la presente investigación no se formulan problemas específicos, debido a que el estudio se estructura a partir de un problema general único orientado a determinar criterios operativos de aplicabilidad de la ciberseguridad basada en la cultura de autoprotección ciudadana para mitigar delitos informáticos en Huacho durante el año 2025.

1.3 Objetivos de la investigación

1.3.1 Objetivo general

Determinar los criterios operativos para el diseño e implementación de un modelo de ciberseguridad fundamentado en la cultura de autoprotección ciudadana, con el fin de reducir la incidencia de delitos informáticos en Huacho durante el año 2025.

1.3.2. Objetivos específicos

- Diagnosticar el nivel de conocimientos y prácticas de autoprotección digital existentes en la comunidad.
- Describir las modalidades de delitos informáticos y riesgos digitales más relevantes para el contexto de estudio.

- Establecer criterios de aplicabilidad de la ciberseguridad para la prevención de dichos riesgos.
- Proponer medidas de fortalecimiento de la cultura de autoprotección ciudadana

1.4 Justificación de la investigación

La presente investigación se fundamenta en la necesidad imperativa de salvaguardar la integridad digital de la comunidad de Huacho frente al crecimiento exponencial de la criminalidad informática. El incremento de estos delitos no solo pone en riesgo los recursos económicos de las familias huachanas, sino que socava la confianza en los servicios digitales, un componente crítico para el desarrollo sostenible y la modernización de la ciudad. Al centrarse en la cultura de autoprotección, este estudio propone un enfoque preventivo y comunitario que actúa de forma complementaria a las soluciones puramente tecnológicas o normativas, la finalidad que se espera es contribuir a una población más informada y resiliente, capaz de gestionar sus propias defensas en el ciberespacio. A continuación, se detalla la importancia de este estudio desde diversas dimensiones:

1.4.1 Justificación Teórica

La investigación realiza un aporte significativo al cuerpo de conocimientos sobre ciberseguridad al proponer un cambio de paradigma: transitar de una visión estrictamente técnica hacia una centrada en el factor humano. Se busca profundizar en la relación entre la psicología del usuario y sus hábitos preventivos, analizando cómo la cultura de autoprotección puede integrarse como una variable determinante en la mitigación de riesgos. De este modo, el estudio ofrece una perspectiva donde el ciudadano deja de ser visto como un eslabón débil para convertirse en el primer escudo de defensa activa en el ecosistema digital.

1.4.2 Justificación Social

Desde el plano social, este trabajo tiene un impacto directo en la protección del patrimonio y la privacidad de los habitantes de Huacho. Busca reducir la vulnerabilidad de sectores que suelen ser blanco de estafas, como los adultos mayores, los jóvenes y los pequeños comerciantes locales que han migrado sus negocios al entorno virtual. Al fortalecer la resiliencia ciudadana, no solo se evitan pérdidas económicas y daños emocionales, sino que se fomenta una convivencia digital más segura, equitativa y consciente, devolviendo a la población el control sobre su propia seguridad.

1.4.3 Justificación Práctica

Los resultados de esta tesis proporcionarán criterios accionables y herramientas tangibles que podrán ser implementadas por las autoridades municipales, instituciones educativas y comisarías de la ciudad. La creación de guías de orientación, programas de concientización y propuestas de políticas públicas locales permitirá que Huacho cuente con un modelo de prevención adaptado a su realidad demográfica y comercial. Este enfoque práctico asegura que la investigación no se quede en la teoría, sino que se convierta en una solución real para enfrentar los fraudes y la suplantación de identidad en el día a día.

1.4.4 Justificación Legal

El estudio se encuentra plenamente alineado con el marco jurídico nacional, específicamente con la Ley N° 30096. Se justifica legalmente al buscar mecanismos que operativicen el espíritu de la ley desde la base ciudadana, facilitando que las normativas de protección tengan un respaldo real en la conducta de las personas. De esta manera, se contribuye a que el marco legal peruano sea más efectivo mediante la reducción de incidentes que muchas veces quedan en la impunidad por falta de prevención básica.

1.4.5 Justificación Metodológica

Finalmente, el diseño de la investigación ofrece un valor metodológico al proponer una combinación de análisis cualitativos y cuantitativos para evaluar la madurez de la ciberseguridad ciudadana en contextos locales. Los instrumentos validados y los criterios establecidos en este estudio servirán como una base sólida y replicable para futuras investigaciones en otras municipalidades del país que enfrenten desafíos similares, permitiendo estandarizar procesos de evaluación de la cultura preventiva en entornos urbanos en expansión.

1.5 Delimitaciones del estudio

La presente investigación se delimita espacialmente en la ciudad de Huacho, específicamente en el Instituto de Idiomas de la Universidad Nacional José Faustino Sánchez Carrión (UNJFSC), donde se desarrollará el trabajo de campo. En cuanto a la delimitación temporal, el estudio será ejecutado durante el año 2025. Respecto a la delimitación poblacional, la investigación estará dirigida a los estudiantes matriculados en el Instituto de Idiomas de la UNJFSC, cuya población total asciende a 435 estudiantes, distribuidos en 29 grupos de estudio, considerando un mínimo de 15 estudiantes por aula.

La elección estratégica de esta población responde a dos criterios fundamentales:

En primer lugar, el criterio de accesibilidad y viabilidad operativa, dado que el investigador es estudiante activo y delegado del curso de inglés intermedio en la misma institución, lo que garantiza un entorno de confianza, minimiza el sesgo de rechazo y facilita la interacción directa para la recolección de datos genuinos.

En segundo lugar, responde a un criterio de fundamentación teórica: enfocar el estudio en estudiantes de idiomas (mayoritariamente jóvenes y adultos jóvenes) permite desmitificar el paradigma que asocia la vulnerabilidad ante ciberdelitos exclusivamente con las personas de la tercera edad o sin acceso tecnológico.

Se busca demostrar empíricamente que la inmersión tecnológica diaria de la juventud no es sinónimo de cultura de autoprotección, existiendo un déficit preventivo profundo en estas generaciones.

Desde el punto de vista temático, el estudio se centrará en la determinación de criterios sobre la aplicabilidad de la ciberseguridad basada en la cultura de autoprotección ciudadana, orientada a la prevención y mitigación de delitos informáticos. En tal sentido, la investigación no abarcará aspectos técnicos avanzados de ciberseguridad institucional, sino que se enfocará en prácticas preventivas, hábitos de autoprotección digital y criterios de seguridad aplicables al comportamiento de los estudiantes frente a riesgos informáticos.

1.6 Viabilidad del estudio

El presente estudio resulta viable debido a que se cuenta con una población claramente identificada y accesible, conformada por los estudiantes del Instituto de Idiomas de la UNJFSC. Asimismo, la institución dispone de 29 grupos de estudio y de una población estimada de 435 estudiantes, lo que facilita la aplicación de instrumentos de recolección de datos en un contexto concreto y delimitado.

De igual manera, la investigación es factible en términos metodológicos, ya que permite obtener información directa mediante la aplicación de encuestas o entrevistas a los estudiantes, quienes constituyen la unidad de análisis. La disponibilidad de tiempo, el acceso a la población y la pertinencia del tema con la realidad actual de los delitos informáticos contribuyen a la ejecución del estudio sin mayores dificultades.

Además, el tema seleccionado presenta relevancia social y académica, debido a que la cultura de autoprotección ciudadana frente a riesgos digitales constituye un aspecto importante para fortalecer conductas preventivas en el uso de herramientas tecnológicas. En consecuencia, la investigación es viable tanto por sus condiciones de acceso y desarrollo como por su aporte al conocimiento en materia de ciberseguridad y prevención de delitos informáticos.

Capítulo II : MARCO TEÓRICO

2.1 Antecedentes de la investigación

2.1.1 Investigaciones internacionales

Sinergia Académica (2026), en la publicación titulada “Conciencia y cultura de ciberseguridad en estudiantes universitarios en entornos de educación virtual”, tuvo como objetivo de investigación analizar las actitudes y la comprensión profunda de los riesgos en línea en usuarios con un alto nivel de inmersión tecnológica. La metodología implementada se basó en un enfoque mixto de nivel descriptivo y explicativo, combinando la recolección de datos estadísticos con el análisis cualitativo del comportamiento digital. Los principales hallazgos revelaron una paradoja conductual alarmante: aunque los usuarios presentan un dominio operativo aceptable para navegar y acceder a diversas plataformas, tienen severas limitaciones cognitivas para identificar amenazas informáticas complejas mediante ingeniería social. De este modo, se llegó a la conclusión de que existe en la sociedad una “falsa sensación de seguridad”, donde la habilidad técnica básica no garantiza la autodefensa en el ciberespacio. El aporte a la presente investigación es crucial para nutrir la justificación y descripción de la realidad problemática, sustentando que en el contexto de Huacho, el simple hecho de saber utilizar WhatsApp o realizar transferencias bancarias no significa estar protegido, haciendo imperativo establecer un modelo preventivo.

Tobar y Casa (2025), en la tesis “La educación digital y su rol en la prevención ante la ciberdelincuencia juvenil” en Ecuador, plantearon como objetivo analizar el papel de la educación digital en la prevención de la ciberdelincuencia juvenil, evaluando su efectividad e identificando estrategias educativas que contribuyan a reducir amenazas y conductas delictivas en el entorno virtual. La metodología utilizada fue mixta, combinando encuestas aplicadas a estudiantes y docentes con entrevistas semiestructuradas, lo que permitió recoger tanto datos cuantitativos como percepciones cualitativas. Los resultados evidenciaron que las iniciativas educativas existentes no son suficientemente eficaces, pues aunque los jóvenes reconocen los riesgos digitales, los programas carecen de una estructura práctica e integral que los involucre de forma real en la prevención. Asimismo, se identificó que el ciberacoso y la suplantación de identidad continúan siendo problemas relevantes. La conclusión más importante fue que los programas de educación en ciberseguridad deben fortalecerse mediante estrategias más interactivas, prácticas y permanentes, junto con la capacitación continua de los docentes y el impulso de políticas públicas. Este trabajo se relaciona directamente con la presente investigación porque confirma que la prevención de delitos

informáticos requiere educación aplicada, hábitos seguros y participación activa del usuario, elementos que se alinean con la cultura de autoprotección ciudadana.

Albarrán y Campos (2024), en la tesis “Análisis de la privacidad y seguridad en las redes sociales en un mundo de ciberdelitos”, plantearon como objetivo evaluar la percepción de los usuarios de redes sociales respecto de la privacidad y la seguridad en línea, además de analizar las amenazas existentes y las medidas de ciberseguridad aplicables en ese entorno. La investigación se desarrolló bajo una metodología de enfoque mixto, apoyada en revisión bibliográfica y aplicación de encuestas, lo que permitió contrastar la percepción subjetiva de los usuarios con su comportamiento real frente a los riesgos digitales. Entre sus principales hallazgos, se evidenció que una parte importante de los encuestados se siente poco segura al navegar en redes sociales; sin embargo, esa percepción no siempre se traduce en cambios concretos de conducta, pues muchos usuarios mantienen sus hábitos digitales pese a reconocer los peligros. La autora concluyó que existe una necesidad crítica de fortalecer la educación y la concienciación sobre privacidad y seguridad en línea, así como de actualizar las medidas de protección y las regulaciones vigentes. Esta investigación refuerza la idea de que la cultura de autoprotección no depende solo del conocimiento del riesgo, sino de la adopción de conductas preventivas sostenidas, aspecto central para determinar criterios de aplicabilidad de la ciberseguridad.

Santos (2023), en su tesis titulada “Marco regulatorio de la ciberseguridad y ciberdefensa dentro de la sociedad de la información y el conocimiento. Respuestas del Estado ecuatoriano en el período 2013-2022”, tuvo como objetivo principal analizar la estructura regulatoria del Estado y la integración del sector privado en el ciberespacio para enfrentar las amenazas digitales. La metodología empleada fue de carácter cualitativo, sustentada en un diseño de análisis documental, dogmático y normativo del marco jurídico nacional e internacional. Los principales hallazgos revelaron que los desarrollos puramente legislativos resultan estériles frente a la cibercriminalidad si no convergen con controles sociales eficientes y políticas integradas, evidenciando que el derecho, actuando de forma aislada, demuestra ser ineficaz. En consecuencia, la autora llegó a la conclusión de que la respuesta penal no es disuasiva si carece de un respaldo estructural enfocado en la prevención ciudadana. El aporte a la presente investigación es fundamental, ya que otorga un sólido sustento jurídico-crítico que justifica cómo la mera tipificación de delitos (como la Ley N° 30096 en el Perú) es insuficiente, demostrando empíricamente la urgencia de establecer los criterios operativos propuestos en la presente investigación para aterrizar la norma legal en una verdadera cultura preventiva.

2.1.2 Investigaciones nacionales

Cajigas Moreano y Pérez Chirinos (2023), en su tesis de grado titulada La incidencia de las nuevas tecnologías en el delito de fraude informático y su aplicación en la Ley N.º 30096 en el Perú, desarrollada en la Universidad Andina del Cusco, analizaron cómo la evolución tecnológica influye en el crecimiento del fraude informático y en la eficacia de la normativa penal vigente. El repositorio señala que el fraude informático ha aumentado en el Perú por la mayor utilización de medios electrónicos, especialmente durante la pandemia, y que la Ley N.º 30096 podría requerir actualización para adaptarse a nuevas modalidades delictivas. En ese marco, los autores evidencian que la normativa actual no basta por sí sola para prevenir estos ilícitos. Este antecedente resulta pertinente para la presente investigación porque confirma la necesidad de complementar el enfoque jurídico con criterios operativos de autoprotección ciudadana, orientados a reducir la incidencia de delitos informáticos en la ciudad de Huacho.

Correa Coronel (2022), en su tesis de maestría titulada Ciberseguridad y su incidencia en el tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021, desarrollada en la Universidad César Vallejo, tuvo como objetivo determinar la incidencia de la ciberseguridad en el tratamiento de datos personales en una municipalidad distrital de Lima Sur. Metodológicamente, realizó una investigación aplicada con diseño no experimental, transversal y de corte correlacional–causal, empleando una muestra de 282 colaboradores, la técnica de encuesta y el cuestionario como instrumento de recolección de datos. Entre sus principales hallazgos, el estudio encontró que la ciberseguridad incide significativamente en el tratamiento de datos personales. En consecuencia, el autor concluyó que el fortalecimiento de la ciberseguridad resulta indispensable para salvaguardar la información sensible en contextos públicos locales. Este antecedente aporta a la presente investigación porque confirma que la ciberseguridad posee un impacto real y medible en ámbitos territoriales concretos, lo cual respalda la necesidad de establecer criterios operativos de autoprotección ciudadana para reducir la vulnerabilidad frente a delitos informáticos en Huacho.

Jancachagua Vera (2021), en su tesis de grado titulada Mejoramiento de la seguridad de la información para reducir los ciberataques del tipo phishing en una entidad financiera, desarrollada en la Universidad Tecnológica del Perú, tuvo como objetivo implementar mejoras de seguridad de la información para contrarrestar los ataques de phishing en una entidad financiera. Su estudio se estructuró bajo la metodología del Project Management Institute (PMI) y propuso la implementación de Gophish como solución para reforzar los

controles existentes. Entre sus hallazgos principales, el repositorio destaca que el phishing utiliza técnicas de engaño para obtener credenciales y que su eficacia depende en gran medida de la capacitación y concientización de las personas. En consecuencia, el trabajo sustenta que la seguridad digital no depende únicamente de herramientas técnicas, sino también del comportamiento preventivo del usuario. Este antecedente se relaciona con la presente investigación porque demuestra que la cultura de autoprotección ciudadana constituye un componente esencial para reducir los delitos informáticos, lo que justifica la necesidad de determinar criterios operativos de aplicabilidad de ciberseguridad para la población de Huacho.

Torres Pozo (2014), en su tesis de grado titulada La problemática de la función investigatoria del delito de fraude informático en el Perú, desarrollada en la Universidad César Vallejo, tuvo como objetivo principal dar a conocer la problemática existente en la investigación del fraude informático y aportar al Código Penal. El repositorio señala que el trabajo recogió entrevistas a autoridades vinculadas con la investigación penal, como la DIVINDAT, el Ministerio Público y el Poder Judicial, además de datos estadísticos que evidencian la magnitud del problema. Entre sus hallazgos principales, se identificó que la dilación del tiempo investigatorio excede plazos razonables y que el fraude informático es uno de los delitos más comunes, más fáciles de cometer y más difíciles de identificar. En consecuencia, el autor concluyó que la función investigatoria presenta serias limitaciones de efectividad. Este antecedente aporta directamente a la presente investigación porque confirma que la respuesta penal resulta insuficiente por sí sola, lo que refuerza la necesidad de establecer criterios operativos de aplicabilidad de ciberseguridad basados en la cultura de autoprotección ciudadana para reducir la incidencia de delitos informáticos en Huacho.

2.2 Bases teóricas

2.2.1 Ciberseguridad

2.2.1.1. Concepto de ciberseguridad

La ciberseguridad constituye el conjunto de prácticas, tecnologías, procesos y comportamientos diseñados para proteger redes, dispositivos, programas y datos de ataques, daños o accesos no autorizados (Von Solms & Van Niekerk, 2013). En el contexto contemporáneo, trasciende la mera protección técnica para convertirse en un ecosistema integral que abarca dimensiones humanas, organizacionales y sociales. La ciberseguridad no es un estado estático sino un proceso dinámico y continuo que evoluciona constantemente para responder a nuevas amenazas y vulnerabilidades (Kott & Arnold, 2016).

Según la Agencia de la Unión Europea para la Ciberseguridad (ENISA, 2023), la ciberseguridad se define como “el conjunto de condiciones que permiten que las personas, las organizaciones y los Estados disfruten de las ventajas de las tecnologías digitales mientras se protegen contra los efectos adversos de los incidentes de seguridad”. Esta definición resalta la importancia de equilibrar el aprovechamiento de beneficios digitales con la protección contra riesgos emergentes.

En el marco de la sociedad de la información y la creciente digitalización de entornos urbanos emergentes, la conceptualización de la seguridad ha migrado desde un enfoque perimetral puramente informático hacia una visión holística e interconectada denominada ciberseguridad. Desde una perspectiva técnica general, Whitman y Mattord (2018) sugieren que la seguridad representa un estado dinámico de resguardo frente al peligro, las brechas de datos o las intrusiones adversas. Cuando este principio se traslada al entorno digital, la ciberseguridad se delimita como la protección integral de los activos de información que transitan, se procesan o se almacenan dentro del ciberespacio, abarcando tanto los componentes de hardware y software como las redes de comunicación asociadas.

Para formalizar su aplicabilidad en políticas públicas y marcos de gobernanza, la Unión Internacional de Telecomunicaciones [UIT] (2020) define la ciberseguridad como el conglomerado sistémico de herramientas, políticas institucionales, directrices conceptuales, metodologías para la administración de riesgos, programas de formación, tecnologías avanzadas y prácticas idóneas orientadas a salvaguardar de manera restrictiva el ciberentorno, así como las propiedades de las organizaciones y de los usuarios individuales. Bajo esta óptica, es fundamental discernir que, a diferencia de la seguridad de la información tradicional la cual protege los datos en cualquier soporte o formato, la ciberseguridad enfoca

sus esfuerzos de manera específica en la naturaleza simbiótica entre el usuario y la infraestructura tecnológica conectada a redes globales. En el contexto específico de un estudio situado en la ciudad de Huacho, entender la ciberseguridad no implica únicamente la adopción de algoritmos criptográficos gubernamentales, sino la asimilación de estas directrices institucionales por parte del ciudadano común, quien interactúa permanentemente en un ciberespacio donde las fronteras jurisdiccionales tradicionales quedan diluidas frente a la criminalidad informática.

2.2.1.2. Importancia y principios básicos: la tríada CIA

La importancia de la ciberseguridad radica en su papel fundamental para proteger la información personal, financiera y estratégica en un entorno digital cada vez más interconectado. A nivel nacional, constituye un elemento crítico para la protección de infraestructuras esenciales, la soberanía digital y la continuidad de servicios básicos. A nivel individual, salvaguarda la privacidad, el patrimonio y la identidad digital de los ciudadanos (Pfleeger & Pfleeger, 2012).

Los principios básicos de la ciberseguridad se fundamentan en la proactividad, la defensa en profundidad, la resiliencia y la adaptabilidad continua. Estos principios reconocen que ninguna medida de seguridad es infalible por sí sola, y que la protección efectiva requiere un enfoque multifacético que combine controles técnicos, procesos organizacionales y capacitación humana (Stallings, 2017).

La relevancia de la ciberseguridad en el ámbito civil radica en su capacidad para garantizar el desarrollo seguro de las actividades socioeconómicas y la estabilidad psicosocial de los ciudadanos. La vulneración de los entornos digitales no se traduce únicamente en pérdidas monetarias abstractas; impacta de forma directa en la intimidad, la confianza pública y la gobernabilidad democrática local. Para estructurar criterios viables de mitigación del delito informático, la literatura científica internacional concuerda en que cualquier arquitectura o política de seguridad digital debe erigirse obligatoriamente sobre tres pilares fundamentales e indivisibles, denominados de manera conjunta como la Tríada CIA: la confidencialidad, la integridad y la disponibilidad (Stallings, 2018).

- **Confidencialidad.** Este principio básico determina que el acceso a la información confidencial o sensible debe restringirse de forma exclusiva a aquellos usuarios explícitamente autorizados para conocerla (Whitman y Mattord, 2018). En términos ciudadanos, la confidencialidad previene que los datos de carácter personal, bancario o residencial sean interceptados por terceros con fines maliciosos. Mecanismos proactivos como el cifrado simétrico y los sistemas restrictivos de control de acceso

son esenciales para garantizar esta propiedad. En el escenario delictivo actual, la pérdida de confidencialidad constituye la antesala de ilícitos graves como la suplantación de identidad, la extorsión cibernética y el fraude financiero.

- **Integridad.** Definida como la cualidad que asegura que la información permanezca exacta, completa y libre de alteraciones maliciosas o accidentales desde su origen hasta su destino (Stallings, 2018). La integridad garantiza que un mensaje, una transacción bancaria o un registro administrativo no hayan sido modificados en el tránsito por un agente externo no autorizado. El uso de funciones hash criptográficas y la implementación de firmas digitales son herramientas técnicas empleadas para verificar que los datos no han sufrido manipulación. La afectación a este pilar se evidencia nítidamente en la alteración de transferencias bancarias o en la inyección de datos falsos dentro de sistemas comerciales de uso público.
- **Disponibilidad.** Este pilar establece que los usuarios legítimos u autorizados deben tener un acceso ágil, ininterrumpido y oportuno tanto a los datos como a los servicios informáticos esenciales en el momento exacto en que lo requieran (ISO/IEC, 2022). La disponibilidad es frecuentemente blanco de ciberataques de denegación de servicio distribuido (DDoS) o del secuestro de datos mediante códigos de tipo *ransomware*, los cuales paralizan plataformas de atención ciudadana o servicios de banca por internet. Para el ciudadano común, la pérdida de disponibilidad implica la imposibilidad de gestionar sus recursos económicos o acceder a servicios esenciales, lo que quiebra la resiliencia operativa de la comunidad digital.

2.2.1.3. Aplicación de la ciberseguridad a nivel de usuario

La aplicación de estos pilares a nivel ciudadano requiere traducir conceptos técnicos a prácticas cotidianas comprensibles y ejecutables. La confidencialidad se manifiesta en el uso de contraseñas seguras y la protección de información personal; la integridad en la verificación de comunicaciones y la detección de intentos de manipulación; y la disponibilidad en el mantenimiento de dispositivos actualizados y la protección contra *ransomware* que impide el acceso a información propia (ENISA, 2023).

En el contexto específico de Huacho, esta aplicación a nivel de usuario adquiere particular relevancia debido al creciente uso de servicios digitales bancarios, comerciales y de comunicación por parte de la población, sin un desarrollo paralelo de competencias digitales de seguridad (Secretaría de Gobierno y Transformación Digital, 2025).

Históricamente, los controles orientados a sostener la Tríada CIA se delegaban de forma exclusiva a departamentos técnicos corporativos o administradores de redes institucionales. No obstante, el advenimiento de la hiperconectividad residencial ha provocado una descentralización crítica de la responsabilidad de seguridad. En la actualidad, los criterios operativos de la ciberseguridad demandan una aplicación práctica a nivel de usuario, comúnmente operada bajo el concepto de “higiene digital” (Schneier, 2019).

La higiene digital comprende la asimilación cotidiana de conductas preventivas elementales por parte del ciudadano, tales como el diseño de contraseñas complejas y diferenciadas, la actualización recurrente de los sistemas operativos y programas de uso diario, y la desconfianza metódica ante canales de comunicación no verificados.

La traslación de estos principios técnicos a la praxis diaria del individuo es el eje donde se fundamenta la viabilidad de cualquier propuesta de autoprotección comunitaria. Cuando el usuario comprende y aplica de manera directa controles de autenticación multifactor (2FA) o identifica de manera autónoma las sutilezas de una dirección web fraudulenta, la ciberseguridad deja de ser un software abstracto instalado en un servidor externo y pasa a convertirse en una competencia cívica activa. De este modo, la aplicación individualizada de buenas prácticas se constituye en el catalizador primario para frenar la proliferación de conductas criminales que se aprovechan, precisamente, del descuido conductual en los dispositivos de uso personal.

2.2.2 Ciberseguridad humana: el componente conductual y su entrenamiento

2.2.2.1. El factor humano en la seguridad digital: análisis del “eslabón más débil”

El concepto de ciberseguridad humana reconoce que el factor humano constituye simultáneamente la mayor vulnerabilidad y el principal activo de defensa en cualquier sistema de protección. Tradicionalmente considerado el “eslabón más débil”, el usuario puede transformarse en la primera línea de defensa mediante capacitación adecuada y desarrollo de competencias específicas (Hadžiosmanović et al., 2015).

Según una investigación de Pfleeger y Caputo (2012), “el factor humano es a menudo considerado el eslabón más débil en la seguridad de la información, pero también puede ser la primera línea de defensa si se le proporciona la capacitación y herramientas adecuadas” (p. 45).

La ciberseguridad humana se fundamenta en la premisa de que los comportamientos seguros pueden ser enseñados, aprendidos y reforzados mediante estrategias pedagógicas adecuadas. Este enfoque reconoce que los errores humanos no son inevitables, sino

consecuencia de falta de conocimiento, entrenamiento insuficiente o sistemas que no consideran factores cognitivos y conductuales (Provan & Lemon, 2018).

A pesar del vertiginoso avance en los sistemas de detección de intrusos, firewalls basados en inteligencia artificial y protocolos criptográficos de última generación, las brechas de seguridad continúan expandiéndose a nivel global. Ello se debe a que los vectores de ataque contemporáneos han desplazado su objetivo principal de las vulnerabilidades del código de programación hacia las vulnerabilidades cognitivas del operador humano. En la disciplina de la ingeniería de seguridad, se acuñó de manera tradicional la premisa de que el ser humano constituye inherentemente el “eslabón más débil” dentro de la cadena de resguardo digital (Mitnick y Simon, 2002). Esta noción se fundamenta en que los atacantes prefieren recurrir a la ingeniería social métodos de manipulación psicológica encaminados a engañar al individuo para que entregue credenciales o ejecute software dañino en lugar de invertir recursos en romper barreras tecnológicas altamente sofisticadas.

Analizando esta problemática desde un enfoque sociotécnico, Schneier (2019) argumenta que catalogar al usuario de forma simplista como el elemento fallido o el “eslabón más débil” denota una deficiencia estructural en el diseño del propio ecosistema digital. Los delitos informáticos comunes que afectan a la población tales como el *phishing* (suplantación de páginas de entidades financieras), el *vishing* (engaños telefónicos masivos) y el *smishing* (mensajes de texto fraudulentos) no explotan fallas en los sistemas informáticos de los bancos, sino que manipulan variables humanas universales como el miedo a la pérdida del dinero, el sentido de urgencia o la confianza hacia las figuras de autoridad simuladas. Por ende, la ciberseguridad humana surge como un campo de estudio especializado que rechaza la mera estigmatización del ciudadano y pasa a evaluar de qué forma los sesgos cognitivos, la fatiga de seguridad y los hábitos digitales influyen de modo determinante en el éxito o fracaso de las actividades delictivas.

2.2.2.2. Factores psicológicos en la ciberseguridad humana

La comprensión de los factores psicológicos que influyen en el comportamiento humano frente a riesgos digitales es fundamental para desarrollar estrategias efectivas de ciberseguridad humana. Según Hadžiosmanović et al. (2015), “los sesgos cognitivos, las heurísticas de decisión y las influencias sociales desempeñan un papel crucial en cómo los usuarios perciben y responden a las amenazas digitales” (p. 132). Entre estos factores se incluyen el optimismo sesgado, que lleva a los usuarios a subestimar su vulnerabilidad personal; la percepción limitada de costos, que hace que prioricen la conveniencia sobre la seguridad; y la influencia social, que puede normalizar comportamientos de riesgo.

2.2.2.3. Enfoques pedagógicos en ciberseguridad humana

Los enfoques pedagógicos para el desarrollo de competencias en ciberseguridad humana han evolucionado desde modelos tradicionales de transmisión de información hacia estrategias más interactivas y personalizadas. Provan y Lemon (2018) identifican tres enfoques principales: la formación basada en concienciación, centrada en transmitir conocimientos sobre riesgos y medidas de protección; el entrenamiento basado en habilidades, enfocado en desarrollar competencias prácticas específicas; y el aprendizaje basado en el comportamiento, orientado a modificar hábitos y rutinas digitales.

2.2.2.4. Medición de la competencia en ciberseguridad humana

La medición efectiva de la competencia en ciberseguridad humana representa un desafío significativo debido a la naturaleza multifacética de este constructo. Según Hadžiosmanović et al. (2015), “la evaluación de la competencia en ciberseguridad humana debe considerar no solo los conocimientos teóricos, sino también la aplicación práctica de medidas de seguridad y la consistencia de los comportamientos seguros a lo largo del tiempo” (p. 135). Esta evaluación puede realizarse mediante simulaciones de ataques, análisis de comportamientos reales en entornos controlados y evaluaciones de conocimientos actitudinales.

2.2.2.5. Desafíos de la ciberseguridad humana en contextos locales

La implementación de estrategias de ciberseguridad humana en contextos locales como Huacho presenta desafíos específicos que deben considerar al desarrollar criterios de aplicabilidad. Estos incluyen factores socioculturales como niveles de alfabetización digital, percepciones de riesgo específicas del contexto local, y recursos disponibles para implementar medidas de seguridad (Secretaría de Gobierno y Transformación Digital, 2025). Además, la diversidad de perfiles de usuarios en términos de edad, formación y experiencia digital requiere enfoques diferenciados que reconozcan estas variaciones.

2.2.2.6. Integración de perspectivas

La integración de perspectivas técnicas y humanas constituye un requisito fundamental para el desarrollo de estrategias de ciberseguridad efectivas. Según Von Solms y Van Niekerk (2013), “la ciberseguridad moderna no puede abordarse exclusivamente desde una perspectiva técnica ni únicamente desde el enfoque humano, sino que requiere la integración sinérgica de ambas dimensiones para crear un ecosistema de protección resiliente y adaptativo” (p. 84). Esta integración implica reconocer que las soluciones técnicas deben

diseñarse considerando factores humanos, mientras que las estrategias de formación deben alinearse con los controles técnicos implementados.

En el contexto de Huacho, esta integración adquiere particular relevancia debido a la necesidad de adaptar soluciones globales a realidades locales específicas, donde tanto las capacidades técnicas como las competencias humanas presentan características distintivas que deben considerarse al desarrollar criterios de aplicabilidad (Secretaría de Gobierno y Transformación Digital, 2025).

2.2.2.7. Modelos de ciberseguridad humana

Diversos modelos teóricos han surgido para comprender y abordar la dimensión humana de la ciberseguridad. El modelo de Competencia en Ciberseguridad Humana desarrollado por Hadžiosmanović et al. (2015) integra conocimientos, habilidades y actitudes en un marco holístico que permite evaluar y desarrollar capacidades específicas. Por otro lado, el marco de Ciberseguridad Centrada en el Humano propuesto por Provan y Lemon (2018) enfatiza la importancia de diseñar sistemas y procesos que consideren las limitaciones y capacidades humanas desde su concepción.

Estos modelos proporcionan fundamentos teóricos importantes para el desarrollo de criterios de aplicabilidad que buscan integrar la cultura de autoprotección ciudadana con técnicas de seguridad.

2.2.2.8. Tendencias emergentes en ciberseguridad humana

Las tendencias emergentes en ciberseguridad humana incluyen el uso de inteligencia artificial para personalizar la formación, el desarrollo de nudges digitales para influir positivamente en comportamientos, y la creación de ecosistemas de aprendizaje continuo que se adaptan a las amenazas cambiantes (Kott & Arnold, 2016). Estas tendencias representan oportunidades para innovar en los criterios de aplicabilidad que se desarrollan en la presente investigación.

2.2.2.9. De eslabón más débil a primera línea de defensa: el entrenamiento ciudadano

El núcleo transformador de la ciberseguridad humana postula que, dado que el comportamiento del usuario es una variable modificable, el denominado “eslabón más débil” posee la capacidad intrínseca de ser educado, entrenado y condicionado positivamente. No se trata de convertir a cada habitante en un ingeniero informático, sino de desarrollar criterios unificados de discernimiento frente al riesgo digital. Diversos estudios empíricos en seguridad conductual evidencian que los programas estructurados de concientización y entrenamiento interactivo basados en la simulación de riesgos reales y la retroalimentación

inmediata alteran significativamente los patrones conductuales defensivos de los individuos, reduciendo drásticamente los índices de efectividad de las estafas cibernéticas de ingeniería social (Whitman y Mattord, 2018).

Este paradigma resulta central y dota de justificación epistemológica al presente trabajo de investigación enfocado en la mitigación de ciberdelitos mediante la autoprotección en Huacho. Al implementar programas comunitarios orientados a la capacitación sobre los modus operandi de los ciberdelincuentes, el ciudadano adquiere la habilidad de identificar anomalías contextuales y técnicas básicas de verificación de fuentes.

En consecuencia, la transferencia de capacidades técnicas hacia el ámbito conductual de la ciudadanía permite mutar la condición pasiva de la víctima potencial hacia una condición activa de resiliencia. El usuario deja de ser un vector de vulnerabilidad, vulnerable al engaño y se consolida formalmente como la primera línea de defensa o un “firewall humano” dentro del entorno digital local. Esta metamorfosis cultural y formativa es el cimiento indispensable para que las políticas preventivas de ciberseguridad alcancen un impacto real, medible y sostenible en la reducción sustantiva de la incidencia delictiva informática para el año 2025.

2.2.3 Delitos informáticos

2.2.3.1. Antecedentes y evolución conceptual del término

La criminalidad informática ha experimentado una transformación significativa desde sus orígenes hasta la actualidad. Según señala la doctrina penal contemporánea, los delitos informáticos representan una categoría emergente dentro del derecho penal que responde a las necesidades de protección de bienes jurídicos en el entorno digital. Como afirma la Real Academia Española, el concepto se ha consolidado como aquellas conductas delictivas donde el medio o el fin involucra sistemas tecnológicos.

La evolución terminológica ha pasado de hablar exclusivamente de “delitos informáticos” a incorporar el concepto de “ciberdelitos”, entendiendo estos últimos como aquellas conductas criminales más estrechamente relacionadas con las redes telemáticas, mientras que los delitos informáticos constituyen una figura más ajustada a la comisión de tipos delictivos empleando las tecnologías de la información y la comunicación (Universidad de La Laguna). Esta distinción resulta fundamental para comprender la amplitud del fenómeno que enfrenta la investigación.

2.2.3.2. Definición de delitos informáticos

El vertiginoso desarrollo de las Tecnologías de la Información y la Comunicación (TIC) no solo ha dinamizado las interacciones sociales y comerciales, sino que ha originado un nuevo ecosistema para la criminalidad. Téllez (2009) define el delito informático como cualquier acto ilícito, antijurídico y culpable en el cual las computadoras, las redes de comunicación o los dispositivos electrónicos son utilizados como el instrumento fundamental, o bien, constituyen el objetivo principal del ataque. A diferencia de la delincuencia tradicional, este fenómeno trasciende el espacio físico, ubicando su esfera de acción en el ciberespacio, un entorno inmaterial donde las fronteras jurisdiccionales tradicionales carecen de operatividad directa.

La definición de delitos informáticos presenta múltiples aproximaciones doctrinales. En términos generales, pueden definirse como aquellos actos ilícitos en los que se utilizan las tecnologías de la información, como las computadoras, los programas informáticos, los medios electrónicos, el Internet, entre otros, como medio o como fin de la conducta delictiva (Justia México, 2026).

Desde una perspectiva más técnica, bajo la denominación de delitos informáticos se encuentran todas aquellas conductas antijurídicas y punibles para cuya comisión los autores se valen de medios informáticos o que atentan contra equipos informáticos (Dexia Abogados, 2024). Esta definición engloba tanto los delitos donde la tecnología es el instrumento de comisión como aquellos donde el sistema informático constituye el objeto directo de la agresión.

El Tribunal Constitucional peruano, en diversas sentencias, ha reconocido que los delitos informáticos constituyen una modalidad delictiva que afecta bienes jurídicos protegidos por la Constitución, como el derecho a la intimidad, el secreto de las comunicaciones y la seguridad jurídica en las transacciones electrónicas.

2.2.3.3. Características de los delitos informáticos

Los delitos informáticos presentan características distintivas que los diferencian de la criminalidad tradicional. Estas particularidades resultan esenciales para comprender su naturaleza y la dificultad de su persecución:

- **Uso de medios tecnológicos.** El elemento común de todos los delitos informáticos es el empleo de medios tecnológicos para vulnerar derechos ajenos, ya sea la intimidad, el patrimonio o la integridad de los datos (GPS Penal, 2025). Esta característica determina que la comisión delictiva requiera conocimientos técnicos específicos sobre el funcionamiento de los sistemas informáticos.

- **Transnacionalidad y extraterritorialidad.** Lo usual en la ejecución de ciberdelitos será la realización de “delitos a distancia”, caracterizados porque la conducta no se inicia o no tiene lugar en el mismo Estado donde se consume el resultado delictivo (SciELO Chile, 2018). Esta característica genera problemas de jurisdicción y competencia penal que dificultan la investigación y sanción de estos ilícitos.
- **Anonimato y dificultad de identificación.** El entorno digital permite que los perpetradores oculten su identidad mediante técnicas de enmascaramiento, proxy, redes Tor y otros mecanismos de anonimización, lo que constituye un desafío para las autoridades de investigación.
- **Velocidad de propagación.** Los delitos informáticos pueden cometerse y propagarse a velocidades sin precedentes, afectando simultáneamente a múltiples víctimas en distintas jurisdicciones geográficas en cuestión de segundos.
- **Ausencia de fronteras físicas.** La naturaleza intangible de los sistemas informáticos elimina las barreras geográficas tradicionales, permitiendo que un delincuente ubicado en un continente diferente pueda afectar sistemas en Perú sin necesidad de desplazamiento físico.

2.2.3.4. Delitos informáticos versus ciberdelitos: delimitación conceptual

Resulta imperativo establecer la diferencia entre delitos informáticos y ciberdelitos, pues aunque frecuentemente se utilizan como sinónimos, presentan matices diferenciadores relevantes para la investigación. Según la Asociación Iberoamericana de Derecho Comparado (AIDCA), mientras el delito informático se vale de elementos informáticos para su perpetración, el ciberdelito se refiere a una posterior generación delictiva vinculada específicamente a las tecnologías de la información y comunicaciones (AIDCA, 2024).

La postura mayoritaria de la doctrina ha considerado a los delitos informáticos más como una categoría o elemento funcional que como un tipo penal propiamente desarrollado, configurándose éstos como meros delitos comunes cometidos mediante el empleo de tecnologías de la información (Universidad de La Laguna). Sin embargo, la evolución legislativa ha reconocido la necesidad de tipificaciones específicas que respondan a la particularidad de estos ilícitos.

2.2.3.5. Marco normativo peruano: ley n° 30096

El Perú cuenta con una normativa específica para la regulación de los delitos informáticos. La ley N° 30096, Ley de delitos informáticos, promulgada el 19 de julio de 2013, constituye el cuerpo normativo principal que tipifica las conductas penalmente

relevantes que afectan los sistemas y datos informáticos, la indemnidad y libertad sexuales, la intimidad y el secreto de las comunicaciones, el patrimonio y la fe pública (IUS360, 2020).

Esta ley tiene por objeto proteger bienes jurídicos específicos del entorno digital, estableciendo penas privativas de libertad y pecuniarias para quienes cometan los ilícitos tipificados. Como señala el Congreso de la República del Perú (2013) en el texto de la norma:

El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos, suplantación de interfaces o páginas web o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años y con sesenta a ciento veinte días-multa (p. 8).

La Ley 30096 se inserta en el Código Penal peruano como Capítulo X de los Delitos Informáticos, articulándose con otras disposiciones del ordenamiento jurídico nacional e internacional, particularmente con los tratados de cooperación en materia de ciberdelincuencia.

2.2.3.6. Clasificación de los delitos informáticos según la ley n° 30096

La Ley 30096 establece una tipificación específica de conductas delictivas que puede clasificarse según el bien jurídico protegido y la modalidad de comisión. A continuación, se desarrollan los principales tipos delictivos:

- **Acceso ilícito a sistemas informáticos (artículo 2°).** El artículo 2° de la Ley 30096 tipifica el acceso indebido o ilícito a sistemas informáticos. Según la norma, el que sin estar facultado accede, intercepta o afecta datos o sistemas informáticos, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. Esta figura delictiva protege la integridad de los sistemas informáticos y la confidencialidad de la información almacenada. El bien jurídico protegido es el derecho a la privacidad y el secreto de las comunicaciones, así como la seguridad de los sistemas de información.
- ✓ **Última modificación.** El Decreto Legislativo N° 1614, publicado el 21 de diciembre de 2023, modificó este artículo para prevenir y hacer frente a la ciberdelincuencia, estableciendo agravantes cuando el acceso ilícito vulnera medidas de seguridad informática, incrementando la pena a un rango de tres a seis años de prisión efectiva (Congreso de la República, 2023).

- **Atentado contra la integridad de datos o sistemas (artículos 3° y 4°).** Los artículos 3° y 4° de la Ley 30096 sancionan conductas que afectan la integridad, disponibilidad o funcionamiento de los datos o sistemas informáticos. Estas figuras incluyen:
 - ✓ ***Daño informático.*** La destrucción, daño, alteración, supresión o inutilización de datos o programas informáticos.
 - ✓ ***Sabotaje informático.*** La introducción de virus, malware o cualquier código malicioso que afecte el funcionamiento de sistemas informáticos.

La pena establecida para estos delitos oscila entre tres y seis años de prisión efectiva, pudiendo incrementarse si se trata de sistemas de infraestructura crítica o de seguridad nacional.

- **Delitos contra la indemnidad sexual: grooming (artículo 5°).** El artículo 5° de la Ley 30096 tipifica el “grooming” o acoso sexual a menores de edad mediante tecnologías de la información. Esta figura sanciona al que mediante tecnologías de la información o comunicaciones busca obtener información sexual de menores de edad o procura encontrarse con ellos para cometer actos sexuales. Según Gálvez Monteagudo Abogados, la pena para este delito es de seis a nueve años de prisión, pudiendo reducirse a tres a seis años si la víctima tiene entre 14 y 17 años y se utiliza engaño para obtener su consentimiento. Este tipo delictivo refleja la preocupación legislativa por proteger a los menores en el entorno digital.
- **Interceptación de datos informáticos (artículo 7°).** El artículo 7° sanciona la interceptación no autorizada de datos informáticos durante su transmisión. El bien jurídico protegido es el secreto de las comunicaciones y la privacidad de la información transmitida por medios electrónicos. La pena establecida para este delito es de tres a seis años de prisión efectiva. La interceptación puede realizarse mediante técnicas de “sniffing”, ataques “man-in-the-middle” u otros mecanismos técnicos que permitan capturar datos en tránsito.
- **Fraude informático (artículo 8°).** El artículo 8° de la Ley 30096 constituye una de las figuras más relevantes por su incidencia en la práctica delictiva y su impacto económico. Según la norma legal:

“El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos, suplantación de interfaces o páginas web o cualquier interferencia o manipulación en

el funcionamiento de un sistema informático” (Congreso de la República, 2013, p. 8).

El fraude informático puede manifestarse en diversas modalidades, incluyendo:

- ✓ **Phishing.** Suplantación de identidad de entidades financieras o instituciones para obtener datos de acceso.
- ✓ **Vishing.** Phishing realizado mediante llamadas telefónicas.
- ✓ **Smishing.** Phishing mediante mensajes de texto SMS.
- ✓ **Clonación de páginas web.** Replicación de sitios legítimos para capturar información de usuarios.
- ✓ **Ingeniería social.** Manipulación psicológica para obtener información confidencial.
- **Modificación al Art. 8.** El Decreto Legislativo N° 1614 de 2023 también modificó el artículo 8°, agravando las penas cuando el fraude informático se comete contra infraestructura crítica o cuando se utilizan técnicas de suplantación de identidad (Marcasur, 2024).
- **Otros delitos informáticos tipificados.** Además de los anteriores, la Ley 30096 y su normativa complementaria tipifican:
 - ✓ **Revelación de secretos.** La divulgación no autorizada de información confidencial obtenida mediante acceso a sistemas informáticos.
 - ✓ **Espionaje informático.** El acceso a información empresarial o estatal con fines de competencia desleal o seguridad.
 - ✓ **Distribución de material de pornografía infantil.** A través de medios digitales.
 - ✓ **Acoso cibernético.** Hostigamiento sistemático mediante tecnologías de la información.

2.2.3.7. Modificaciones recientes: decreto legislativo n° 1614

El 21 de diciembre de 2023, el Poder Ejecutivo peruano promulgó el **Decreto Legislativo N° 1614**, que modifica la Ley N° 30096 con el objeto de prevenir y hacer frente a la ciberdelincuencia (Juris.pe, 2024). Esta reforma resulta fundamental para la investigación, pues actualiza las figuras delictivas ante las nuevas modalidades de criminalidad digital.

Las principales modificaciones incluyen:

1. **Agravamiento de penas** para el acceso ilícito cuando se vulneran medidas de seguridad informática.
2. **Tipificación expresa** de conductas de suplantación de identidad en medios digitales.

3. **Incorporación de protocolos** para la actuación de agentes encubiertos en entornos digitales.
4. **Coordinación institucional** entre la Policía Nacional del Perú y el Ministerio Público para la investigación de ciberdelitos.

Como señala Mazuelos Abogados (2024), estas modificaciones responden a la necesidad de actualizar el marco legal frente a la evolución de las técnicas delictivas y la creciente sofisticación de los ciberdelincuentes.

2.2.3.8. Impacto de los delitos informáticos en la sociedad

El impacto de los delitos informáticos trasciende el ámbito individual para afectar la estructura económica, social y política de los países. Según diversos estudios, la ciberdelincuencia no solo se traduce en temor e inseguridad, sino que tiene un impacto económico sustancial, afectando desde las inversiones extranjeras hasta el turismo (eBIZ Noticias, 2024).

- **Impacto económico.** La ciberdelincuencia genera pérdidas millonarias para el sector empresarial y los ciudadanos. Según datos periodísticos recientes, en el año 2024 los ciberdelincuentes robaron un total de 90 millones de soles solo en Lima Metropolitana, y en lo que va del año 2025, ya se ha reportado más de 3 millones de soles robados por estafas digitales (RPP Noticias, 2025).
Las empresas que no han implementado un enfoque sistemático en ciberseguridad corren el riesgo de enfrentar no solo pérdidas económicas y daños a su reputación, sino también sanciones legales y una disminución en su competitividad (La República, 2025).
- **Impacto social y psicológico.** Las víctimas de delitos informáticos experimentan consecuencias psicológicas significativas, incluyendo ansiedad, depresión y desconfianza en los medios digitales. El robo de identidad y la suplantación de personalidad pueden generar daños reputacionales de largo alcance que afectan la vida personal y profesional de los afectados.
- **Impacto en la seguridad nacional.** Los ataques a infraestructuras críticas (energía, agua, transporte, comunicaciones) representan una amenaza para la seguridad nacional. La vulneración de sistemas gubernamentales puede comprometer información sensible de inteligencia y defensa.
- **Magnitud del problema en el Perú.** Las estadísticas oficiales revelan una tendencia alarmante en la incidencia de delitos informáticos en el Perú. Según la Unidad Fiscal Especializada en Ciberdelincuencia, solo en el primer trimestre de 2025 ingresaron

9.193 denuncias por delitos informáticos, lo que representa un promedio de 102 casos diarios (La República, 2025).

Esta cifra representa un aumento del 129% en los últimos dos años, consolidando a los delitos informáticos como una de las principales problemáticas de seguridad ciudadana en el país. La ciudad de Lima encabeza la lista de regiones con mayor número de casos y denuncias, aunque el fenómeno se ha extendido progresivamente a regiones del interior del país.

El Instituto Nacional de Estadística e Informática (INEI) ha documentado que la sociedad peruana está experimentando un constante progreso tecnológico que supone nuevas formas de delinquir y nuevos actos ilícitos, lo que ha originado un debate en torno a la necesidad de diferenciar los delitos informáticos dentro de la estadística criminal tradicional (INEI, 2021).

2.2.3.9. Delitos informáticos y la necesidad de cultura de autoprotección

A pesar de la existencia de un marco normativo sancionador como la Ley 30096, el derecho penal posee una naturaleza fundamentalmente reactiva, interviniendo únicamente cuando el bien jurídico ya ha sido lesionado (Zaffaroni, 2000). En el contexto proyectado hacia la ciudad de Huacho para el 2025, es utópico pretender mitigar el cibercrimen confiando exclusivamente en el poder punitivo del Estado, ya que requiere complementarse con políticas de prevención basadas en la educación y sensibilización de la población.

La ciberdelincuencia en el Perú, según la Defensoría del Pueblo (2023), presenta características particulares que demandan respuestas integrales donde la autoprotección ciudadana constituye un pilar fundamental. La determinación de criterios sobre aplicabilidad de ciberseguridad basada en la cultura de autoprotección emerge entonces como una estrategia necesaria para mitigar la victimización por delitos informáticos, especialmente en contextos donde la brecha digital y la falta de alfabetización tecnológica aumentan la vulnerabilidad de la población.

Por ende, la aplicabilidad de la ciberseguridad debe abordarse desde la prevención temprana a través de una cultura de autoprotección ciudadana. Cuando el ciudadano conoce los tipos penales (como el fraude informático o la interceptación) y comprende las mecánicas delictivas que los posibilitan, desarrolla una postura crítica frente a sus propios hábitos digitales.

La legislación peruana debe servir como un respaldo jurídico, pero la reducción real de la incidencia delictiva recae en la barrera preventiva primaria: un usuario conscientemente entrenado y educado para no ceder ante la ingeniería social que precede al delito tipificado.

2.2.4 Cultura de seguridad (cultura de autoprotección ciudadana)

2.2.4.1. Antecedentes y evolución del concepto de cultura de seguridad

El concepto de cultura de seguridad tiene sus raíces en las ciencias organizacionales y la psicología del trabajo, migrando posteriormente al ámbito de la ciberseguridad ante la creciente sofisticación de las amenazas digitales. Según la Agencia de la Unión Europea para la Ciberseguridad (ENISA), citada por PricewaterhouseCoopers (PWC), la cultura de la ciberseguridad de las organizaciones se refiere a los conocimientos, hábitos, percepciones, actitudes, normas y valores de las personas en relación con la seguridad cibernética y la forma en que se manifiestan en el comportamiento de las personas con las tecnologías de la información (PWC España, 2020).

La evolución del término refleja un cambio paradigmático: de un enfoque exclusivamente tecnológico centrado en firewalls y antivirus, hacia una visión integral que reconoce al factor humano como el eslabón crítico en la cadena de seguridad. Esta transición resulta fundamental para la presente investigación, puesto que se busca determinar criterios que potencien la capacidad del ciudadano de Huacho para protegerse ante los delitos informáticos.

2.2.4.2. Definición de cultura de seguridad

La cultura de seguridad puede definirse como el conjunto de actitudes, políticas, comportamientos y conocimientos respecto a la ciberseguridad con que cuentan los individuos o colectivos (S2Grupo, 2024). Esta definición trasciende el ámbito organizacional para extenderse a la ciudadanía en general, configurándose como un marco de referencia que orienta las decisiones y acciones de las personas en el entorno digital.

De manera más específica, el Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF) de España señala que se trata de crear un ambiente en el que todo el personal es consciente de los riesgos digitales existentes y actúa de forma responsable, entendiendo que cuando todo el mundo comprende la importancia de proteger la información, se reduce considerablemente el riesgo de ataques o errores (INTEF).

Para efectos de esta investigación, la cultura de seguridad se entiende como el sistema integrado de creencias, valores, conocimientos y prácticas que posee la población de Huacho respecto a la protección de su información personal, su identidad digital y sus activos tecnológicos frente a las amenazas cibernéticas identificadas en la Ley N° 30096.

2.2.4.3. Importancia de la cultura de seguridad en la prevención de delitos informáticos

La importancia de desarrollar una cultura de seguridad robusta radica en el reconocimiento científico de que el error humano constituye el eslabón más vulnerable en la cadena de seguridad. Como señala Seguritecnia (2024), la tendencia a priorizar la comodidad sobre la seguridad conduce a comportamientos como la reutilización de contraseñas en múltiples plataformas o la selección de contraseñas sencillas y fáciles de recordar (y de quebrantar), configurando vectores de ataque explotables por los ciberdelincuentes.

La relevancia de este constructo para la investigación se manifiesta en tres dimensiones fundamentales:

Primera dimensión: reducción de la victimización. Una cultura de seguridad adecuadamente desarrollada disminuye la probabilidad de que los ciudadanos se conviertan en víctimas de los delitos informáticos tipificados en líneas anteriores, particularmente del fraude informático (Art. 8° Ley 30096) y el acceso ilícito (Art. 2°).

Segunda dimensión: empoderamiento ciudadano. La cultura de seguridad traslada la responsabilidad de la protección desde exclusivamente institucional (Policía Nacional, Ministerio Público) hacia una corresponsabilidad donde el ciudadano adquiere agencia para autoprotgerse.

Tercera dimensión: efectividad costo-beneficio. Según Panda Security (2025), instaurar una cultura de ciberseguridad resulta más efectivo que invertir exclusivamente en soluciones tecnológicas, puesto que las personas deben ser responsables de mantener un entorno seguro en línea, lo que implica conciencia, capacitación y una actitud proactiva hacia la seguridad cibernética.

2.2.4.4. Conceptualización de la cultura de autoprotección ciudadana

La autoprotección ciudadana constituye el conjunto de normas y conductas de protección que adopta una persona como sujeto independiente para su seguridad, previniendo situaciones de emergencia que puedan suponer un peligro al ciudadano (Monografías Plus). Este concepto, originado en el ámbito de la protección civil y la seguridad física, adquiere una dimensión particular cuando se traslada al entorno digital.

En el contexto de la presente investigación, la **cultura de autoprotección ciudadana digital** se define como el sistema integrado de conocimientos, actitudes, valores y prácticas comportamentales que adoptan los ciudadanos de manera autónoma y responsable para proteger su integridad física, psicológica, patrimonial y su identidad digital en el ciberespacio, mediante la identificación de riesgos, la aplicación de medidas preventivas y la respuesta adecuada ante incidentes de seguridad.

Esta conceptualización incorpora elementos del concepto original de autoprotección ciudadana desarrollado por el Ministerio del Interior de España, que señala que constituyen las acciones y procedimientos que adopta el ciudadano orientados a prevenir las amenazas sobre las personas y los bienes, configurándose como la estrategia óptima de prevención y de actuación ante situaciones de riesgo (Ministerio del Interior de España).

2.2.4.5. Dimensiones y componentes de la cultura de autoprotección ciudadana digital

La cultura de autoprotección ciudadana digital se estructura en tres componentes fundamentales interrelacionados: conocimiento, actitud y comportamiento. Esta tripartición responde a modelos teóricos de psicología social y de la salud que explican la adopción de conductas de protección.

- **Componente cognitivo: conocimiento.** El conocimiento en materia de ciberseguridad constituye la base sobre la cual se construyen las demás dimensiones de la cultura de autoprotección. Según el modelo de competencias digitales de la ciudadanía española, la alfabetización digital crítica y reflexiva implica el desarrollo de conocimientos sobre el cuidado y las responsabilidades digitales, referidos a la construcción de ambientes digitales seguros (Ministerio de Educación de Chile, 2025).

Este componente cognitivo incluye:

- a. ***Conocimiento sobre amenazas.*** Identificación de los diferentes tipos de delitos informáticos (fraude informático, phishing, malware, grooming) y sus modalidades de ejecución.
- b. ***Conocimiento técnico básico.*** Comprensión de mecanismos de protección como contraseñas seguras, autenticación de dos factores, encriptación y configuraciones de privacidad.
- c. ***Conocimiento sobre derechos digitales.*** Conocimiento de los derechos de protección de datos personales y las vías de denuncia ante la comisión de delitos informáticos.
- d. ***Conocimiento sobre huella digital.*** Comprensión de la persistencia de los datos en el entorno digital y las implicaciones de la exposición pública de información personal.

Según Meliá (2007), en el contexto de la seguridad basada en el comportamiento, el conocimiento debe traducirse en comportamientos observables y medibles que permitan establecer indicadores de protección efectiva.

- **Componente afectivo-evaluativo: actitud.** La actitud hacia la ciberseguridad se refiere al conjunto de predisposiciones psicológicas evaluativas que orientan la

conducta del ciudadano frente a los riesgos digitales. Este componente incluye percepciones, creencias y valores compartidos sobre la importancia de la protección en el entorno digital.

La Agencia de la Unión Europea para la Ciberseguridad (ENISA), citada por PWC España (2020), enfatiza que la cultura de ciberseguridad abarca las percepciones, actitudes y valores de las personas respecto a la seguridad cibernética. Estas actitudes se manifiestan en la valoración que el individuo hace de la gravedad de las amenazas y de su propia vulnerabilidad ante ellas.

Desde la perspectiva de la Teoría de la Motivación de Protección (Protection Motivation Theory - PMT), desarrollada por Rogers (1983) y aplicada recientemente al contexto de ciberseguridad por investigadores latinoamericanos, la actitud de protección se construye mediante la evaluación de la severidad de la amenaza y la probabilidad de ocurrencia, así como la evaluación de la eficacia de las respuestas de autoprotección disponibles (Revista de Investigación Educativa de la REDIECH, 2024).

Las actitudes fundamentales en la cultura de autoprotección ciudadana digital incluyen:

- a. ***Percepción de vulnerabilidad.*** Conciencia de que cualquier persona puede ser víctima de delitos informáticos, superando la ilusión de invulnerabilidad.
- b. ***Valoración de la privacidad.*** Consideración de la información personal como un activo valioso que merece protección.
- c. ***Responsabilidad personal.*** Asunción de que la protección digital es una obligación individual y no exclusivamente estatal o institucional.
- d. ***Desconfianza saludable.*** Actitud de escepticismo ante comunicaciones no solicitadas, ofertas demasiado ventajosas y solicitudes de información personal.
- **Componente conductual: comportamiento digital seguro.** El comportamiento digital seguro constituye la manifestación observable de la cultura de autoprotección, resultante de la interacción entre el conocimiento y las actitudes en un contexto determinado. Según el Observatorio de Economía de la Conducta, las intervenciones conductuales más efectivas para incrementar el nivel de ciberseguridad son aquellas que logran modificar patrones de comportamiento establecidos. El comportamiento digital seguro incluye prácticas específicas como:
 - a. ***Higiene digital.*** Actualización regular de software, uso de antivirus, revisión periódica de configuraciones de privacidad.

- b. **Gestión de credenciales.** Uso de contraseñas robustas y únicas, activación de autenticación multifactor, no compartir credenciales de acceso.
- c. **Navegación segura.** Verificación de certificados de seguridad en sitios web, evitación de redes Wi-Fi públicas para transacciones sensibles, verificación de remitentes en comunicaciones electrónicas.
- d. **Gestión de la identidad digital.** Control de la información compartida en redes sociales, configuración de privacidad restrictiva, limitación de la exposición pública de datos personales.
- e. **Respuesta ante incidentes.** Conocimiento de procedimientos de denuncia ante delitos informáticos, respaldo de información importante, desconexión inmediata ante sospecha de compromiso de seguridad.

Según 3Digits, el análisis conductual (Behavioral Analysis) en ciberseguridad permite anticipar posibles movimientos de los atacantes y desarrollar contramedidas efectivas, pero también permite identificar patrones de comportamiento seguro que pueden ser replicados por la ciudadanía.

2.2.4.6. Autoprotección digital: conceptualización específica.

La autoprotección digital representa la aplicación específica del concepto de autoprotección ciudadana al entorno cibernético. Se define como el conjunto de precauciones, medidas y comportamientos que adopta el ciudadano para garantizar su seguridad en los medios electrónicos y el ciberespacio (Gobierno de Canarias).

Esta conceptualización se articula con el concepto de ciudadanía digital, definida por Wikipedia (2026) como la capacidad de utilizar los recursos digitales de manera segura, ética y consciente, respetando los derechos fundamentales y comprendiendo tanto las oportunidades como los riesgos del entorno en línea.

- **Elementos constitutivos de la autoprotección digital.** La autoprotección digital se compone de los siguientes elementos:
 - a. **Conciencia situacional.** Capacidad de identificar situaciones de riesgo en el entorno digital, reconociendo señales de alerta como solicitudes de información sensible, enlaces sospechosos o comunicaciones de remitentes desconocidos.
 - b. **Competencias técnicas básicas.** Habilidades operativas para implementar medidas de protección como configuración de privacidad, gestión de contraseñas, identificación de sitios seguros.

- c. **Competencias socioemocionales.** Capacidad para resistir la manipulación psicológica (ingeniería social), gestionar el estrés ante posibles amenazas y mantener la calidad del juicio en situaciones de presión.
- d. **Competencias ético-legales.** Conocimiento de las normas de conducta en el ciberespacio, comprensión de las consecuencias legales de las acciones propias y ajenas, respeto por los derechos de terceros en el entorno digital.
- **Modelo de autoprotección digital basado en la teoría de la motivación de protección.** La Teoría de la Motivación de Protección (Protection Motivation Theory - PMT), desarrollada originalmente por Rogers (1983) y aplicada al contexto de ciberseguridad en investigaciones recientes, proporciona un marco teórico robusto para comprender la autoprotección digital. Según este modelo, la intención de protección y el comportamiento de autoprotección resultan de dos procesos evaluativos:
 - a. **Evaluación de la amenaza.** El ciudadano evalúa la severidad de las consecuencias potenciales de los delitos informáticos (percepción de severidad) y la probabilidad de que ocurra un incidente que le afecte (percepción de vulnerabilidad).
 - b. **Evaluación del afrontamiento.** El ciudadano evalúa la eficacia de las medidas de autoprotección disponibles (eficacia de la respuesta) y su propia capacidad para implementarlas (autoeficacia).

Como señalan los investigadores de la Revista de Investigación Educativa de la REDIECH (2024), la conciencia de ciberseguridad influye positivamente en la eficacia de respuesta, y el hábito de protección se define como la tendencia a realizar comportamientos de seguridad de forma automática debido al refuerzo continuo.

2.2.4.7. Relación entre cultura de autoprotección y mitigación de delitos informáticos

La presente investigación postula que existe una relación inversa entre el nivel de desarrollo de la cultura de autoprotección ciudadana digital y la incidencia de victimización por delitos informáticos. Esta relación se fundamenta en los siguientes mecanismos:

- **Mecanismo de prevención primaria.** Una cultura de autoprotección desarrollada reduce la exposición a situaciones de riesgo, disminuyendo la probabilidad de que los ciberdelincuentes identifiquen víctimas potenciales vulnerables. Como señala el Banco Interamericano de Desarrollo (BID, 2022), los ciudadanos digitales éticos no solo evitan conductas dañinas, sino que también denuncian y se oponen activamente a comportamientos perjudiciales cuando los encuentran.

- **Mecanismo de detección temprana.** La cultura de autoprotección sensibiliza al ciudadano para identificar intentos de fraude informático, phishing y otras modalidades delictivas en etapas tempranas, permitiendo abortar el ataque antes de que se concrete el daño patrimonial o personal.
- **Mecanismo de resiliencia.** Ante la materialización de un delito informático, los ciudadanos con cultura de autoprotección poseen mayor capacidad de respuesta: conocen los canales de denuncia, tienen respaldos de información, y pueden minimizar las consecuencias del incidente.
- **Mecanismo de efecto disuasivo colectivo.** Cuando la cultura de autoprotección se extiende a la comunidad, se eleva el nivel general de protección, incrementando el esfuerzo requerido por los ciberdelincuentes para encontrar víctimas vulnerables, lo que puede desplazar la actividad delictiva hacia otras zonas geográficas o hacia otros modus operandi.

2.2.4.8. Contextualización al ámbito de huacho, 2025

La determinación de criterios sobre aplicabilidad de ciberseguridad basada en cultura de autoprotección ciudadana adquiere particular relevancia en el contexto de Huacho, provincia de Huaura, departamento de Lima, en el año 2025.

- **Contexto digital de Huacho.** Huacho, como capital de provincia y zona de influencia regional, presenta características específicas que impactan la cultura de autoprotección:
 - a. **Brecha digital.** Posibles asimetrías en el acceso y uso de tecnologías que pueden generar desigualdades en la exposición a riesgos y en la capacidad de autoprotección.
 - b. **Crecimiento del comercio electrónico.** La expansión de transacciones digitales en el contexto provincial incrementa la exposición a riesgos de fraude informático.
 - c. **Uso intensivo de redes sociales.** La comunicación digital constituye un pilar de la interacción social, generando riesgos asociados a la exposición de información personal.
- **Factores que condicionan la cultura de autoprotección en Huacho.**
 - a. **Factores facilitadores.**
 - ✓ Creciente conciencia sobre delitos informáticos mediada por noticias de victimización
 - ✓ Disponibilidad de información sobre ciberseguridad a través de medios digitales
 - ✓ Existencia de normativa clara (Ley 30096) que tipifica conductas sancionables

b. Factores limitantes.

- ✓ Posible escasez de programas de capacitación sistemática en ciberseguridad dirigidos a la ciudadanía
- ✓ Dependencia de dispositivos móviles con posibles vulnerabilidades de seguridad
- ✓ Posible subestimación de riesgos por parte de la población (sesgo de optimismo)

2.2.4.9. Marco integrador: de la cultura de seguridad a la autoprotección efectiva

El desarrollo de una cultura de autoprotección ciudadana digital efectiva requiere la articulación de los tres componentes (conocimiento, actitud, comportamiento) en un modelo integrador que considere:

- **Educación continua.** Programas de formación no puntuales sino sostenidos en el tiempo, que actualicen los conocimientos ante la evolución de las técnicas delictivas.
- **Diseño de entornos favorables.** Configuración por defecto de dispositivos y servicios con niveles óptimos de seguridad, reduciendo la carga cognitiva sobre el usuario.
- **Feedback y reforzamiento.** Sistemas de retroalimentación que reconozcan y refuercen los comportamientos de protección, generando hábitos automatizados.
- **Participación comunitaria.** Construcción de redes de apoyo entre ciudadanos para la identificación y denuncia de intentos de delitos informáticos.

Según Computer Weekly (2022), una cultura de ciberseguridad es aquella que abarca a toda la organización (y por extensión, a la comunidad), a través de equipos, procesos, métricas y herramientas, incorporando atributos y mejores prácticas que reducen el riesgo de incidentes.

2.2.5 Factor humano (como principal vulnerabilidad - objetivo vulnerable)

2.2.5.1. El factor humano como eslabón débil en la ciberseguridad

La ciberseguridad tradicional ha privilegiado históricamente el desarrollo de soluciones tecnológicas como los firewalls, antivirus, sistemas de detección de intrusiones, operando bajo el supuesto de que la tecnología constituye el principal escudo contra las amenazas digitales. Sin embargo, la evidencia empírica acumulada durante las últimas dos décadas ha demostrado de manera contundente que el factor humano representa la vulnerabilidad más crítica y explotable en la cadena de seguridad.

Según el Observatorio de Economía de la Conducta, el error humano es un factor significativo en las brechas de seguridad, manifestado en comportamientos como la

priorización de la comodidad sobre la seguridad, la reutilización de contraseñas en múltiples plataformas o la selección de contraseñas sencillas y fáciles de recordar (y de quebrantar).

Esta realidad cobra particular relevancia para la presente investigación, dado que busca precisamente fortalecer la capacidad del ciudadano de Huacho para convertirse de víctima potencial en agente activo de su propia protección.

El factor humano en ciberseguridad puede definirse como el conjunto de características psicológicas, cognitivas, conductuales y sociales de los individuos que determinan su susceptibilidad ante ataques cibernéticos, así como su capacidad para identificar, prevenir y responder adecuadamente a las amenazas digitales. Esta definición trasciende la mera consideración del error técnico para incorporar dimensiones motivacionales, perceptuales y decisionales que explican por qué los ciudadanos, aun conociendo los riesgos, toman decisiones que los exponen a la victimización por delitos informáticos.

2.2.5.2. Comportamiento del usuario: teorías explicativas de la toma de riesgos en línea

La comprensión del comportamiento de riesgo en línea requiere la incorporación de marcos teóricos provenientes de la psicología social, la psicología cognitiva y la economía conductual. A continuación, se desarrollan las principales teorías que explican por qué las personas asumen riesgos en el entorno digital, configurándose como objetivos vulnerables para los ciberdelincuentes.

- **Sesgo de optimismo y falta de percepción de vulnerabilidad.** El sesgo de optimismo, descrito inicialmente por Weinstein (1980) y aplicado posteriormente al contexto de ciberseguridad, se refiere a la tendencia sistemática de los individuos a creer que son menos propensos a experimentar eventos negativos que otras personas. En el ámbito digital, este sesgo se manifiesta cuando el ciudadano considera que los delitos informáticos (phishing, fraude informático, robo de identidad) le afectan a otros, pero no a él mismo.

Según la Teoría de la Motivación de Protección (Protection Motivation Theory - PMT) desarrollada por Rogers (1983) y aplicada al contexto de ciberseguridad en investigaciones recientes latinoamericanas, la intención de protección depende crucialmente de la evaluación de la amenaza. Cuando el individuo subestima su vulnerabilidad (baja percepción de vulnerabilidad), disminuye significativamente la probabilidad de que adopte comportamientos protectores. Como señalan los investigadores de la Revista de Investigación Educativa de la REDIECH (2024), la conciencia de ciberseguridad influye positivamente en la eficacia de respuesta, lo que

implica que la falta de percepción de riesgo debilita la motivación para la autoprotección.

Este fenómeno explica por qué ciudadanos que conocen teóricamente los delitos informáticos (incluso pueden describir modalidades como el phishing o el fraude) no implementan medidas de protección, operando bajo la creencia ilusoria de que “a mí no me va a pasar”. El sesgo de optimismo constituye, por tanto, un factor explicativo central de la victimización por delitos informáticos en contextos como Huacho, donde la familiaridad con la tecnología puede generar falsa confianza en la propia invulnerabilidad.

- **Teoría del procesamiento elaborado y heurístico.** La Teoría del Modelo de Elaboración Likelihood (Elaboration Likelihood Model - ELM), desarrollada por Petty y Cacioppo (1986), resulta pertinente para comprender por qué los ciudadanos procesan de manera superficial las señales de riesgo en el entorno digital. Según esta teoría, cuando los individuos carecen de motivación o capacidad para procesar información compleja, recurren a atajos cognitivos (heurísticos) que, aunque eficientes, pueden generar decisiones subóptimas.

En el contexto de los delitos informáticos, el ciudadano de Huacho frente a una comunicación electrónica que solicita información sensible puede no realizar un análisis profundo de la legitimidad del mensaje (vía central de procesamiento), sino que se basa en atajos como la apariencia profesional del correo, el logo institucional o el tono de urgencia (vía periférica). Este procesamiento heurístico facilita el éxito de técnicas de ingeniería social empleadas por ciberdelincuentes, quienes diseñan sus ataques específicamente para activar estos atajos cognitivos.

- **Teoría del comportamiento planificado.** La Teoría del Comportamiento Planificado (Theory of Planned Behavior - TPB), desarrollada por Ajzen (1991), postula que el comportamiento está determinado por la intención conductual, la cual a su vez es función de tres componentes: actitud hacia el comportamiento, norma subjetiva y control conductual percibido. Aplicada al contexto de ciberseguridad, esta teoría explica por qué los ciudadanos pueden mantener actitudes positivas hacia la protección digital pero no traducirlas en comportamiento efectivo.

El control conductual percibido resulta particularmente relevante: cuando el ciudadano considera que implementar medidas de seguridad (contraseñas complejas, autenticación multifactor, verificación constante de remitentes) excede sus capacidades técnicas o demanda esfuerzos inaceptables, disminuye la intención de

comportamiento protector, aun cuando exista actitud favorable hacia la seguridad. Esta barrera percibida entre intención y comportamiento constituye un objetivo de intervención para la presente investigación.

- **Teoría prospectiva y aversión a la pérdida.** La Teoría Prospectiva de Kahneman y Tversky (1979), fundamental en la economía conductual, demuestra que los individuos evalúan las pérdidas y ganancias de manera asimétrica, mostrando mayor aversión a las pérdidas que motivación equivalente por ganancias similares. Sin embargo, en el contexto de ciberseguridad, se observa una paradoja: los ciudadanos subestiman sistemáticamente la probabilidad de pérdida (victimización por delito informático) y sobreestiman el costo de las medidas preventivas (tiempo, esfuerzo cognitivo, incomodidad).

Según el Observatorio de Economía de la Conducta, la tendencia a priorizar la comodidad sobre la seguridad conduce a comportamientos de riesgo. Esta asimetría explica por qué, aun cuando los ciudadanos reconocen potencialmente las consecuencias de un fraude informático o un robo de identidad, el comportamiento inmediato se orienta hacia la minimización de esfuerzo (contraseñas simples, aceptación de términos sin lectura, clic en enlaces sin verificación) en detrimento de la protección.

- **Teoría de la carga cognitiva y fatiga de seguridad.** La Teoría de la Carga Cognitiva (Cognitive Load Theory), desarrollada por Sweller (1988), sostiene que la capacidad de procesamiento de información del ser humano es limitada. En el contexto digital contemporáneo, donde los ciudadanos enfrentan múltiples demandas de atención simultáneas, la carga cognitiva asociada a la verificación constante de seguridad genera fatiga de seguridad (security fatigue).

Esta fatiga se manifiesta en la reducción progresiva de la vigilancia ante señales de riesgo, la automatización de respuestas sin verificación y la adopción de atajos que comprometen la seguridad. Para el contexto de Huacho, donde el uso de dispositivos móviles y la conectividad han crecido exponencialmente, la fatiga de seguridad constituye un factor explicativo relevante de la vulnerabilidad humana ante delitos informáticos.

2.2.5.3. Teoría de las actividades rutinarias: el ciudadano como objetivo vulnerable

La Teoría de las Actividades Rutinarias (Routine Activity Theory - RAT), desarrollada por Cohen y Felson en 1979, constituye uno de los marcos teóricos más

influyentes en la criminología contemporánea y resulta particularmente pertinente para comprender la victimización por delitos informáticos en el contexto de la presente investigación.

- **Fundamentos de la Teoría.** La Teoría de las Actividades Rutinarias postula que la ocurrencia del delito no requiere de un delincuente patológico o de condiciones sociales estructurales profundas, sino que emerge de la convergencia espacio-temporal de tres elementos fundamentales en el curso de las actividades cotidianas:
 1. **Una persona motivada para cometer un delito** (delincuente motivado)
 2. **Un objetivo adecuado** (víctima potencial)
 3. **La ausencia de un guardián competente** (ausencia de control)

Según Cohen y Felson (1979), la estructura de las actividades rutinarias de la vida cotidiana crea oportunidades para el delito cuando estos tres elementos convergen. La teoría enfatiza que los cambios en los patrones de actividad social (trabajo, ocio, interacción) modifican las oportunidades delictivas de manera más significativa que las características individuales de los delincuentes.

- **Aplicación al ciberespacio y los delitos informáticos.** La aplicación de la Teoría de las Actividades Rutinarias al ciberespacio ha sido desarrollada por criminólogos como Yar (2005) y Reyns (2013), quienes han demostrado que la estructura de la teoría mantiene validez explicativa en el entorno digital, aunque requiere adaptaciones conceptuales.
 - a. ***El delincuente motivado en el ciberespacio.*** En el contexto de los delitos informáticos tipificados en la Ley N° 30096 (fraude informático, acceso ilícito, interceptación de datos), el delincuente motivado no requiere desplazamiento físico hacia Huacho para afectar a sus ciudadanos. La conectividad global permite que delincuentes ubicados en cualquier punto del planeta converjan espacio-temporalmente con víctimas en el contexto ciudadano mediante plataformas digitales. Esta deslocalización del delito incrementa exponencialmente la oferta de delincuentes potenciales.
 - b. ***El objetivo adecuado (víctima potencial).*** El ciudadano de Huacho que carece de cultura de autoprotección digital se configura como objetivo adecuado desde la perspectiva de la teoría. La adecuación del objetivo se determina por características como:

- ✓ **Visibilidad.** Presencia activa en redes sociales, plataformas de comercio electrónico y servicios bancarios en línea que expone información personal y patrones de comportamiento.
- ✓ **Accesibilidad.** Disponibilidad de canales de contacto (correo electrónico, mensajería instantánea, redes sociales) que permiten la aproximación del delincuente.
- ✓ **Atractivo.** Valor percibido de la información o recursos que posee el ciudadano (datos bancarios, información personal, credenciales de acceso).
- ✓ **Vulnerabilidad.** Ausencia de medidas de protección que dificulten el éxito del ataque (contraseñas débiles, falta de verificación de identidad, desconocimiento de señales de alerta).

Según la teoría, cuando el ciudadano presenta alta visibilidad, accesibilidad y atractivo, combinado con baja capacidad de protección, se constituye en objetivo altamente adecuado para el delito informático.

- c. ***La ausencia de guardián competente.*** Tradicionalmente, la teoría identifica tres tipos de guardianes: guardianes formales (policía, autoridades), guardianes informales (vecinos, familiares) y guardianes personales (autoprotección). En el ciberespacio, la ausencia de guardián competente se manifiesta en múltiples niveles:
- ✓ **Nivel institucional.** Limitaciones en la capacidad de investigación y respuesta de las autoridades especializadas ante delitos transnacionales.
 - ✓ **Nivel comunitario.** Ausencia de redes de alerta y apoyo entre ciudadanos para la identificación y denuncia de intentos de delitos informáticos.
 - ✓ **Nivel individual.** Carencia de conocimientos, actitudes y comportamientos de autoprotección que funcionarían como guardianes personales.

La convergencia de estos tres elementos (delincuente motivado globalmente conectado, ciudadano como objetivo adecuado vulnerable, y ausencia de guardianes competentes) explica la elevada tasa de victimización por delitos informáticos documentada en el Perú y, específicamente, proyectada para el contexto de Huacho en 2025.

- **Implicaciones para la investigación: transformación del objetivo vulnerable.** La Teoría de las Actividades Rutinarias tiene implicaciones directas para la presente investigación. Si la victimización emerge de la convergencia del delincuente motivado, el objetivo adecuado y la ausencia de guardián, entonces las intervenciones pueden dirigirse a modificar los factores controlables: la adecuación del objetivo y la presencia de guardianes.

La determinación de criterios sobre aplicabilidad de ciberseguridad basada en cultura de autoprotección ciudadana responde precisamente a esta lógica teórica: mediante el fortalecimiento del conocimiento, las actitudes y los comportamientos de autoprotección, se reduce la vulnerabilidad del ciudadano (disminuyendo su adecuación como objetivo) y se incrementa la presencia de guardianes personales. Según la teoría, pequeñas modificaciones en las actividades rutinarias (verificación de remitentes, no clic en enlaces sospechosos, uso de contraseñas robustas) pueden alterar significativamente la convergencia espacio-temporal que facilita el delito, desplazando al ciudadano de la categoría de “objetivo adecuado” hacia la categoría de “objetivo protegido”.

2.2.5.4. Modelo integrador de vulnerabilidad humana en ciberseguridad

La integración de las teorías presentadas permite construir un modelo explicativo de la vulnerabilidad humana ante delitos informáticos que articula factores individuales, situacionales y estructurales.

- **Nivel individual: factores psicológicos y cognitivos.** En el nivel individual, la vulnerabilidad se explica por la interacción de:
 - ✓ ***Sesgos cognitivos.*** Optimismo sesgado, ilusión de control, efecto de inmediatez (preferencia por recompensas inmediatas sobre protección futura).
 - ✓ ***Limitaciones cognitivas.*** Carga cognitiva elevada, fatiga de seguridad, procesamiento heurístico superficial.
 - ✓ ***Características motivacionales.*** Baja motivación de protección debida a subestimación de riesgo, alta aversión al esfuerzo de protección.
 - ✓ ***Capacidades técnicas.*** Deficiencias en alfabetización digital que limitan la capacidad de identificar amenazas y aplicar contramedidas.
- **Nivel situacional: contexto de exposición digital.** El nivel situacional considera las características del entorno digital que incrementan la exposición:
 - ✓ ***Hiperconectividad.*** Uso simultáneo de múltiples plataformas y dispositivos que fragmenta la atención y reduce la vigilancia.
 - ✓ ***Diseño persuasivo.*** Interfaces tecnológicas diseñadas para maximizar la engagement que pueden generar comportamientos impulsivos.

- ✓ **Ingeniería social sofisticada.** Técnicas de manipulación psicológica cada vez más elaboradas que explotan vulnerabilidades emocionales (miedo, urgencia, curiosidad).
- ✓ **Entorno de confianza.** Plataformas legítimas que generan expectativas de seguridad que pueden transferirse indebidamente a comunicaciones fraudulentas.
- **Nivel estructural: contexto socio-tecnológico.** El nivel estructural abarca factores macrosociales:
 - ✓ **Brecha digital.** Desigualdades en acceso a educación digital de calidad que generan asimetrías en capacidades de protección.
 - ✓ **Marco regulatorio.** Existencia de normativa (Ley 30096) que, sin embargo, puede no traducirse en protección efectiva sin apropiación ciudadana.
 - ✓ **Economía del cibercrimen.** Bajo costo y alto retorno de los delitos informáticos que genera abundancia de delincuentes motivados.
 - ✓ **Globalización digital.** Ausencia de fronteras que dificulta la aplicación de controles jurisdiccionales tradicionales.

2.2.5.5. *Prevención digital: medidas, hábitos y buenas prácticas*

Frente a la vulnerabilidad del factor humano, la prevención digital constituye el conjunto de medidas, hábitos y buenas prácticas que el ciudadano puede implementar para reducir su adecuación como objetivo delictivo y aumentar su capacidad de autoprotección. Estas prácticas se articulan con la cultura de autoprotección ciudadana desarrollada en el punto anterior.

- **Dimensiones de la prevención digital.** Según el Ministerio del Interior de España, la autoprotección constituye la estrategia óptima de prevención y de actuación ante situaciones de riesgo. Trasladado al ámbito digital, la prevención comprende tres dimensiones interrelacionadas:
 - ✓ **Prevención primaria.** Orientada a reducir la probabilidad de exposición a delitos informáticos mediante la adopción de comportamientos que disminuyen la visibilidad y accesibilidad del ciudadano como objetivo potencial.
 - ✓ **Prevención secundaria.** Dirigida a detectar tempranamente intentos de victimización, abortando el ataque antes de que se concrete el daño.
 - ✓ **Prevención terciaria.** Referida a la respuesta post-victimización que minimiza el impacto y previene la revictimización.

- **Medidas técnicas de prevención.** Las medidas técnicas constituyen el primer nivel de protección y comprenden prácticas instrumentales:
 - a. ***Gestión de credenciales de acceso.***
 - ✓ Uso de contraseñas robustas (mínimo 12 caracteres, combinación de mayúsculas, minúsculas, números y símbolos)
 - ✓ Unicidad de contraseñas (no reutilización entre plataformas)
 - ✓ Implementación de autenticación multifactor (MFA) siempre que esté disponible
 - ✓ Uso de gestores de contraseñas para facilitar el cumplimiento de las prácticas anteriores
 - b. ***Protección de dispositivos.***
 - ✓ Mantenimiento de sistemas operativos y aplicaciones actualizados
 - ✓ Instalación y mantenimiento de soluciones antivirus/antimalware
 - ✓ Configuración de cortafuegos personales
 - ✓ Desactivación de funciones innecesarias que expanden la superficie de ataque
 - c. ***Navegación segura.***
 - ✓ Verificación de certificados de seguridad (HTTPS) en sitios web
 - ✓ No ingreso de información sensible en redes Wi-Fi públicas no seguras
 - ✓ Uso de redes privadas virtuales (VPN) cuando se requiere privacidad
 - ✓ Verificación de URLs antes de realizar clic en enlaces
- **Hábitos conductuales de prevención.** Más allá de las medidas técnicas, los hábitos conductuales reflejan la internalización de la cultura de autoprotección:
 - a. ***Hábito de verificación.*** Tendencia automática a verificar la legitimidad de comunicaciones antes de responder o hacer clic. Incluye:
 - ✓ Verificación de remitentes en correos electrónicos
 - ✓ Confirmación telefónica de solicitudes inusuales
 - ✓ Escaneo visual de señales de alerta (errores ortográficos, urgencia excesiva, solicitudes de información sensible)
 - b. ***Hábito de confidencialidad.*** Práctica consistente de no compartir información personal o credenciales de acceso, incluso ante presiones sociales o comunicaciones aparentemente institucionales.
 - c. ***Hábito de respaldo.*** Realización periódica de copias de seguridad de información importante, facilitando la recuperación ante incidentes de ransomware o pérdida de datos.

- d. ***Hábito de actualización.*** Tendencia a mantenerse informado sobre nuevas modalidades de delitos informáticos y actualizar prácticas de protección correspondientemente.
- **Buenas Prácticas en Comunicación Digital.** Las buenas prácticas en comunicación digital abordan específicamente los vectores más comunes de ataque:
 - a. ***Gestión del correo electrónico.***
 - ✓ No apertura de archivos adjuntos de remitentes desconocidos
 - ✓ No clic en enlaces sin verificación previa (hover para visualizar URL real)
 - ✓ Desconfianza ante mensajes que generan urgencia o amenaza
 - ✓ Verificación independiente de comunicaciones bancarias o institucionales
 - b. ***Uso de redes sociales.***
 - ✓ Configuración de privacidad restrictiva
 - ✓ Limitación de información personal visible públicamente
 - ✓ Desconfianza ante solicitudes de amistad de perfiles desconocidos
 - ✓ No publicación de información que facilite respuestas a preguntas de seguridad
 - c. ***Transacciones en línea.***
 - ✓ Uso exclusivo de plataformas reconocidas y seguras
 - ✓ Verificación de sellos de seguridad y certificados
 - ✓ No realización de transacciones desde dispositivos públicos o redes inseguras
 - ✓ Registro y conservación de comprobantes de transacciones
- **Respuesta ante Incidentes de Seguridad.** Aun con la implementación de medidas preventivas, la posibilidad de victimización persiste. Las buenas prácticas de respuesta incluyen:
 - a. ***Detección temprana.*** Revisión periódica de estados de cuenta, alertas de acceso a cuentas, y comportamientos anómalos en dispositivos (lentitud, ventanas emergentes).
 - b. ***Contención inmediata.*** Desconexión de dispositivos de internet ante sospecha de compromiso, cambio inmediato de credenciales afectadas.
 - c. ***Denuncia y reporte.*** Conocimiento y uso de canales de denuncia ante delitos informáticos (Policía Nacional del Perú, Ministerio Público Fiscalía Especializada en Ciberdelincuencia).
 - d. ***Recuperación.*** Restauración desde respaldos, notificación a entidades bancarias si corresponde, y monitoreo de posible uso fraudulento de información comprometida.

2.2.5.6. Integración con el marco de ciberseguridad basada en cultura de autoprotección

El desarrollo del punto sobre factor humano y prevención digital se articula directamente con el objetivo central de la presente investigación: la determinación de criterios sobre aplicabilidad de ciberseguridad basada en cultura de autoprotección ciudadana.

- **De la vulnerabilidad a la resiliencia.** La comprensión teórica del factor humano como vulnerabilidad permite diseñar intervenciones que transformen al ciudadano de objetivo vulnerable en ciudadano resiliente. Esta transformación requiere:
 - ✓ **Reducción del sesgo de optimismo.** Intervenciones que incrementen la percepción realista de vulnerabilidad sin generar parálisis por ansiedad.
 - ✓ **Desarrollo de capacidades.** Formación que incremente el control conductual percibido, reduciendo la brecha entre intención y comportamiento.
 - ✓ **Automatización de hábitos protectores.** Diseño de intervenciones que generen hábitos de seguridad que operen automáticamente, reduciendo la dependencia de la atención consciente.
 - ✓ **Fortalecimiento de guardianes.** Desarrollo de capacidades de autoprotección que funcionen como guardianes personales, complementando la protección institucional.
- **Relevancia para el contexto de Huacho, 2025.** Para el contexto específico de Huacho, la vulnerabilidad del factor humano presenta características particulares que deben considerarse en la determinación de criterios:
 - ✓ **Transición digital acelerada.** El rápido crecimiento del uso de tecnologías financieras y de comunicación puede generar brechas entre adopción tecnológica y desarrollo de capacidades de protección.
 - ✓ **Diversidad de perfiles de usuario.** Desde usuarios nativos digitales hasta adultos mayores en proceso de alfabetización digital, requiriendo estrategias diferenciadas.
 - ✓ **Tejido social comunitario.** La existencia de redes sociales sólidas en el contexto provincial puede facilitar la construcción de guardianes informales de seguridad digital.
 - ✓ **Acceso a recursos de soporte.** Limitaciones potenciales en acceso a soporte técnico especializado que incrementan la relevancia de la autoprotección.

2.2.5.7. Conclusión del capítulo: el factor humano como eje de intervención

El factor humano constituye simultáneamente la principal vulnerabilidad y la mayor oportunidad en el sistema de ciberseguridad. La evidencia teórica y empírica revisada

demuestra que los delitos informáticos tipificados en la Ley N° 30096 encuentran en el comportamiento humano su vector de ataque más efectivo, pero también encuentran en la cultura de autoprotección ciudadana su contramedida más sustentable.

La Teoría de las Actividades Rutinarias proporciona el marco explicativo para comprender por qué los ciudadanos de Huacho se constituyen en objetivos vulnerables, mientras que las teorías del comportamiento de riesgo ofrecen las claves para diseñar intervenciones que modifiquen las percepciones, actitudes y comportamientos que facilitan la victimización.

La determinación de criterios de ciberseguridad basada en cultura de autoprotección ciudadana, objeto de la presente investigación, emerge entonces como respuesta científica y socialmente pertinente al desafío de mitigar los delitos informáticos mediante la transformación del factor humano de eslabón débil a agente activo de protección.

2.2.6 Derecho informático, derechos digitales y comportamiento preventivo

2.2.6.1. El derecho informático: conceptualización y naturaleza preventiva

El Derecho Informático no se limita a ser una rama sancionadora, sino que constituye un ecosistema normativo transversal que regula los efectos jurídicos derivados de la interacción humana con las Tecnologías de la Información y la Comunicación (TIC). Según Téllez Valdés (2017), esta disciplina tiene una doble vertiente: por un lado, protege los bienes jurídicos inmateriales (como los datos y la identidad digital) y, por otro, establece un marco de actuación para reprimir la cibercriminalidad. Sin embargo, desde una perspectiva sociológica del derecho, la norma por sí sola es ineficaz si los ciudadanos que debe proteger desconocen su existencia y no adoptan conductas de salvaguarda.

2.2.6.2. Marco legal peruano frente a los delitos informáticos

En el Perú, la principal herramienta punitiva contra la cibercriminalidad es la Ley N.º 30096, ley de delitos informáticos (promulgada en 2013 y modificada por la Ley N.º 30171). Esta normativa tipifica conductas ilícitas como el acceso ilícito a sistemas, el fraude informático, la suplantación de identidad y la interceptación de datos corporativos o personales.

Caro John (2018) señala que, aunque la legislación peruana es dogmáticamente sólida, adolece de una naturaleza eminentemente reactiva; es decir, el aparato estatal (Policía Nacional, Ministerio Público) se activa únicamente cuando el daño patrimonial o moral ya se ha consumado. En este sentido, la ley no previene el delito. Por consiguiente, la efectividad del marco normativo requiere inexorablemente de la cultura de autoprotección

ciudadana como primera barrera preventiva, limitando las oportunidades para que el delincuente materialice el tipo penal.

2.2.6.3. Convenios internacionales: el convenio de budapest

A nivel supranacional, la ciberseguridad y el Derecho Informático se unifican mediante el convenio sobre la ciberdelincuencia o Convenio de Budapest (2001), al cual el Perú se adhirió formalmente en 2019. Este tratado internacional es el instrumento vinculante más relevante a nivel global, diseñado para armonizar las leyes penales nacionales, mejorar las técnicas de investigación forense y aumentar la cooperación internacional rápida y eficaz (Organización de los Estados Americanos [OEA], 2020).

Para el contexto de una investigación sobre mitigación de delitos, el Convenio de Budapest demuestra que las amenazas que enfrentará un ciudadano en Huacho en 2025 pueden originarse en servidores ubicados en Europa del Este o Asia. Ante esta deslocalización del victimario, la autodefensa digital (evitar ser perfilado como una víctima fácil) se vuelve más efectiva que la persecución judicial transfronteriza.

2.2.6.4. Derechos digitales y la autodeterminación informativa

El goce seguro de la tecnología exige el reconocimiento y ejercicio de los Derechos Digitales, entendidos como la extensión de los derechos humanos fundamentales al entorno virtual. En el Perú, el pilar fundamental es el derecho a la protección de datos personales, regulado por la Ley N.º 29733.

Saldaña (2020) explica que esta ley consagra el principio de “autodeterminación informativa”, otorgando al ciudadano el poder de controlar, consentir o denegar el uso de su información personal por parte de terceros. No obstante, el ejercicio de este derecho es prácticamente nulo si el usuario carece de cultura de seguridad y acepta masivamente términos y condiciones sin leerlos o expone voluntariamente sus datos financieros en redes públicas. La autoprotección es la manifestación empírica del ejercicio de este derecho.

2.2.6.5. Ciberhigiene y conciencia digital: el ejercicio práctico del derecho

Para que el sujeto de derecho no se convierta en “objetivo vulnerable”, la teoría de la seguridad de la información propone dos constructos complementarios:

- **La ciberhigiene.** Análoga a las prácticas de higiene personal para prevenir enfermedades biológicas, la ciberhigiene se define como el conjunto de hábitos y prácticas rutinarias adoptadas por los usuarios para mantener el estado de salud y la seguridad de sus dispositivos, redes y cuentas digitales (Cain et al., 2018). Incluye la

limpieza regular de caché, la depuración de aplicaciones no utilizadas y la actualización constante de software.

- **La conciencia digital (*digital awareness*).** Va un paso más allá del mero uso tecnológico. Kruger y Kearney (2006) argumentan que la conciencia digital comprende el grado de lucidez y conocimiento continuo que tiene un usuario sobre las amenazas latentes en el ciberespacio, lo que dirige directamente su comportamiento frente a situaciones de riesgo (como identificar intuitivamente un correo de *phishing*).

2.2.6.6. Teorías relacionadas con el comportamiento preventivo

Para fundamentar científicamente cómo un ciudadano adopta la cultura de autoprotección, se recurre a marcos teóricos de la psicología conductual aplicados al entorno informático:

- **Teoría de la motivación de protección (PMT).** Propuesta originalmente por Rogers (1975) y adaptada a la ciberseguridad por Boss et al. (2015), esta teoría postula que un ciudadano adoptará medidas de protección digital basándose en dos procesos cognitivos: la evaluación de la amenaza (qué tan grave es el riesgo y qué tan vulnerable se siente ante él) y la evaluación de su afrontamiento (si cree que las medidas de autoprotección funcionarán y si se siente capaz de aplicarlas).
- **Teoría del comportamiento planificado (TPB).** Ajzen (1991) sostiene que la adopción de un comportamiento seguro (como negarse a compartir una contraseña) está determinada por la “intención” del individuo, la cual se forja por su actitud hacia la ciberseguridad, las normas subjetivas de su entorno (lo que hacen sus familiares o compañeros de trabajo) y el control conductual percibido.

2.2.6.7. Limitaciones del sistema judicial y necesidad de autoprotección en huacho (2025)

Aterrizando el marco normativo a la jurisdicción del Distrito Judicial de Huaura (cuya sede es Huacho), es imperativo evidenciar que las fiscalías locales a menudo carecen de laboratorios forenses digitales de alta tecnología o de personal informático suficiente para investigar micro-extorsiones o suplantaciones de identidad a pequeña escala.

En este contexto de saturación procesal y limitación técnica-investigativa, la judicialización del delito informático presenta altos índices de archivamiento. Por ello, la presente investigación sostiene que, hacia el 2025, la verdadera política criminal en Huacho no debe centrarse exclusivamente en fortalecer el Código Penal, sino en instaurar *criterios de aplicabilidad de la ciberseguridad a nivel ciudadano*. Capacitar a la población en

ciberhigiene y autoprotección es el método más costo-efectivo y eficiente para vaciar de contenido a las redes delictivas informáticas locales e internacionales.

2.2.7 Criterios de aplicabilidad en la cultura de autoprotección

2.2.7.1. Definición y factores determinantes de la viabilidad

En el ámbito de la seguridad de la información, la efectividad dogmática de una directriz técnica carece de valor si no es viable para el usuario final. Para el ciudadano común de Huacho, los criterios de aplicabilidad se definen como el conjunto de condiciones operativas, económicas y cognitivas que determinan si una medida preventiva de ciberseguridad será adoptada de forma sostenida o si será rechazada por resultar excesivamente compleja.

Según Furnell y Clarke (2012), la ciberseguridad a nivel ciudadano fracasa a menudo, no por carencias de software, sino porque las soluciones exigen una carga de atención y esfuerzo que supera la disposición del individuo promedio. Por lo tanto, el factor determinante principal es el principio de fricción mínima, el cual postula que toda medida de autoprotección debe integrarse orgánicamente en la cotidianidad digital, evitando alterar el dinamismo con el que el usuario utiliza la tecnología en su rutina diaria.

2.2.7.2. Modelos de referencia adaptados al entorno ciudadano

Históricamente, los marcos de trabajo fueron diseñados para proteger grandes infraestructuras. No obstante, para mitigar el cibercrimen a nivel civil, estos ecosistemas deben ser transliterados a competencias ciudadanas.

- **El *framework* de ciberseguridad del NIST.** El Instituto Nacional de Estándares y Tecnología (NIST, 2018) desarrolló un modelo central basado en un ciclo de vida de cinco funciones concurrentes. A nivel de autoprotección ciudadana personal, estas funciones se reinterpretan de la siguiente manera:
 - ✓ ***Identificar.*** El ciudadano reconoce qué activos digitales posee (cuentas bancarias, redes sociales, dispositivos) y el nivel de riesgo asociado a cada uno.
 - ✓ ***Proteger.*** Implementación activa de barreras (uso de gestores de contraseñas, autenticación multifactor y bloqueos biométricos).
 - ✓ ***Detectar.*** Desarrollo de la lucidez cognitiva para identificar enlaces fraudulentos (*phishing*) o accesos inusuales en sus plataformas.
 - ✓ ***Responder.*** Acción inmediata del usuario para bloquear tarjetas o revocar accesos en caso de sustracción de dispositivos.

- ✓ **Recuperar.** Restauración de la normalidad mediante la ejecución de copias de seguridad de la información personal.
- **La norma ISO/IEC 27001 y la ciberhigiene.** De manera complementaria, la Organización Internacional de Normalización (ISO, 2022) postula en su norma 27001 la gestión sistemática y auditable de los riesgos de la información. Al aplicarlo como criterio en un ciudadano común, este estándar abandona el formalismo de la auditoría para convertirse en ciberhigiene. Esta se comprende como la adopción de hábitos de depuración constante, como la revisión periódica de los permisos otorgados a las aplicaciones móviles y la eliminación del rastro digital no indispensable.

2.2.7.3. Modelos teóricos de adopción y comportamiento en ciberseguridad

Para predecir científicamente si un ciudadano huachano utilizará una medida mitigadora, la presente investigación se apoya en modelos sociocognitivos consolidados.

- **Teoría del comportamiento planificado (TPB).** Formulada por Ajzen (1991), esta teoría sostiene que la intención de un individuo de adoptar un comportamiento seguro está cimentada en tres pilares:
 1. **Actitud hacia la conducta.** La evaluación personal sobre si proteger el propio *smartphone* es una tarea valiosa y beneficiosa.
 2. **Norma subjetiva.** La presión o influencia de su entorno cercano (familia y pares de trabajo); si percibe que en su círculo social de Huacho la privacidad digital es irrelevante, su intención de autoprotegerse decaerá.
 3. **Control conductual percibido.** El grado de autoeficacia del usuario; es decir, su percepción sobre cuán capaz se siente para configurar exitosamente los parámetros de privacidad sin requerir asistencia técnica.
- **Modelo de aceptación de la tecnología (TAM).** Desarrollado originalmente por Davis (1989), el TAM resulta fundamental para establecer directrices de ciberseguridad. Este modelo argumenta que la aceptación de una herramienta preventiva depende de dos determinantes axiales: la “utilidad percibida” y la “facilidad de uso percibida”. Para el logro de la mitigación del delito informático, es imperativo que los planes formativos y el software de seguridad exijan el mínimo nivel de conocimientos previos.
- **Teoría de la motivación de protección (PMT).** Surgida desde la psicología preventiva, la PMT afirma que frente a un ciberdelito, las personas se protegen

basándose en dos procesos de evaluación. El ciudadano evalúa primero la gravedad de la amenaza (por ejemplo, el vaciado de sus cuentas bancarias) y su vulnerabilidad personal frente a esta. Posteriormente, evalúa el afrontamiento, es decir, calcula mentalmente si el costo y esfuerzo de la medida de seguridad justifican la recompensa de evitar el ataque informático (Boss et al., 2015).

Respecto a la integración de estos modelos sociocognitivos para el diseño empírico de planes de concientización, diversos investigadores de ciberseguridad concluyen que la pura transferencia de datos no consolida una cultura preventiva real. (Sommestad et al. 2014) afirmaron lo siguiente al evaluar programas formativos:

Los programas de concientización sobre seguridad de la información a menudo se basan en la suposición ingenua de que proporcionar conocimientos sobre las amenazas y las contramedidas conducirá automáticamente a un comportamiento seguro. Sin embargo, las intervenciones más efectivas son aquellas que logran modificar las actitudes subyacentes y aumentan la autoeficacia del usuario, demostrando que el esfuerzo requerido para aplicar la medida de seguridad es sustancialmente menor que el costo potencial de sufrir un incidente cibernético. (p. 25)

2.2.7.4. Contextualización socio-tecnológica en Huacho, 2025

Para que los criterios de aplicabilidad logren un impacto medible, los modelos teóricos expuestos deben filtrarse por las características socio-tecnológicas específicas del distrito de Huacho hacia el año 2025. El auge del comercio electrónico local, apoyado masivamente en billeteras digitales y aplicaciones de pago instantáneo desde dispositivos móviles, ha ampliado la superficie de ataque que los ciberdelincuentes pueden explotar.

En este escenario, el ciudadano huachano interactúa con plataformas bancarias de alta sensibilidad a través de redes inalámbricas urbanas que, a menudo, carecen de protección cifrada. Por lo tanto, el principal criterio de aplicabilidad contextual es la desmitificación de la ciberseguridad: abandonar la percepción de que la mitigación de delitos recae exclusivamente en la Policía Nacional del Perú, asumiendo la corresponsabilidad mediante la cultura de autoprotección como una capa de seguridad preventiva primaria.

2.2.7.5. La tríada de aplicabilidad social para la mitigación

Como síntesis del marco teórico, esta investigación establece que cualquier propuesta de seguridad tecnológica dirigida a los ciudadanos locales debe someterse a la validación de tres ejes fundamentales para ser viable:

- **Accesibilidad cognitiva.** La instrucción y configuración de la herramienta debe utilizar un lenguaje exento de anglicismos técnicos complejos.
- **Sostenibilidad práctica.** La medida protectora no debe requerir mantenimiento o actualizaciones manuales permanentes que generen la denominada “fatiga de seguridad”.
- **Proporcionalidad económica.** Los mecanismos de protección deben basarse primariamente en las configuraciones nativas de los sistemas operativos y aprovechar soluciones de ciberseguridad de código abierto o integradas, evitando un gravamen económico para las familias de la localidad.

2.2.8 Criterios operativos para el diseño e implementación de un modelo de ciberseguridad fundamentado en la cultura de autoprotección ciudadana, con el fin de reducir la incidencia de delitos informáticos

2.2.8.1. Fundamentación del modelo de ciberseguridad basado en cultura de autoprotección

La determinación de criterios operativos para el diseño e implementación de un modelo de ciberseguridad requiere una comprensión integral de las interrelaciones entre los constructos teóricos desarrollados en los puntos anteriores: delitos informáticos (Ley 30096), cultura de seguridad, factor humano como vulnerabilidad, marco jurídico y criterios de aplicabilidad.

El modelo de ciberseguridad fundamentado en la cultura de autoprotección ciudadana puede definirse como un marco sistemático, integral y sostenible de intervención que, mediante el fortalecimiento de conocimientos, actitudes y comportamientos de autoprotección digital en la población, reduce la vulnerabilidad frente a delitos informáticos y mitiga su incidencia en el contexto específico de la ciudad de Huacho.

Este modelo se distingue de enfoques exclusivamente tecnológicos o represivos por su énfasis en el empoderamiento ciudadano como agente activo de su propia seguridad digital. Según el Instituto Nacional de Ciberseguridad de España (INCIBE), la efectividad sostenible de la ciberseguridad requiere que los ciudadanos no sean meros receptores pasivos de protección, sino actores conscientes y responsables de su seguridad en el entorno digital.

2.2.8.2. Criterios operativos para el diseño del modelo

El diseño del modelo debe atender a criterios que aseguren su pertinencia, viabilidad y efectividad. Estos criterios operativos se organizan en dimensiones que abarcan desde la fundamentación teórica hasta la operativización práctica.

- **Criterio de fundamentación teórico-empírica.** El modelo debe construirse sobre bases teóricas sólidas y evidencia empírica disponible:
- ✓ ***Integración de marcos teóricos.*** El diseño debe incorporar de manera coherente la Teoría de las Actividades Rutinarias (Cohen y Felson, 1979), la Teoría de la Motivación de Protección (Rogers, 1975), la Teoría del Comportamiento Planificado (Ajzen, 1991) y el Modelo de Aceptación de Tecnología (Davis, 1989), articulándolos en un marco explicativo integrado de la conducta de autoprotección digital.
La convergencia de teorías del comportamiento humano permite comprender no solo por qué los ciudadanos toman riesgos en línea, sino también qué mecanismos pueden activarse para transformar esa conducta hacia la protección (Rogers, 1983, p. 156).
- ✓ ***Evidencia empírica local.*** El diseño debe considerar estudios previos sobre victimización por delitos informáticos en el Perú, particularmente datos de la Unidad Fiscal Especializada en Ciberdelincuencia y reportes de la Defensoría del Pueblo, que documentan patrones de victimización y factores de riesgo específicos del contexto nacional.
- ✓ ***Adaptación contextual.*** Los componentes del modelo deben adaptarse a las características sociodemográficas, culturales y tecnológicas de Huacho, considerando niveles de alfabetización digital, acceso a tecnologías, y patrones de uso característicos de la población local.
- **Criterio de integralidad y sistematicidad.** El modelo debe abarcar de manera integral las dimensiones del fenómeno:
- ✓ ***Cobertura de tipos de delitos.*** El diseño debe incluir componentes específicos para prevenir los principales delitos informáticos tipificados en la Ley N° 30096: fraude informático (Art. 8°), acceso ilícito (Art. 2°), daño informático (Art. 3° y 4°), grooming (Art. 5°), e interceptación de datos (Art. 7°).
- ✓ ***Articulación de niveles de intervención.*** El modelo debe operar simultáneamente en el nivel individual (conocimientos, actitudes, comportamientos del ciudadano), el nivel comunitario (redes de apoyo, normas sociales compartidas) y el nivel institucional (coordinación con autoridades, canales de denuncia).
- ✓ ***Secuencialidad lógica.*** Los componentes del modelo deben organizarse en una secuencia que respete la lógica del cambio conductual: concienciación sobre riesgos → adquisición de conocimientos → desarrollo de actitudes favorables → práctica de comportamientos seguros → automatización de hábitos de protección.

- **Criterio de pertinencia cultural y lingüística.** El modelo debe ser culturalmente apropiado para la población de Huacho:
- ✓ ***Lenguaje accesible.*** Utilizar español estándar, evitando anglicismos innecesarios o jerga técnica que dificulte la comprensión. Cuando se requiera terminología técnica (phishing, malware), debe acompañarse de definiciones claras.
- ✓ ***Relevancia contextual.*** Los ejemplos y casos utilizados en el modelo deben reflejar situaciones cotidianas de la población de Huacho: uso de banca móvil, compras en marketplaces locales, interacción en redes sociales populares en la ciudad, modalidades de fraude reportadas localmente.
- ✓ ***Respeto a la diversidad.*** El diseño debe considerar la heterogeneidad de la población en términos de edad, nivel educativo, ocupación y experiencia tecnológica, proponiendo adaptaciones para diferentes segmentos.
- **Criterio de viabilidad técnica y económica.** El modelo debe ser implementable con los recursos disponibles:
- ✓ ***Bajo costo.*** Priorizar medidas que no requieran inversión económica significativa por parte de los ciudadanos, aprovechando configuraciones gratuitas, software libre y funcionalidades nativas de dispositivos y aplicaciones.
- ✓ ***Compatibilidad tecnológica.*** Asegurar que las recomendaciones funcionen en los dispositivos más comunes en la población (smartphones de gama media, computadores básicos, conexiones de datos móviles).
- ✓ ***Sostenibilidad técnica.*** Diseñar componentes que no requieran mantenimiento técnico especializado por parte de los usuarios, minimizando la dependencia de soporte externo.

2.3 Definiciones de términos básicos

Ciberhigiene: Cain et al. (2018) definen este concepto como el conjunto de hábitos y prácticas rutinarias adoptadas por los usuarios para mantener el estado de salud y la seguridad de sus dispositivos, redes y cuentas digitales. Incluye medidas proactivas como la depuración de aplicaciones, la actualización de software y la gestión robusta de contraseñas.

Ciberseguridad: Constituye el ecosistema integral de prácticas, tecnologías, procesos y comportamientos diseñados para proteger redes, dispositivos, programas y datos contra ataques, daños o accesos no autorizados (Whitman y Mattord, 2018). Trasciende el enfoque puramente técnico para abarcar dimensiones humanas, organizacionales y sociales de la prevención.

Conciencia digital (Digital awareness): Es el grado de lucidez y conocimiento continuo que posee un usuario sobre las amenazas latentes en el ciberespacio. Abawajy (2014) afirma que este nivel de conciencia dirige y condiciona directamente el comportamiento frente a situaciones de riesgo, tales como la identificación instintiva de un ataque de ingeniería social.

Cultura de autoprotección ciudadana digital: Sistema integrado por conocimientos cognitivos, predisposiciones actitudinales y prácticas conductuales que los ciudadanos adoptan de manera autónoma para salvaguardar su integridad física, patrimonial y su identidad digital en el ciberespacio (Organización de las Naciones Unidas [ONU], 2013).

Delitos informáticos: Conductas delictivas antijurídicas tipificadas penalmente en las que se emplean las tecnologías de la información, plataformas digitales o dispositivos electrónicos, ya sea como el instrumento para cometer el acto o como el objetivo principal del ataque (ONU, 2013).

Derechos digitales: Representan la extensión de los derechos humanos fundamentales al entorno virtual, cuyo pilar primordial es el derecho a la protección de datos personales y el principio de autodeterminación informativa (Zukerfeld, 2020).

Factor humano en ciberseguridad: Conjunto de características cognitivas, psicológicas y conductuales que determinan el nivel de susceptibilidad de un individuo frente a ataques informáticos. Aunque es considerado tradicionalmente el “eslabón más débil”, posee la capacidad de transformarse en la primera línea de defensa activa mediante el entrenamiento continuo (Whitman y Mattord, 2018).

Fatiga de seguridad (Security fatigue): Fenómeno cognitivo que se manifiesta como una reducción progresiva de la vigilancia del usuario ante alertas de riesgo. Stanton et al. (2016) demostraron que esta fatiga surge a partir de la sobrecarga o exigencia constante de atención para verificar credenciales y configuraciones en el entorno digital.

Fraude informático: Ilícito penal caracterizado por la obtención deliberada de un provecho económico indebido en perjuicio de un tercero, valiéndose de la manipulación, suplantación o interferencia en el funcionamiento de un sistema informático o plataforma digital (ONU, 2013).

Ingeniería social: Métodos de manipulación psicológica empleados por ciberdelincuentes con el propósito de engañar al individuo para que, de manera involuntaria, entregue información confidencial, credenciales de acceso o ejecute códigos maliciosos (Hadnagy, 2018).

Sesgo de optimismo: Tendencia sistemática y distorsión cognitiva mediante la cual los individuos creen erróneamente que son menos propensos a experimentar eventos negativos, operando bajo la premisa ilusoria de invulnerabilidad personal frente a las amenazas del ciberespacio (Rhee et al., 2009).

Tríada CIA: Principios arquitectónicos fundamentales de la seguridad de la información compuestos por la Confidencialidad, la Integridad y la Disponibilidad, cuyo fin es garantizar el acceso ininterrumpido y seguro a los servicios requeridos (Whitman y Mattord, 2018).

2.4 Hipótesis de la investigación

2.4.1 Hipótesis general

Si se determinan como criterios operativos de aplicabilidad de la ciberseguridad basada en la cultura de autoprotección ciudadana la accesibilidad cognitiva de la información preventiva, la sostenibilidad práctica de los hábitos digitales seguros, la proporcionalidad económica de las medidas de protección, la educación digital continua y la adopción de prácticas básicas de verificación, confidencialidad e integridad de la información, entonces se favorecerá la mitigación de los delitos informáticos en Huacho durante el año 2025, mediante la reducción de la vulnerabilidad ciudadana frente a riesgos como el fraude informático, la suplantación de identidad, el acceso no autorizado y la manipulación de datos personales.

2.4.2 Hipótesis específicas

La presente investigación no formula hipótesis específicas, debido a que no se han planteado problemas específicos autónomos. Los objetivos específicos cumplen una función metodológica de desarrollo del objetivo general y permiten organizar el diagnóstico, análisis y propuesta de criterios preventivos; sin embargo, no constituyen subproblemas independientes que exijan hipótesis particulares. En consecuencia, la contrastación se realizará respecto de la hipótesis general, a partir del análisis de los resultados obtenidos mediante el cuestionario aplicado y de su vinculación con el marco teórico y jurídico de la ciberseguridad preventiva.

2.5 Las variables

La presente investigación se estructura sobre la base de dos variables centrales, derivadas directamente del problema general, del objetivo general y de la hipótesis general.

- **Variable independiente.** Criterios de aplicabilidad de ciberseguridad basada en la cultura de autoprotección ciudadana.
- **Variable dependiente.** Mitigación de delitos informáticos.

2.6 Operacionalización de las variables

Dicha investigación se realiza con 2 variables:

Operacionalización de las Variables (Fuente: Elaboración propia)

Variable	Definición conceptual	Definición operacional	Dimensiones	Indicadores
Variable independiente <i>Criterios de aplicabilidad de ciberseguridad basada en la cultura de autoprotección ciudadana</i>	Conjunto de parámetros preventivos, educativos, conductuales y operativos que permiten aplicar la ciberseguridad en la vida cotidiana de los ciudadanos, mediante hábitos de protección digital, reconocimiento de riesgos, verificación de información, protección de datos personales y uso responsable de herramientas tecnológicas.	Se medirá mediante el cuestionario aplicado a los estudiantes del Instituto de Idiomas de la UNJFSC, a partir de indicadores relacionados con conocimientos de ciberseguridad, prácticas de autoprotección digital, actualización de medidas de seguridad, uso de contraseñas, copias de seguridad, verificación de fuentes, configuración de privacidad, educación digital y adopción de hábitos preventivos.	Conocimiento preventivo en ciberseguridad	➤ Identificación de amenazas cibernéticas actuales. ➤ Conocimiento de medidas básicas de seguridad digital. ➤ Reconocimiento de posibles vulneraciones a derechos digitales.
			Prácticas de autoprotección digital	➤ Uso de contraseñas seguras y diferenciadas. ➤ Actualización de software o mecanismos de seguridad. ➤ Realización de copias de seguridad de información relevante. ➤ Revisión de configuración de privacidad en redes sociales.
			Verificación y gestión responsable de la información	➤ Verificación de autenticidad de fuentes digitales. ➤ Control de la información personal compartida en línea. ➤ Revisión de políticas de privacidad de aplicaciones utilizadas.
			Cultura educativa y participación preventiva	➤ Acceso a formación en ciberseguridad y derechos digitales. ➤ Participación en talleres o cursos de seguridad en línea. ➤ Valoración de la educación digital como estrategia preventiva.
			Criterios operativos de aplicabilidad	➤ Accesibilidad cognitiva de las medidas preventivas. ➤ Sostenibilidad práctica de los hábitos de seguridad digital. ➤ Proporcionalidad económica de las medidas de autoprotección.
Variable dependiente <i>Mitigación de delitos informáticos</i>	Condición preventiva orientada a reducir la vulnerabilidad y exposición de los ciudadanos frente a conductas ilícitas cometidas mediante tecnologías de la información, tales como fraude informático, suplantación de identidad, acceso no autorizado, robo de datos personales, divulgación indebida y manipulación de información digital.	Se medirá mediante la identificación de experiencias, percepciones y conductas de riesgo reportadas por los encuestados, así como mediante indicadores vinculados con accesos no autorizados, pérdida o alteración de información, fraude informático, uso indebido de datos personales, vulneración de derechos digitales, afectación de la confidencialidad y manipulación de información.	Exposición a riesgos informáticos	➤ Experiencia de accesos no autorizados a dispositivos o cuentas. ➤ Problemas de seguridad informática en el último año. ➤ Pérdida o alteración de información personal por ataques informáticos.
			Riesgo de fraude y suplantación digital	➤ Experiencia de fraude informático vinculado con datos personales. ➤ Conocimiento de intentos de suplantación de identidad digital. ➤ Uso no autorizado de datos personales.
			Protección de derechos digitales y datos personales	➤ Percepción de vulneración de derechos digitales. ➤ Preocupación por el uso indebido de datos personales en línea. ➤ Confianza en las herramientas tecnológicas de protección.
			Confidencialidad e integridad de la información	➤ Implementación de medidas para proteger información confidencial. ➤ Experiencia de divulgación no autorizada de información. ➤ Detección de cambios no autorizados en datos personales o profesionales. ➤ Dificultad para detectar manipulación de datos en entornos digitales.

Capítulo III : METODOLOGÍA

3.1 Diseño metodológico

El diseño metodológico es la estructura lógica que orienta la forma en que se organizará, recogerá y analizará la información para responder al problema de investigación. En términos generales, constituye el plan que articula las variables, los objetivos, la población, los instrumentos y el tratamiento de los datos.

Hernández Sampieri et al. (2014) sostienen que el diseño metodológico permite establecer la estrategia general del estudio, de modo que exista coherencia entre el problema planteado, las hipótesis y los procedimientos de recolección y análisis. Por su parte, Bernal (2010) afirma que el diseño metodológico no es un elemento accesorio, sino la base que permite asegurar orden, rigor y sistematicidad en el desarrollo de la investigación. Vara (2012) añade que, en estudios aplicados, el diseño debe responder a una necesidad concreta y no limitarse a describir un fenómeno de manera aislada.

Entre sus características principales, el diseño metodológico se distingue por ser sistemático, porque sigue una secuencia lógica; coherente, porque articula todos los elementos de la investigación; flexible, porque puede adaptarse a las condiciones del campo; y verificable, porque permite revisar la consistencia entre objetivos, hipótesis e instrumentos.

El diseño metodológico de la presente investigación es no experimental y transversal, debido a que no se manipulan deliberadamente las variables, sino que se observan y analizan las prácticas, conocimientos, percepciones y niveles de exposición digital de los encuestados en un momento determinado. Asimismo, el estudio posee orientación descriptiva-propositiva, porque primero diagnostica condiciones de vulnerabilidad y cultura de autoprotección digital en una población determinada, para luego establecer criterios operativos de aplicabilidad de ciberseguridad orientados a la mitigación preventiva de delitos informáticos.

El estudio no pretende demostrar experimentalmente la reducción estadística de delitos informáticos mediante una intervención previa y posterior, sino determinar criterios preventivos razonables a partir de la información empírica obtenida, del marco teórico sobre ciberseguridad humana y del marco jurídico aplicable a los delitos informáticos y derechos digitales. En consecuencia, el diseño resulta coherente con la finalidad aplicada de la investigación, pues busca aportar criterios útiles para fortalecer la autoprotección ciudadana frente a riesgos informáticos en el contexto de Huacho.

3.2 Tipo de investigación

La investigación es de tipo aplicada, porque su finalidad no es únicamente ampliar el conocimiento teórico, sino generar criterios útiles para enfrentar una problemática real y concreta: la incidencia de delitos informáticos en Huacho.

Vara (2012) explica que la investigación aplicada busca producir conocimiento con utilidad práctica, es decir, conocimiento que pueda emplearse en la solución de un problema específico. De igual manera, Bernal (2010) señala que este tipo de investigación se orienta a la intervención sobre la realidad, priorizando resultados que tengan impacto en el contexto donde se desarrolla el estudio. Vara (2012) en su libro 7 pasos para una tesis exitosa nos menciona que la investigación aplicada normalmente identifica cual es la situación al problema y busca las posibles soluciones, finalmente busca la más adecuada para el contexto específico.

Las principales características de la investigación aplicada son su orientación práctica, su vinculación directa con necesidades reales, su utilidad para diseñar soluciones y su cercanía con contextos específicos. En la presente investigación, este carácter aplicado se refleja en la intención de proponer un modelo de ciberseguridad basado en la cultura de autoprotección ciudadana, con criterios operativos que puedan implementarse en una población concreta. Por ello, el estudio no se agota en la descripción del fenómeno, sino que busca ofrecer una respuesta funcional frente a la vulnerabilidad digital de los ciudadanos.

3.3 Nivel de la investigación

La presente investigación se ubica en un nivel descriptivo-propositivo, con alcance explicativo limitado.

Es descriptiva porque identifica y caracteriza el nivel de conocimientos, prácticas, percepciones y experiencias vinculadas con la autoprotección digital y la exposición frente a delitos informáticos.

Es propositiva porque, a partir de dicho diagnóstico, formula criterios operativos de aplicabilidad de la ciberseguridad basada en la cultura de autoprotección ciudadana.

El alcance explicativo es limitado, en tanto la investigación permite establecer relaciones razonadas entre déficit de cultura preventiva, vulnerabilidad digital y necesidad de medidas de autoprotección, pero no desarrolla un diseño experimental destinado a comprobar causalidad directa o reducción estadística efectiva de la incidencia delictiva.

3.4 Diseño de la investigación

El diseño de la investigación es no experimental y de corte transversal. Es no experimental porque no se manipularán deliberadamente las variables; el fenómeno será observado tal como se presenta en su contexto natural.

Hernández Sampieri et al. (2014) precisan que en los diseños no experimentales el investigador no introduce estímulos ni modifica condiciones, sino que observa los hechos tal como ocurren. Es transversal porque la información se recogerá en un solo momento, durante el año 2025. Y es correlacional-explicativo porque busca identificar la relación entre la cultura de autoprotección ciudadana y la reducción de la incidencia de delitos informáticos, además de interpretar cómo se vinculan estos elementos en el contexto estudiado.

Las características de este diseño son la observación directa del fenómeno, la ausencia de manipulación de variables, la medición en un solo tiempo y la posibilidad de analizar asociaciones entre variables. Este tipo de diseño resulta apropiado para investigaciones donde el investigador desea comprender relaciones reales en escenarios sociales o educativos sin intervenir sobre ellos. En la presente investigación, este diseño permite examinar la conducta preventiva de los estudiantes del Instituto de Idiomas de la UNJFSC y su relación con la vulnerabilidad frente a delitos informáticos, sin alterar el entorno natural en el que se desarrollan dichas conductas.

3.5 Enfoque de la investigación

El enfoque de la presente investigación es cuantitativo. Según Hernández-Sampieri y Mendoza (2018), el enfoque cuantitativo se orienta a la medición objetiva de las variables, basando la recolección de datos en la medición numérica y el análisis en procedimientos estadísticos para establecer patrones de comportamiento. Bernal (2010) añade que este enfoque permite trabajar con información estandarizada, comparable y susceptible de análisis matemático.

En el contexto de este estudio, el carácter cuantitativo se evidencia en la medición de las dimensiones de la “cultura de autoprotección ciudadana” y los “delitos informáticos” a través de un cuestionario estructurado con escala tipo Likert, asignando valores numéricos a las respuestas para su posterior procesamiento y contrastación de hipótesis mediante estadística descriptiva. No se considera un enfoque cualitativo ni mixto, ya que no se emplean herramientas de interpretación subjetiva o de discurso abierto, sino que se busca generalizar resultados a partir de una muestra estadísticamente representativa.

3.6 Estilo de la investigación

El estilo de la investigación es analítico-sintético, con orientación propositiva. Es analítico porque descompone el problema en partes: ciberseguridad, cultura de autoprotección ciudadana, delitos informáticos y criterios operativos. Y es sintético porque integra esos elementos para construir una propuesta coherente de intervención.

Bernal (2010) explica que el análisis permite estudiar cada componente de manera individual para comprender su función dentro del fenómeno general, mientras que la síntesis posibilita recomponer el problema con una visión integral. Vara (2012) agrega que en estudios aplicados resulta indispensable no quedarse en la fragmentación del dato, sino convertirlo en una propuesta útil.

Las características de este estilo son la identificación de componentes, el examen crítico de relaciones, la integración de hallazgos y la elaboración de una propuesta final, en otras palabras, no solo se analiza el problema, sino que se construye una respuesta viable.

3.7 Población y muestra

La población es la totalidad de todos elementos a los que hará referencia la presente investigación y la muestra será solo una parte de la población para realizar el presente estudio.

3.7.1 Población

De acuerdo con Fracica (1988), población es “el conjunto de todos los elementos a los cuales se refiere la investigación. Se puede definir también como el conjunto de todas las unidades de muestreo” (p. 36). Según Bernal (2010) menciona que Jany en 1994 señala que la población es “la totalidad de elementos o individuos que tienen ciertas características similares y sobre las cuales se desea hacer inferencia”. O bien, unidad de análisis. (p.160)

Así, la población está conformada por los estudiantes matriculados en el Instituto de Idiomas de la Universidad Nacional José Faustino Sánchez Carrión (UNJFSC). Según la información proporcionada por dicha institución, se cuenta con 29 grupos de estudio de idiomas, considerando que cada grupo se apertura con un mínimo de 15 estudiantes.

La elección de los estudiantes del Instituto de Idiomas de la UNJFSC como población empírica de estudio obedece a criterios de accesibilidad y representatividad estratégica. El investigador, en su calidad de estudiante de inglés intermedio y delegado de aula, mantiene un contacto directo y cotidiano con sus compañeros y otros grupos, lo que facilitó la aplicación de instrumentos y la observación natural del fenómeno.

La población total asciende a 435 estudiantes, resultado de multiplicar el número de grupos por la cantidad mínima de estudiantes por aula ($29 \times 15 = 435$).

$$\text{Población Total} = 29 \times 15$$

$$\text{Población Total} = 435$$

Esta delimitación de población responde a criterios de viabilidad, accesibilidad y pertinencia temática, dado que se trata de usuarios activos de herramientas digitales, plataformas virtuales, redes sociales y servicios en línea.

En consecuencia, los resultados obtenidos permiten diagnosticar condiciones de cultura de autoprotección digital en dicha población y utilizarlas como referencia empírica para proponer criterios preventivos aplicables al contexto local.

3.7.2 Muestra

Bernal (2010) señala que la muestra es una parte representativa del universo de estudio, elegida para recolectar información válida y generalizable. Hernández Sampieri et al. (2014) agregan que una muestra bien seleccionada permite aproximarse con mayor precisión a las características de la población.

Según Bernal (2010) “Es la parte de la población que se selecciona, de la cual realmente se obtiene la información para el desarrollo del estudio y sobre la cual se efectuarán la medición y la observación de las variables objeto de estudio”. (p.161). En la determinación de la muestra se puede llegar a trabajar con los siguientes valores estadísticos:

E = Error de muestreo (existe tabla de valores) 0,07

Z = Valor de la tabla Normal estándar para un nivel de confianza de 95% en los resultados muestrales 1,96

P = Proporción de la variable 0,5

Q = Proporción de fracaso 0,5

N = Población total 435

$$n = \frac{Z^2 PQN}{Z^2 PQ + (N - 1)E^2}$$

$$n = \frac{(1,96)^2(0,5)(0,5)(435)}{(1,96)^2(0,5)^2 + 435(0,07)^2}$$

$$n = \frac{85260}{631} = 135,118859$$

$$n = 135$$

Debe precisarse que la muestra no representa estadísticamente a la totalidad de habitantes de Huacho, sino que constituye una unidad empírica de análisis relevante para observar prácticas, riesgos y déficits preventivos en usuarios digitales vinculados a un entorno educativo local.

Por ello, las conclusiones de la investigación se formularán con prudencia metodológica, evitando generalizaciones absolutas sobre toda la ciudadanía huachana y orientando los hallazgos hacia la determinación de criterios preventivos de aplicabilidad local.

3.8 Técnicas de recolección de datos

3.8.1 Técnicas de recolección de datos a emplear

La técnica principal de recolección de datos será la encuesta. Esta técnica consiste en recoger información directamente de los sujetos de estudio mediante preguntas previamente estructuradas, con el fin de obtener respuestas comparables y medibles. Bernal (2010) considera que la encuesta es una técnica adecuada cuando se busca conocer opiniones, conocimientos o prácticas de un grupo determinado. Su uso es especialmente útil en investigaciones cuantitativas, porque permite trabajar con resultados estandarizados.

Sus características principales son la uniformidad, porque todos responden a los mismos ítems; la economía de tiempo, porque puede aplicarse a varios sujetos en poco tiempo; la comparabilidad, porque todas las respuestas siguen el mismo patrón; y la sistematización, porque facilita el tratamiento posterior de los datos.

3.8.2 Descripción de los instrumentos

El instrumento será un cuestionario estructurado con escala tipo Likert. Este instrumento permitirá medir las variables relacionadas con la cultura de autoprotección ciudadana y la incidencia de delitos informáticos. Hernández Sampieri et al. (2014) señalan que los instrumentos de recolección deben ser claros, pertinentes y alineados con las dimensiones del estudio. En este caso, el cuestionario permitirá recoger información sobre conocimientos, actitudes y comportamientos preventivos.

Sus características son la precisión, porque cada ítem se formula para medir un aspecto específico; la validez de contenido, porque debe reflejar las dimensiones de la variable; la confiabilidad, porque debe producir resultados estables; y la facilidad de aplicación, porque puede ser administrado a un grupo amplio de estudiantes sin dificultad.

3.8.3 Recolección de datos

La recolección de datos consistirá en aplicar el cuestionario a los estudiantes seleccionados en la muestra, previa coordinación institucional y respeto de los principios éticos de consentimiento y confidencialidad. Bernal (2010) sostiene que la recolección debe ejecutarse de manera ordenada, controlada y respetuosa de la información obtenida. En la presente investigación, el proceso se realizará en un solo momento y bajo condiciones homogéneas para todos los participantes.

Las características de esta etapa son la planificación previa, la uniformidad en la aplicación, la confidencialidad de las respuestas y la trazabilidad de la información. Esta fase es esencial porque de su correcta ejecución depende la calidad de los datos que luego serán analizados.

3.8.4 Codificación

La codificación consiste en asignar valores numéricos a las respuestas obtenidas. En una escala Likert, por ejemplo, puede utilizarse la siguiente equivalencia: 1 = Nunca, 2 = Casi nunca, 3 = A veces, 4 = Casi siempre y 5 = Siempre. Este procedimiento permite transformar las respuestas verbales en datos cuantificables para su posterior análisis. Hernández Sampieri et al. (2014) destacan que la codificación es fundamental para organizar la base de datos y facilitar el procesamiento estadístico.

Las características de la codificación son la ordenación, porque clasifica respuestas; la uniformidad, porque todas las opciones tienen una equivalencia numérica; la practicidad, porque simplifica el análisis; y la objetividad, porque reduce ambigüedades al momento de procesar la información.

3.8.5 Tabulación

La tabulación es el proceso mediante el cual las respuestas codificadas se organizan en tablas de frecuencia y porcentaje. Bernal (2010) explica que tabular permite resumir grandes volúmenes de información en estructuras comprensibles y útiles para la interpretación. En esta investigación, la tabulación ayudará a identificar patrones, tendencias y distribuciones de respuesta en cada dimensión evaluada.

Sus características son la síntesis, porque resume la información; la claridad, porque facilita la lectura de los datos; la comparabilidad, porque permite contrastar resultados entre ítems o dimensiones; y la utilidad interpretativa, porque hace visibles los hallazgos más relevantes.

3.8.6 Registro de datos

El registro de datos es la consignación ordenada de la información obtenida en una base de datos, generalmente en Excel u otro programa estadístico como SPSS. Este paso permite conservar la información de manera segura, estructurada y accesible para el análisis. Hernández Sampieri et al. (2014) resaltan que el registro debe ser consistente y verificable, de modo que cualquier análisis posterior pueda reproducirse sin dificultad.

Las características del registro son la sistematicidad, porque sigue un orden definido; la seguridad, porque conserva la información de forma controlada; la trazabilidad, porque permite identificar el origen de cada dato; y la disponibilidad, porque facilita su consulta para el procesamiento estadístico.

3.8.7 Presentación de datos

La presentación de datos consiste en mostrar los resultados en tablas, cuadros y gráficos, acompañados de su interpretación. Bernal (2010) sostiene que la presentación clara de los resultados es indispensable para comunicar con precisión los hallazgos de una investigación. En el presente estudio dicha presentación permitirá visualizar el nivel de conocimientos, prácticas y percepciones de autoprotección ciudadana, así como su relación con la incidencia de delitos informáticos.

Sus características son la claridad, porque facilita la lectura; la ordenación, porque organiza la información de forma lógica; la visualización, porque los gráficos ayudan a comprender los resultados; y la interpretabilidad, porque los datos adquieren significado cuando se exponen adecuadamente.

3.9 Técnicas para el procesamiento de la información

El procesamiento de la información se realizará mediante estadística descriptiva, utilizando frecuencias absolutas, porcentajes y, de ser necesario, medidas de tendencia central. Hernández Sampieri et al. (2014) explican que el análisis cuantitativo requiere organizar y transformar los datos en información útil para la interpretación. Bernal (2010) también señala que el tratamiento estadístico es indispensable para reducir la información cruda a resultados comprensibles y técnicamente válidos.

Las características de este procesamiento son la objetividad, porque se basa en cifras; la ordenación, porque clasifica los datos; la síntesis, porque reduce la información a indicadores comprensibles; y la utilidad analítica, porque permite interpretar los resultados en función de los objetivos e hipótesis del estudio.

Capítulo IV : RESULTADOS

4.1 Análisis de resultados

Tabla 1

Sexo

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Masculino	70	52,4	52,4	52,4
	Femenino	65	47,6	47,6	100,0
	Total	135	100,0	100,0	

Fuente: De investigación propia.

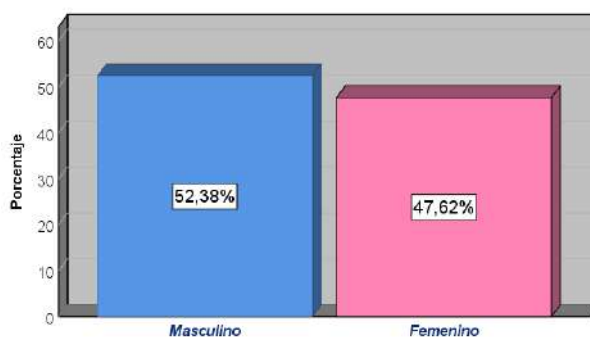


Figura 1 - Sexo

En la tabla 1 indica que el 52,4% de los encuestados son varones y el resto equivalente a 47,6% son mujeres

Tabla 2

Grupo etario

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	18 - 28	135	100,0	100,0	100,0

Fuente: De investigación propia.

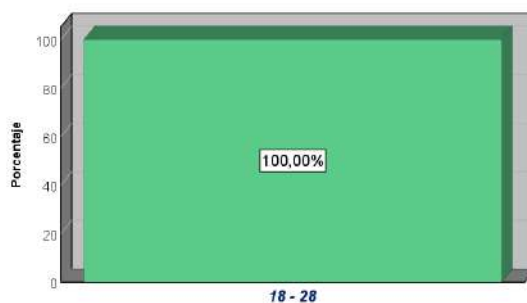


Figura 2 - Grupo etario

En la tabla 2 establece que el 100% de los encuestados pertenecen al grupo etario entre los 18 y 28 años de edad.

Tabla 3

Experiencia con accesos no autorizados de terceras personas a los dispositivos o sistemas informáticos personales

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	97	71,4	71,4	71,4
	Casi Nunca	13	9,5	9,5	81,0
	Ocasionalmente	19	14,3	14,3	95,2
	Casi siempre	6	4,8	4,8	100,0
	Total	135	100,0	100,0	

Fuente: De investigación propia.

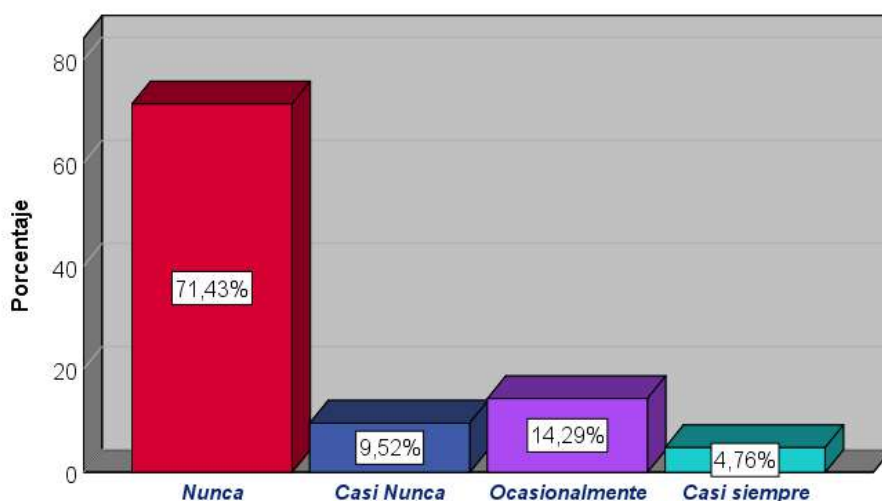


Figura 3 - Experiencia con accesos no autorizados de terceras personas a los dispositivos o sistemas informáticos personales

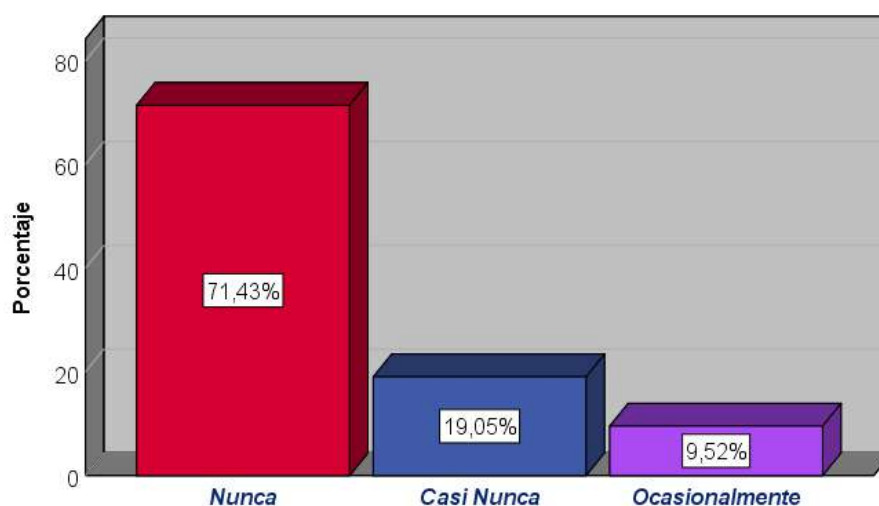
En la Tabla 3 se observa que el 71.4% respondió que **nunca** ha tenido alguna experiencia en violación a sus datos por terceros no autorizados a sus dispositivos informáticos, seguido de un 9.5% respondió que **casi nunca** ha tenido alguna experiencia en violación a sus datos por terceros no autorizados a sus dispositivos informáticos.

Por otro lado, un 14.3% respondió que **ocasionalmente** ha tenido alguna experiencia en violación a sus datos por terceros no autorizados a sus dispositivos informáticos, reflejando un moderado. En las frecuencias más altas, un 4.8% manifestó que **casi siempre** ha tenido alguna experiencia en violación a sus datos por terceros no autorizados a sus dispositivos informáticos.

Tabla 4*Problemas de seguridad en sistemas informáticos personales en el último año*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	98	71,4	71,4	71,4
	Casi Nunca	26	19,0	19,0	90,5
	Ocasionalmente	13	9,5	9,5	100,0
	Total	135	100,0	100,0	

Fuente: De investigación propia.

*Figura 4 - Problemas de seguridad en sistemas informáticos personales en el último año*

En la tabla 4 se observa que el 71.4% respondió que **nunca** ha presentado problemas de seguridad en sistemas informáticos personales en el último año, seguido de un 19.0% que respondió **casi nunca** presentó problemas de seguridad en sistemas informáticos personales en el último año. Por otro lado, un 9,5% manifestó que **ocasionalmente**, presentó problemas de seguridad en sistemas informáticos personales en el último año.

Tabla 5*Pérdida o alteración de información personal por ataques informáticos*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	117	85,7	85,7	85,7
	Casi Nunca	18	14,3	14,3	100,0
	Total	21	100,0	100,0	

Fuente: De investigación propia.

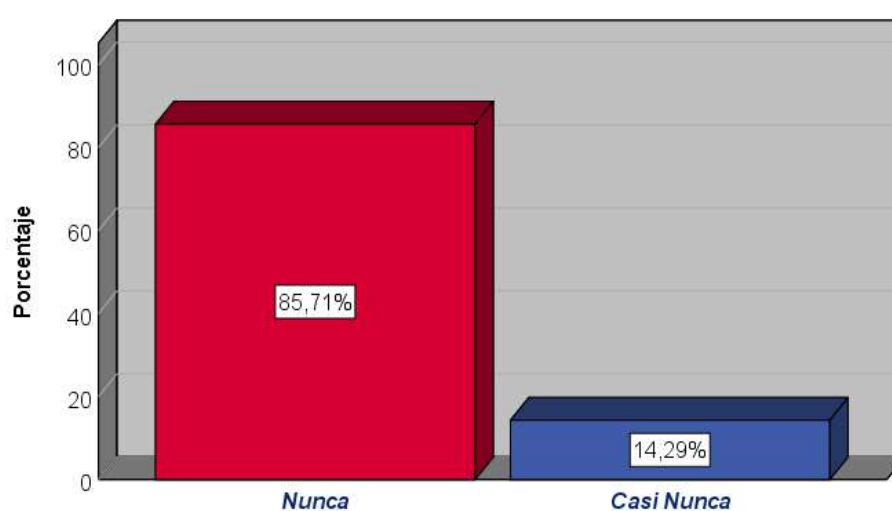


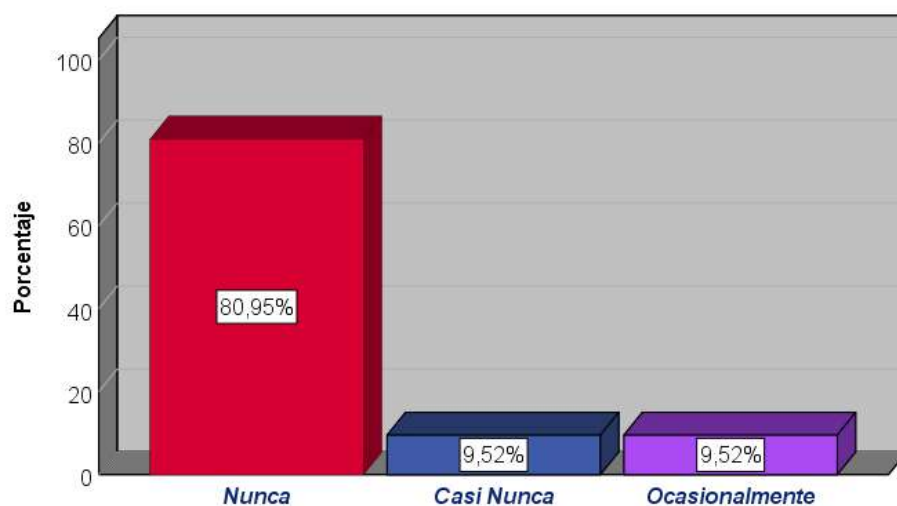
Figura 5 - Pérdida o alteración de información personal por ataques informáticos

En la tabla 5 se observa que el 85.7% respondió que **nunca** presentó pérdida o alteración de información personal por ataques informáticos, seguido de un 14.3% manifestó que **casi nunca**, pérdida o alteración de información personal por ataques informáticos.

Tabla 6*Revisiones propias regulares de seguridad en los sistemas informáticos personales*

		Frecuenci a	Porcenta je	Porcentaje válido	Porcentaje acumulado
Válid o	Nunca	109	81,0	81,0	81,0
	Casi Nunca	13	9,5	9,5	90,5
	Ocasionalmen te	13	9,5	9,5	100,0
	Total	135	100,0	100,0	

Fuente: De investigación propia.

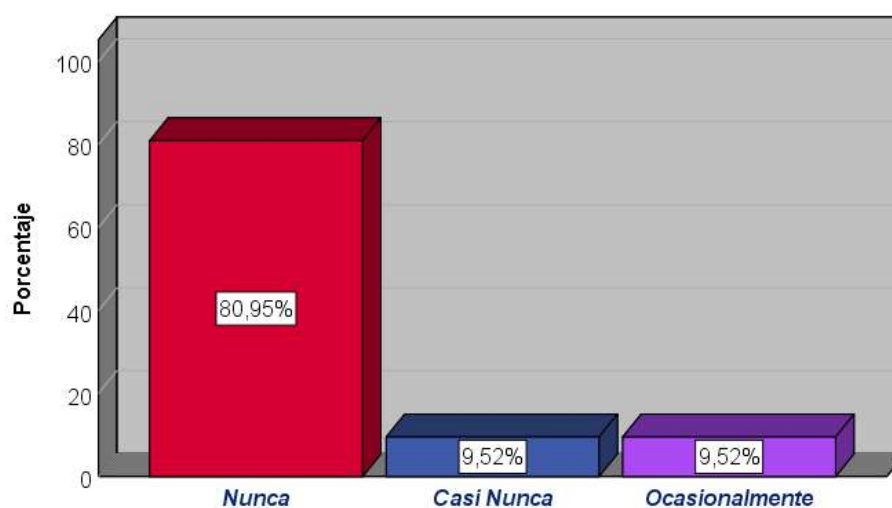
*Figura 6 - Revisiones propias regulares de seguridad en los sistemas informáticos personales*

En la tabla 6 se observa que el 81.0% respondió que **nunca** realiza revisiones propias regulares de seguridad en los sistemas informáticos personales, seguido de un 9.5% respondió que **casi nunca** realiza revisiones propias regulares de seguridad en los sistemas informáticos personal. Por otro lado, un 9.5% manifestó que **ocasionalmente** realiza revisiones propias regulares de seguridad en los sistemas informáticos personales.

Tabla 7*Frecuencia de actualización del software de seguridad personal*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	110	81,0	81,0	81,0
	Casi Nunca	13	9,5	9,5	90,5
	Ocasionalmente	13	9,5	9,5	100,0
	Total	135	100,0	100,0	

Fuente: De investigación propia.

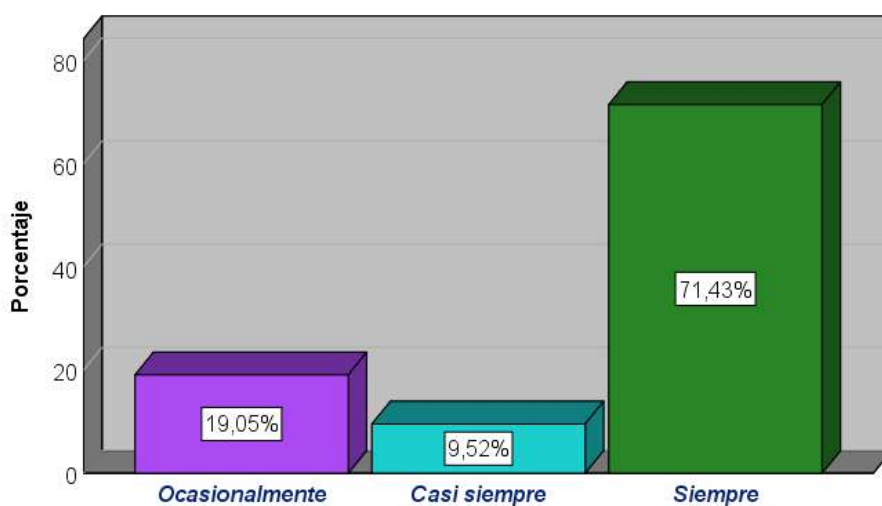
*Figura 7 - Frecuencia de actualización del software de seguridad personal*

En la tabla 7 se observa que el 81.0% respondió que **nunca** actualiza el software de seguridad personal, seguido de un 9.5% respondió que **casi nunca** actualiza el software de seguridad personal. Por otro lado, un 9.5% respondió que **ocasionalmente** actualiza el software de seguridad personal, finalmente un 4.8% manifestó que **casi siempre** actualiza el software de seguridad personal.

Tabla 8*Uso de contraseñas personales seguras y únicas en cuentas en línea*

		Frecuenci a	Porcenta je	Porcentaje válido	Porcentaje acumulado
Válid o	Ocasionalmen te	26	19,0	19,0	19,0
	Casi siempre	12	9,5	9,5	28,6
	Siempre	97	71,4	71,4	100,0
	Total	135	100,0	100,0	

Fuente: De investigación propia.

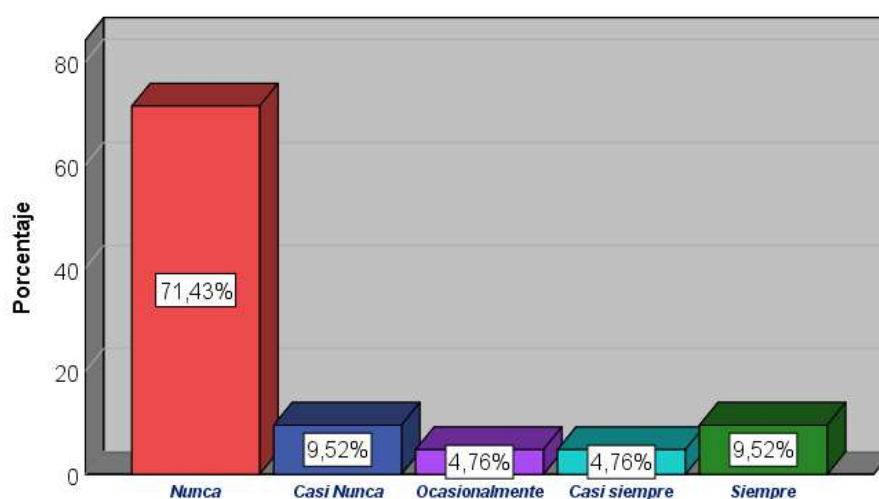
*Figura 8 - Uso de contraseñas personales seguras y únicas en cuentas en línea*

En la tabla 8 se observa que el 19.0% respondió que **ocasionalmente** usa contraseñas personales seguras y únicas en cuentas en línea. Un 9.5% respondió que **casi siempre** usa contraseñas personales seguras y únicas en cuentas en línea, y un 71.4% manifestó que **“siempre”** usa contraseñas personales seguras y únicas en cuentas en línea.

Tabla 9*Frecuencia de realización de copias de seguridad de datos importantes personales*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	97	71,4	71,4	71,4
	Casi Nunca	13	9,5	9,5	81,0
	Ocasionalmente	6	4,8	4,8	85,7
	Casi siempre	6	4,8	4,8	90,5
	Siempre	13	9,5	9,5	100,0
	Total	135	100,0	100,0	

Fuente: De investigación propia.

*Figura 9 - Frecuencia de realización de copias de seguridad de datos importantes personales*

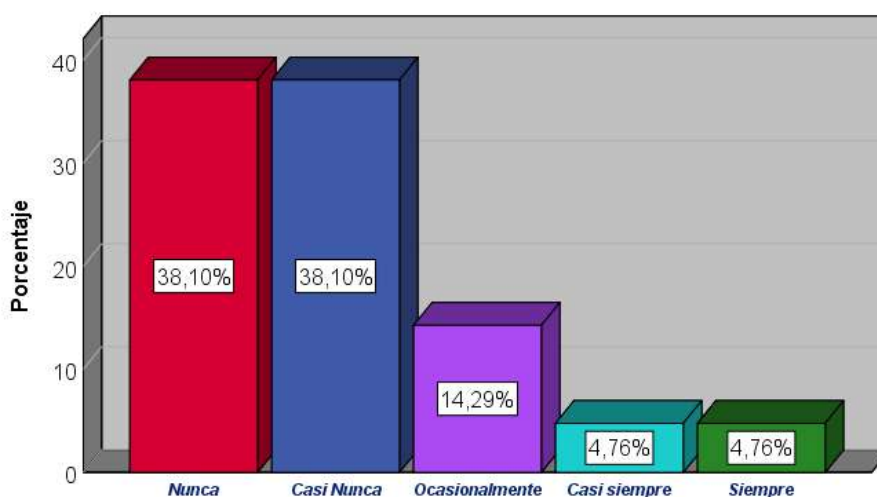
En la tabla 9 se observa que el 71.4% respondió que **nunca** realiza copias de seguridad de datos importantes personales, seguido de un 9.5% respondió que **casi nunca** realiza copias de seguridad de datos importantes personales.

Por otro lado, un 4.8% respondió que **ocasionalmente** realiza copias de seguridad de datos importantes personales. Un 4.8% respondió que **casi siempre** realiza copias de seguridad de datos importantes personales, y por último un 9.5% manifestó que “**siempre**” realiza copias de seguridad de datos importantes personales.

Tabla 10*Información sobre amenazas cibernéticas actuales*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	52	38,1	38,1	38,1
	Casi Nunca	52	38,1	38,1	76,2
	Ocasionalmente	19	14,3	14,3	90,5
	Casi siempre	6	4,8	4,8	95,2
	Siempre	6	4,8	4,8	100,0
	Total	135	100,0	100,0	

Fuente: De investigación propia.

*Figura 10 - Información sobre amenazas cibernéticas actuales*

En la tabla 10 se observa que el 38.1% respondió que **nunca** se informa sobre amenazas cibernéticas actuales, seguido de un 38.1% respondió que **casi nunca** se informa sobre amenazas cibernéticas actuales. Por otro lado, un 14.3% respondió que **ocasionalmente** se informa sobre amenazas cibernéticas actuales. Un 4.8% respondió que **casi siempre** se informa sobre amenazas cibernéticas actuales, y por último un 4.8% manifestó que “**siempre**” se informa sobre amenazas cibernéticas actuales.

Tabla 11

Experiencia respecto al fraude informático relacionado con datos personales

		Frecuenci	Porcenta	Porcentaje	Porcentaje
		a	je	válido	acumulado
Válid o	Nunca	96	71,4	71,4	71,4
	Casi Nunca	26	19,0	19,0	90,5
	Ocasionalmen te	13	9,5	9,5	100,0
	Total	135	100,0	100,0	

Fuente: De investigación propia.

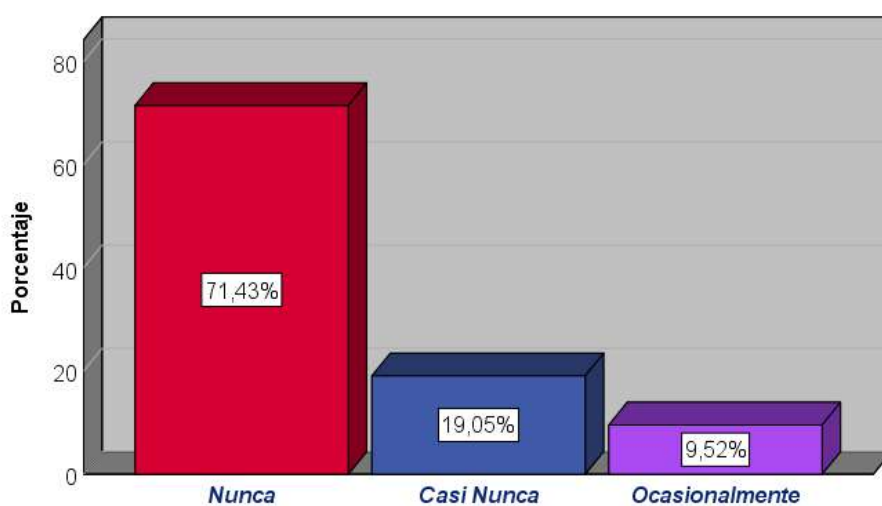


Figura 11 - Experiencia respecto al fraude informático relacionado con datos personales

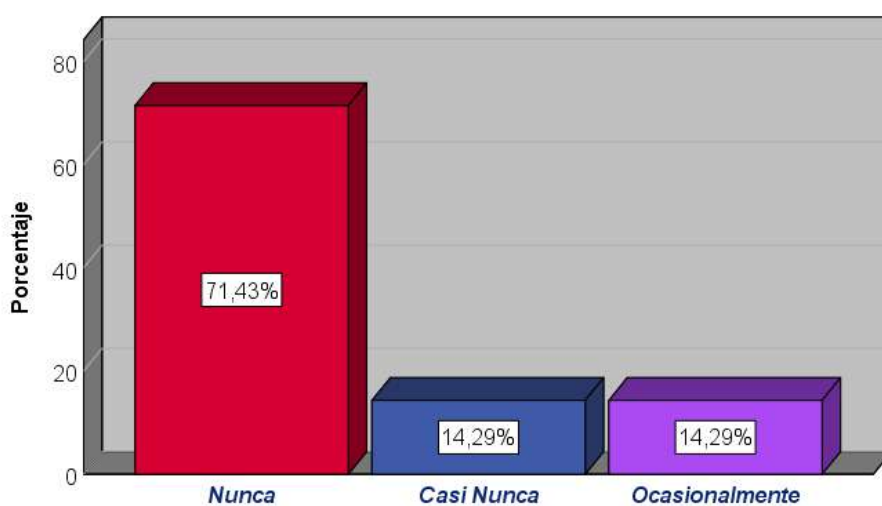
En la tabla 11 se observa que el 71.4% respondió que **nunca** tuvo una experiencia respecto al fraude informático relacionado con datos personales, seguido de un 19.0% respondió que **casi nunca** tuvo una experiencia respecto al fraude informático relacionado con datos personales.

Por otro lado, un 9.5% manifestó que **ocasionalmente** tuvo una experiencia respecto al fraude informático relacionado con datos personales.

Tabla 12*Experiencia de robo o uso no autorizado de datos personales*

		Frecuenci	Porcenta	Porcentaje	Porcentaje
		a	je	válido	acumulado
Válid o	Nunca	97	71,4	71,4	71,4
	Casi Nunca	19	14,3	14,3	85,7
	Ocasionalmen te	19	14,3	14,3	100,0
	Total	135	100,0	100,0	

Fuente: De investigación propia.

*Figura 12 - Experiencia de robo o uso no autorizado de datos personales*

En la tabla 12 se observa que el 71.4% respondió que **nunca** ha experimentado robo o uso no autorizado de datos personales, seguido de un 14.3% respondió que **casi nunca** ha experimentado robo o uso no autorizado de datos personales. Por otro lado, un 14.3% manifestó que **ocasionalmente** ha experimentado robo o uso no autorizado de datos personales.

Tabla 13

A visualizado o conoce casos de intentos de suplantación de identidad digital

		Frecuenci a	Porcenta je	Porcentaje válido	Porcentaje acumulado
Válid o	Nunca	96	71,4	71,4	71,4
	Casi Nunca	13	9,5	9,5	81,0
	Ocasionalmen te	26	19,0	19,0	100,0
	Total	135	100,0	100,0	

Fuente: De investigación propia.

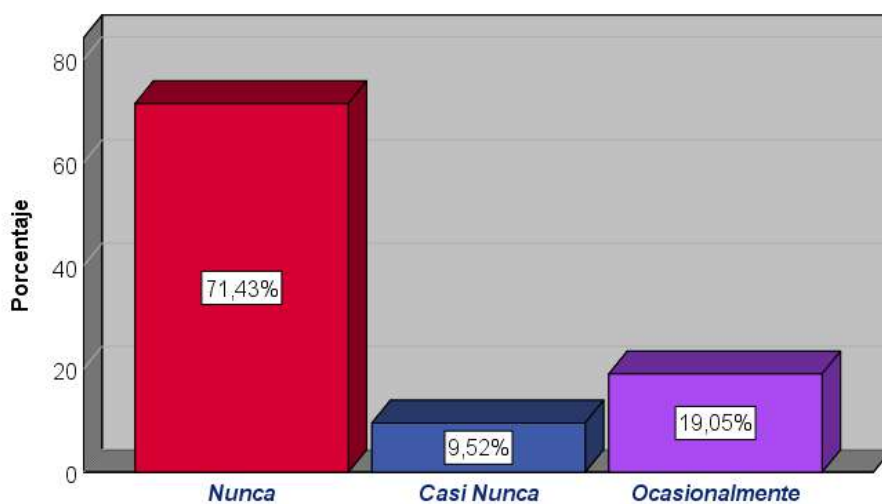


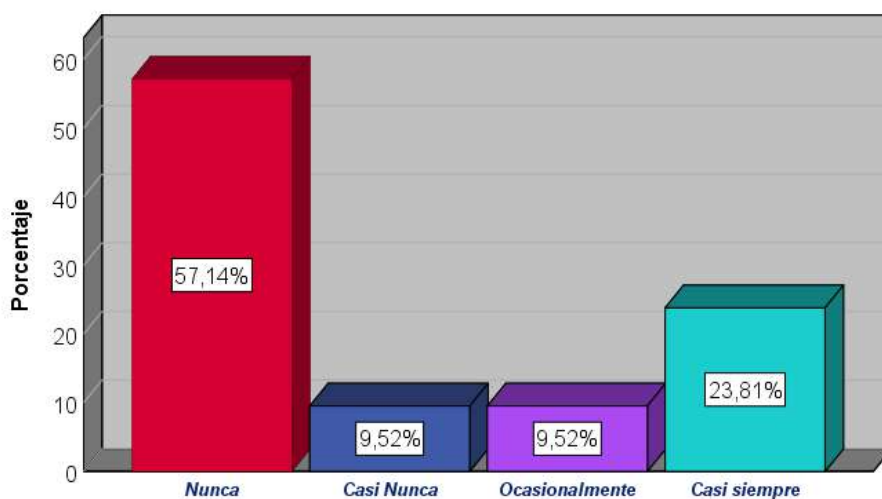
Figura 13 - A visualizado o conoce casos de intentos de suplantación de identidad digital

En la tabla 13 se observa que el 71.4% respondió que **nunca** ha visualizado o conoce casos de intentos de suplantación de identidad digital, seguido de un 9.5% respondió que **casi nunca** ha visualizado o conoce casos de intentos de suplantación de identidad digital. Por otro lado, un 19.0% manifestó que **ocasionalmente** ha visualizado o conoce casos de intentos de suplantación de identidad digital.

Tabla 14*Medidas activas de protección de datos informáticos personales*

		Frecuenci	Porcenta	Porcentaje	Porcentaje
		a	je	válido	acumulado
Válid	Nunca	78	57,1	57,1	57,1
	Casi Nunca	13	9,5	9,5	66,7
	Ocasionalmen	13	9,5	9,5	76,2
	te				
	Casi siempre	31	23,8	23,8	100,0
	Total	135	100,0	100,0	

Fuente: De investigación propia.

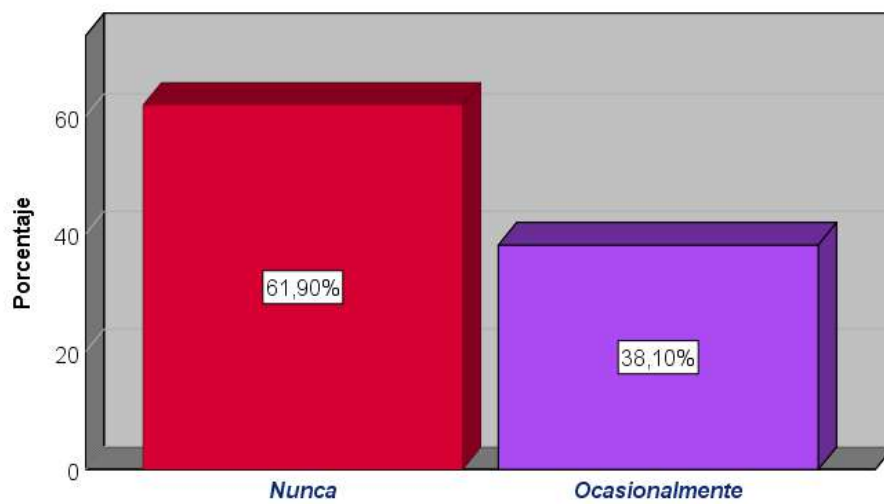
*Figura 14 - Medidas activas de protección de datos informáticos personales*

En la tabla 14 se observa que el 57.1% respondió que **nunca** toma medidas activas de protección de datos informáticos personales, seguido de un 9.5% que respondió que **casi nunca** toma medidas activas de protección de datos informáticos personales. Por otro lado, un 9.5% respondió que **ocasionalmente** toma medidas activas de protección de datos informáticos personales y por último un 23.8% manifestó que **casi siempre** toma medidas activas de protección de datos informáticos personales.

Tabla 15*Revisión de su configuración de privacidad en redes sociales*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	83	61,9	61,9	61,9
	Ocasionalmente	52	38,1	38,1	100,0
	Total	135	100,0	100,0	

Fuente: De investigación propia.

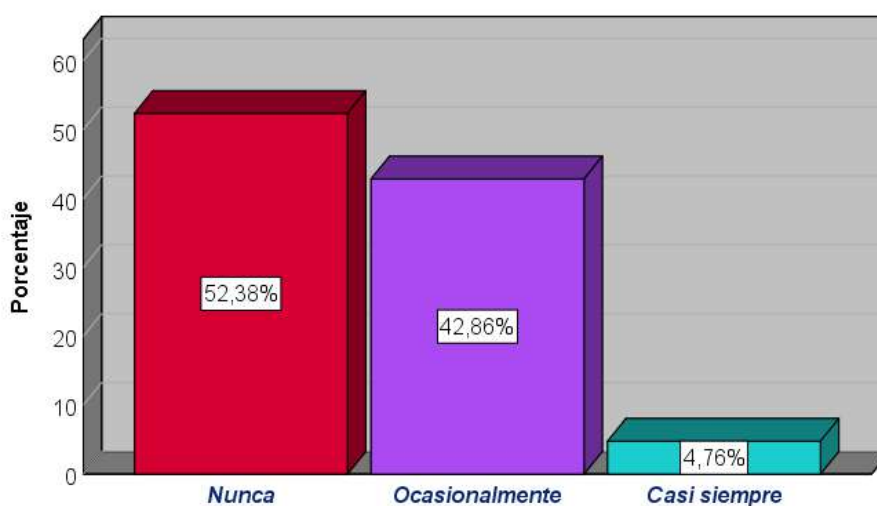
*Figura 15 - Revisión de su configuración de privacidad en redes sociales*

En la tabla 15 se observa que el 61.9% respondió que **nunca** revisa su configuración de privacidad en redes sociales y por otro lado, un 38.1% respondió que **ocasionalmente** revisa su configuración de privacidad en redes sociales.

Tabla 16*Preocupación por el uso indebido de datos personales en línea*

		Frecuenci a	Porcenta je	Porcentaje válido	Porcentaje acumulado
Válid o	Nunca	71	52,4	52,4	52,4
	Ocasionalmen te	58	42,9	42,9	95,2
	Casi siempre	6	4,8	4,8	100,0
	Total	135	100,0	100,0	

Fuente: De investigación propia.

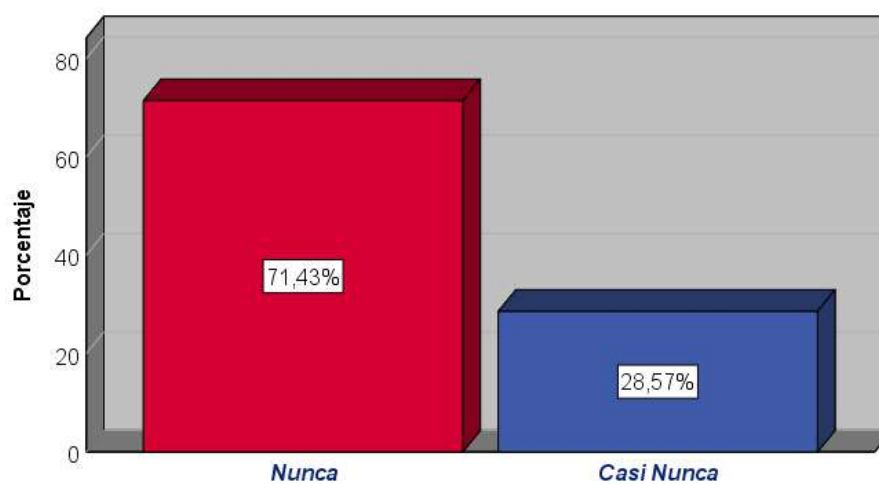
*Figura 16 - Preocupación por el uso indebido de datos personales en línea*

En la tabla 16 se observa que el 52.4% respondió que **nunca** se preocupa por el uso indebido de datos personales en línea. Por otro lado, un 42.9% respondió que **ocasionalmente** se preocupa por el uso indebido de datos personales en línea. Por último, un 4.8% manifestó que **casi siempre** se preocupa por el uso indebido de datos personales en línea.

Tabla 17*Frecuencia de compartir información personal sensible en línea*

		Frecuencia	Porcenta je	Porcentaje válido	Porcentaje acumulado
Válid o	Nunca	96	71,4	71,4	71,4
	Casi Nunca	39	28,6	28,6	100,0
	Total	135	100,0	100,0	

Fuente: De investigación propia.

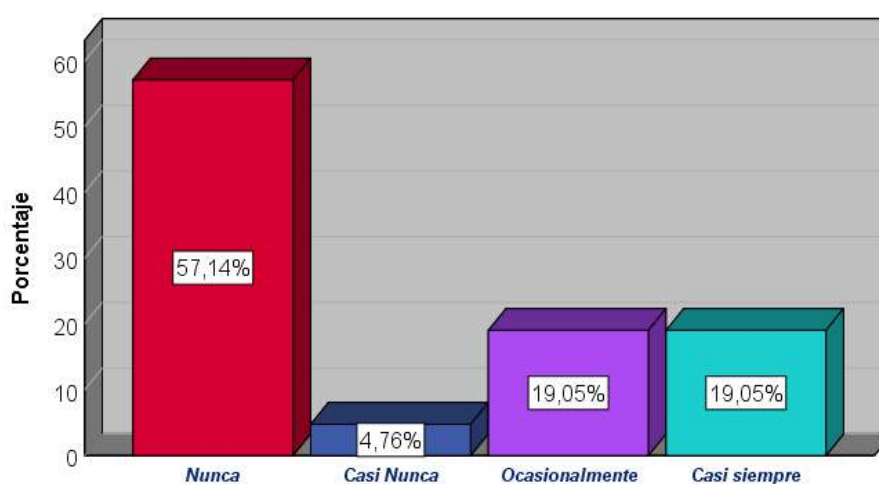
*Figura 17 - Frecuencia de compartir información personal sensible en línea*

En la tabla 17 se observa que el 71.4% respondió que **nunca** comparte información personal sensible en línea, seguido de un 28.6% respondió que **casi nunca** comparte información personal sensible en línea.

Tabla 18*Verificación de la autenticidad de las fuentes antes de compartir información en línea*

		Frecuenci a	Porcenta je	Porcentaje válido	Porcentaje acumulado
Válid o	Nunca	77	57,1	57,1	57,1
	Casi Nunca	6	4,8	4,8	61,9
	Ocasionalmen te	26	19,0	19,0	81,0
	Casi siempre	26	19,0	19,0	100,0
	Total	135	100,0	100,0	

Fuente: De investigación propia.

**Figura 18 - Verificación de la autenticidad de las fuentes antes de compartir información en línea**

En la tabla 18 se observa que el 57.1% respondió que **nunca** verifica la autenticidad de las fuentes antes de compartir información en línea, seguido de un 4.8% respondió que **casi nunca** verifica la autenticidad de las fuentes antes de compartir información en línea.

Por otro lado, un 19.0% verifica la autenticidad de las fuentes antes de compartir información en línea **ocasionalmente** verifica la autenticidad de las fuentes antes de compartir información en línea, sumado a ello un 19.0% manifestó que **casi siempre** verifica la autenticidad de las fuentes antes de compartir información en línea.

Tabla 19

Implementación de medidas eficaces por parte de las autoridades locales para proteger los derechos digitales.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	58	24,3	42,9	42,9
	Casi Nunca	71	29,7	52,4	95,2
	Ocasionalmente	6	2,7	4,8	100,0
	Total	135	56,8	100,0	

Fuente: De investigación propia.

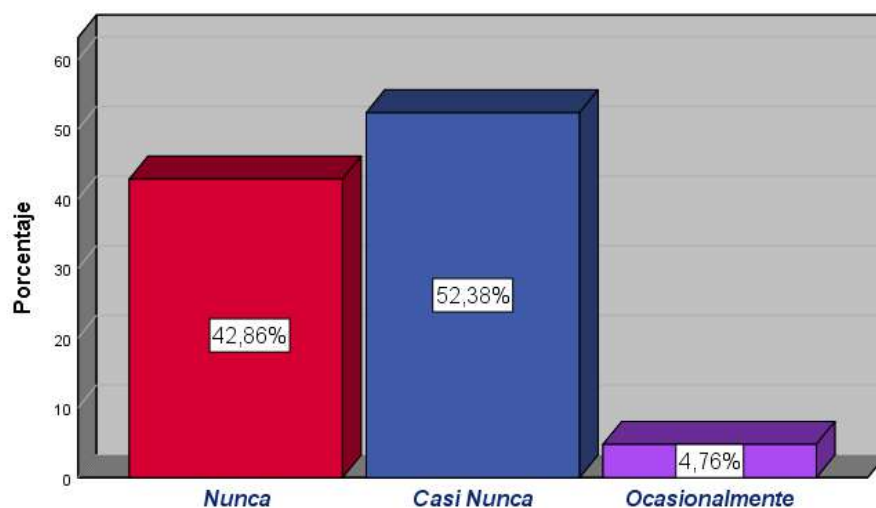


Figura 19 - Implementación de medidas eficaces por parte de las autoridades locales para proteger los derechos digitales.

En la **Tabla 19** se observa que el 42.9% de los encuestados señaló que **nunca** las autoridades locales implementan medidas eficaces para proteger los derechos digitales, reflejando una percepción de ineficiencia en las acciones tomadas. Por otro lado, un 52.4% indicó que **casi nunca** perciben tales medidas, lo cual refuerza la falta de confianza en las autoridades. Finalmente, un 4.8% manifestó que **ocasionalmente** se implementan acciones, aunque estos resultados reflejan un esfuerzo insuficiente en la gestión y promoción de medidas efectivas.

Tabla 20

Garantía de protección adecuada a través de las leyes actuales sobre derechos digitales.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	70	29,7	52,4	52,4
	Casi Nunca	52	21,6	38,1	90,5
	Ocasionalmente	13	5,4	9,5	100,0
	Total	135	56,8	100,0	

Fuente: De investigación propia.

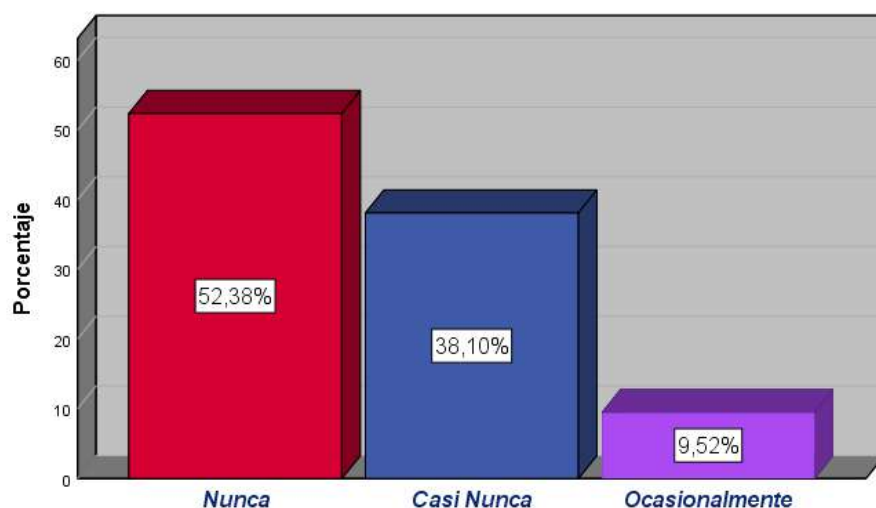


Figura 20 - Garantía de protección adecuada a través de las leyes actuales sobre derechos digitales.

La **Tabla 20** muestra que el 52.4% de los encuestados consideró que las leyes actuales **nunca** garantizan protección adecuada a sus derechos digitales, mientras que un 38.1% señaló que **casi nunca** sienten esta garantía. Solo un 9.5% mencionó que **ocasionalmente** las leyes cumplen esta función. Estos resultados evidencian una percepción generalizada de ineficiencia en la legislación vigente y la necesidad de reformas que aseguren una protección efectiva de los derechos digitales de los ciudadanos.

Tabla 21

Participación ciudadana en iniciativas gubernamentales para fortalecer la protección de derechos digitales.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	135	100,0	100,0	100,0
Total		135			

Fuente: De investigación propia.

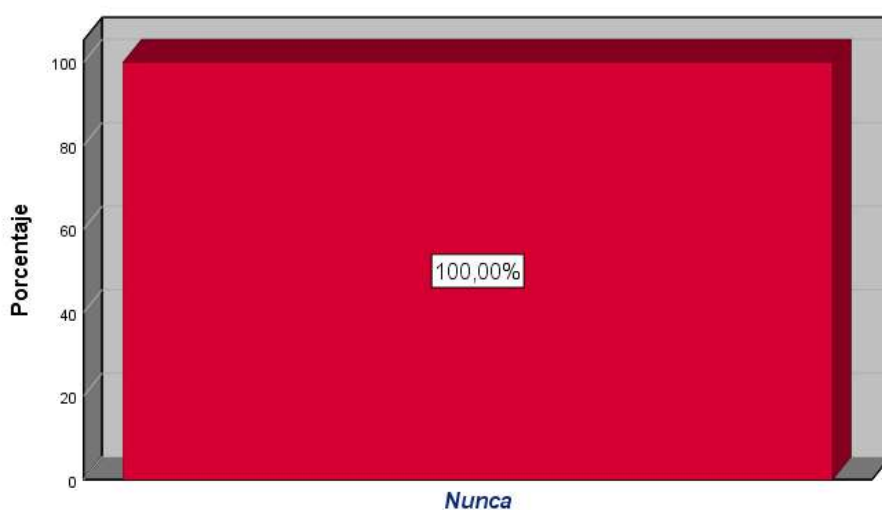


Figura 21 - Participación ciudadana en iniciativas gubernamentales para fortalecer la protección de derechos digitales.

En la **Tabla 21** se evidencia que el 100% de los encuestados respondió que **nunca** ha participado en iniciativas gubernamentales para fortalecer la protección de los derechos digitales. Esta cifra revela una ausencia total de vinculación entre la ciudadanía y las políticas públicas relacionadas con los derechos digitales, lo que puede atribuirse a la falta de difusión, oportunidades de participación y estrategias efectivas que promuevan la inclusión activa de la población.

Tabla 22

Confianza en las herramientas tecnológicas como medio para prevenir vulneraciones digitales.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	91	37,8	66,7	66,7
	Casi Nunca	18	8,1	14,3	81,0
	Ocasionalmente	26	10,8	19,0	100,0
	Total	135	56,8	100,0	

Fuente: De investigación propia.

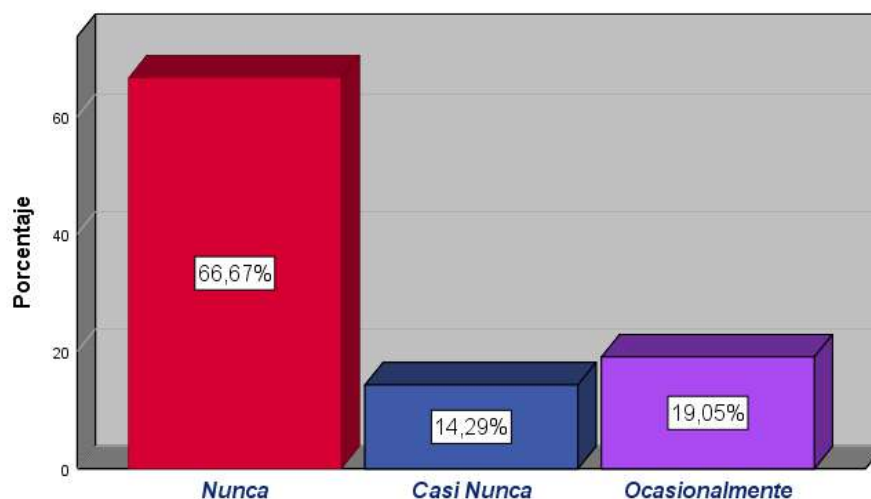


Figura 22 - Confianza en las herramientas tecnológicas como medio para prevenir vulneraciones digitales.

La **Tabla 22** refleja que el 66.7% de los encuestados indicó que **nunca** confían en las herramientas tecnológicas para prevenir vulneraciones a sus derechos digitales. A esto se suma un 14.3% que mencionó que **casi nunca** tiene confianza en estas herramientas. Por otro lado, un 19% respondió que **ocasionalmente** confían en ellas. Los datos sugieren un bajo nivel de confianza en la tecnología disponible, lo cual podría estar asociado con experiencias negativas previas o desconocimiento de su funcionamiento.

Tabla 23

Información constante sobre las leyes que protegen los derechos digitales.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	70	29,7	52,4	52,4
	Casi Nunca	65	27,0	47,6	100,0
	Total	135	56,8	100,0	

Fuente: De investigación propia.

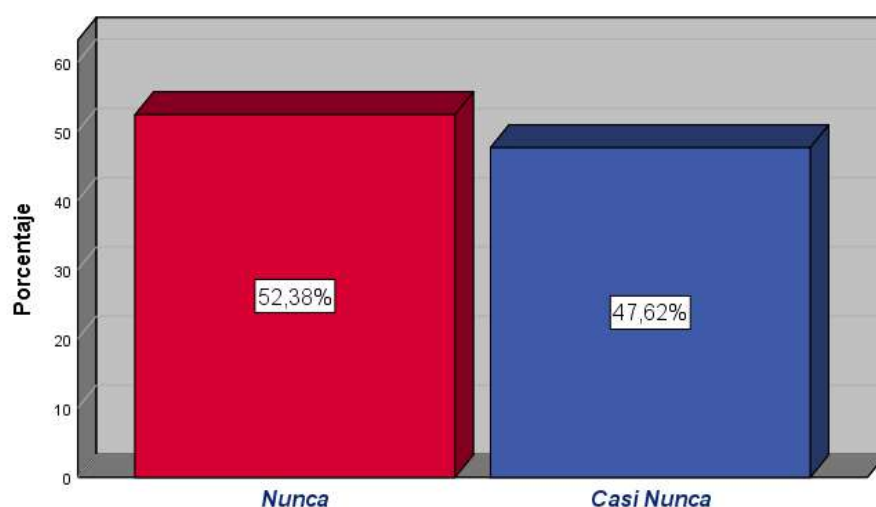


Figura 23 - Información constante sobre las leyes que protegen los derechos digitales.

En la **Tabla 23**, el 52.4% manifestó que **nunca** recibe información constante sobre las leyes que protegen los derechos digitales, mientras que un 47.6% indicó que **casi nunca** accede a este tipo de información. Estos resultados evidencian una falta de comunicación efectiva entre las autoridades y la ciudadanía, lo que podría estar limitando el conocimiento general sobre los derechos digitales y las legislaciones vigentes.

Tabla 24

Efectividad de las leyes actuales para la protección de los derechos en línea.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	58	24,3	42,9	42,9
	Casi Nunca	32	13,5	23,8	66,7
	Ocasionalmente	45	18,9	33,3	100,0
	Total	135	56,8	100,0	

Fuente: De investigación propia.

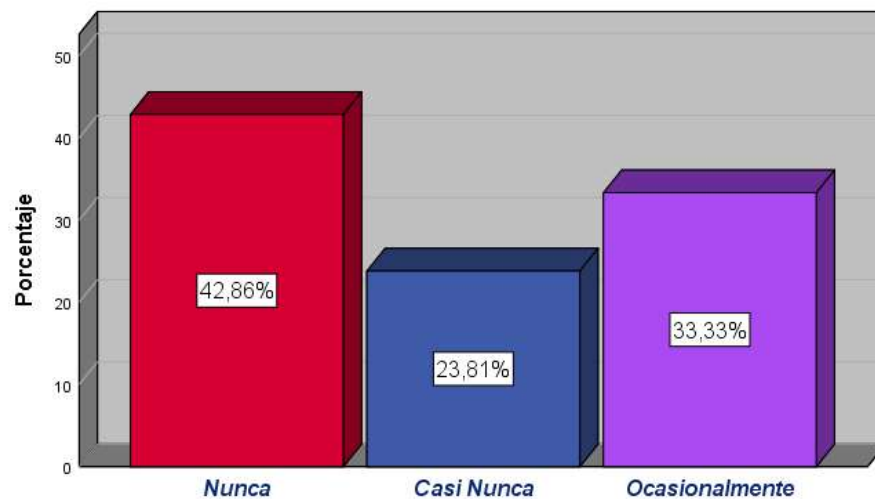


Figura 24 - Efectividad de las leyes actuales para la protección de los derechos en línea.

En la **Tabla 24** se observa que el 42.9% respondió que las leyes actuales **nunca** son efectivas para proteger los derechos en línea. Además, un 23.8% manifestó que **casi nunca** son efectivas, mientras que un 33.3% indicó que **ocasionalmente** cumplen con su objetivo. Estos datos reflejan una percepción de ineficiencia en la legislación y la necesidad de fortalecer su aplicación y difusión para garantizar una protección más efectiva.

Tabla 25

Frecuencia con la que las personas experimentan vulneraciones a sus derechos digitales.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	110	45,9	81,0	81,0
	Casi Nunca	19	8,1	14,3	95,2
	Ocasionalmente	6	2,7	4,8	100,0
	Total	135	56,8	100,0	

Fuente: De investigación propia.

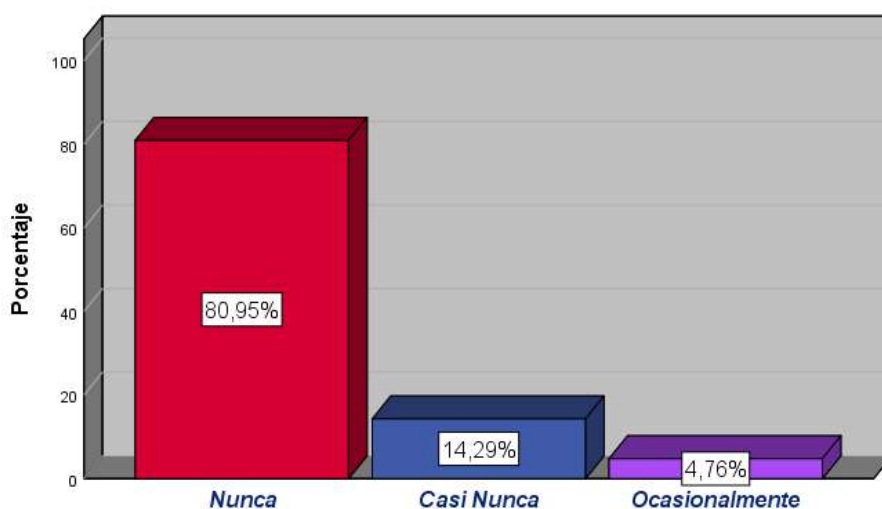


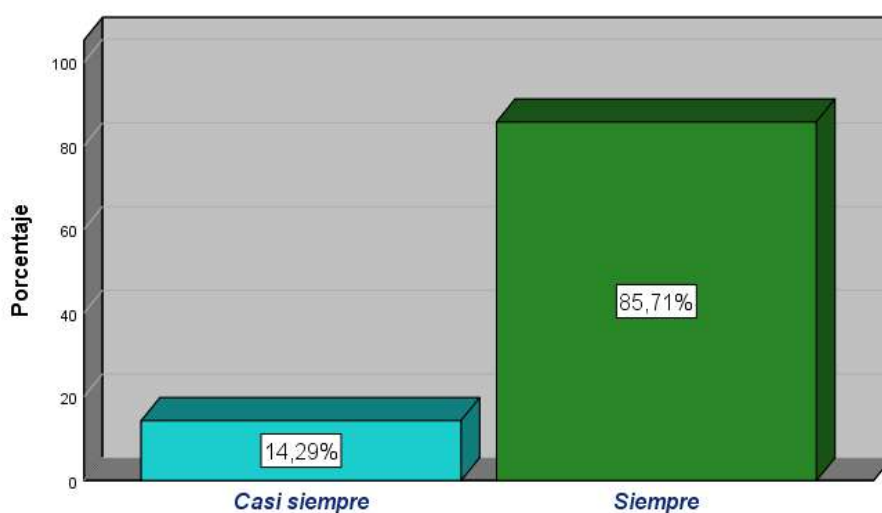
Figura 25 - Frecuencia con la que las personas experimentan vulneraciones a sus derechos digitales.

En la **Tabla 25**, el 81% de los encuestados indicó que **nunca** ha experimentado vulneraciones a sus derechos digitales, seguido de un 14.3% que señaló que **casi nunca** le ha sucedido. Por otro lado, un 4.8% manifestó que **ocasionalmente** ha sido víctima de vulneraciones. Estos resultados sugieren que, si bien la mayoría no ha tenido experiencias negativas, existe un pequeño porcentaje que sí ha enfrentado estas situaciones, lo que subraya la necesidad de medidas preventivas más robustas.

Tabla 26*Promoción de la educación sobre derechos digitales por parte de las autoridades.*

		Frecuen cia	Porcent aje	Porcentaje válido	Porcentaje acumulado
Válido	Casi siempre	18	8,1	14,3	14,3
	Siempre	117	48,6	85,7	100,0
	Total	135	56,8	100,0	

Fuente: De investigación propia.

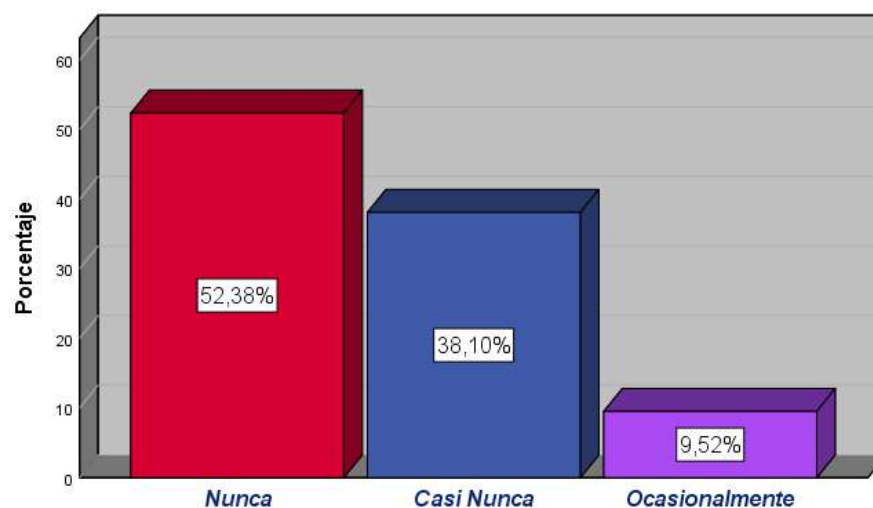
*Figura 26 - Promoción de la educación sobre derechos digitales por parte de las autoridades.*

En la **Tabla 26**, el 85.7% de los encuestados afirmó que las autoridades **siempre** promueven la educación sobre derechos digitales, mientras que un 14.3% señaló que esto ocurre **casi siempre**. Los resultados reflejan una percepción positiva en cuanto a la promoción educativa, lo cual es alentador, aunque se requiere mantener y fortalecer estos esfuerzos a largo plazo.

Tabla 27*Conocimiento de medidas de seguridad necesarias para prevenir ataques cibernéticos.*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	70	29,7	52,4	52,4
	Casi Nunca	52	21,6	38,1	90,5
	Ocasionalmente	13	5,4	9,5	100,0
	Total	135	56,8	100,0	

Fuente: De investigación propia.

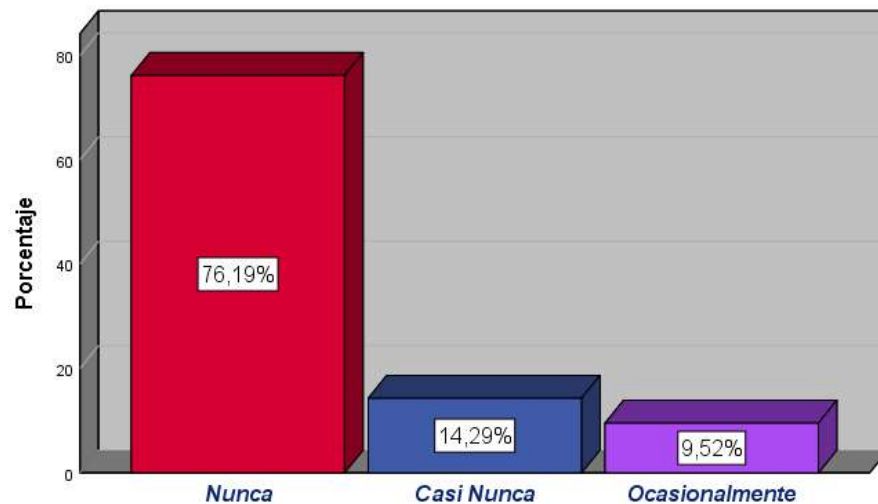
*Figura 27 - Conocimiento de medidas de seguridad necesarias para prevenir ataques cibernéticos.*

La **Tabla 27** muestra que el 52.4% de los encuestados **nunca** conoce las medidas de seguridad necesarias para prevenir ataques cibernéticos, mientras que un 38.1% señaló que **casi nunca** las conoce. Por otro lado, solo un 9.5% indicó que **ocasionalmente** tiene este conocimiento. Estos datos reflejan una brecha considerable en la educación sobre ciberseguridad.

Tabla 28*Identificación de posibles vulneraciones a los derechos digitales personales.*

		Frecuen cia	Porcent aje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	104	43,2	76,2	76,2
	Casi Nunca	18	8,1	14,3	90,5
	Ocasionalme nte	13	5,4	9,5	100,0
	Total	135	56,8	100,0	

Fuente: De investigación propia.

*Figura 28 - Identificación de posibles vulneraciones a los derechos digitales personales.*

En la **Tabla 28**, el 76.2% respondió que **nunca** puede identificar vulneraciones a sus derechos digitales, seguido de un 14.3% que señaló que **casi nunca** puede hacerlo. Finalmente, un 9.5% indicó que **ocasionalmente** logra identificarlas. Esto revela la necesidad de mejorar las capacidades de la población para detectar posibles vulneraciones.

Tabla 29

Recepción de información educativa sobre ciberseguridad y derechos digitales por parte de las autoridades.

		Frecuen cia	Porcent aje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	129	54,1	95,2	95,2
	Casi Nunca	6	2,7	4,8	100,0
	Total	135	56,8	100,0	

Fuente: De investigación propia.

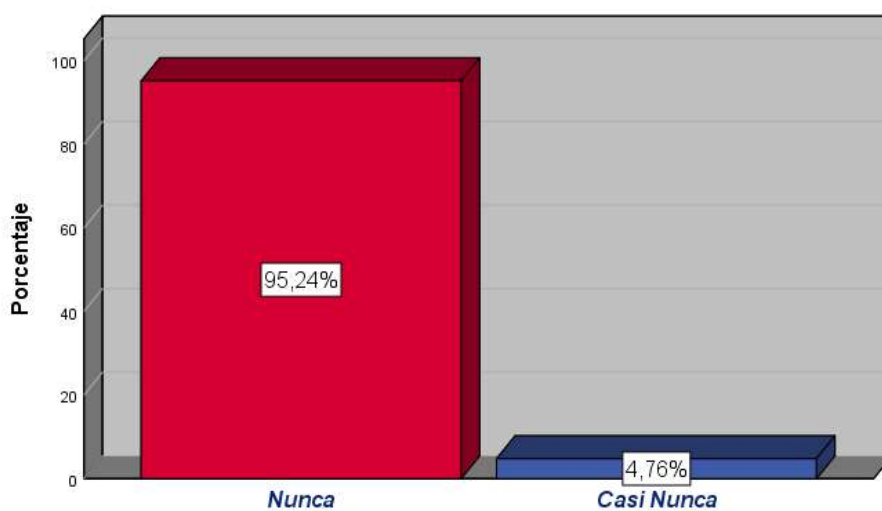


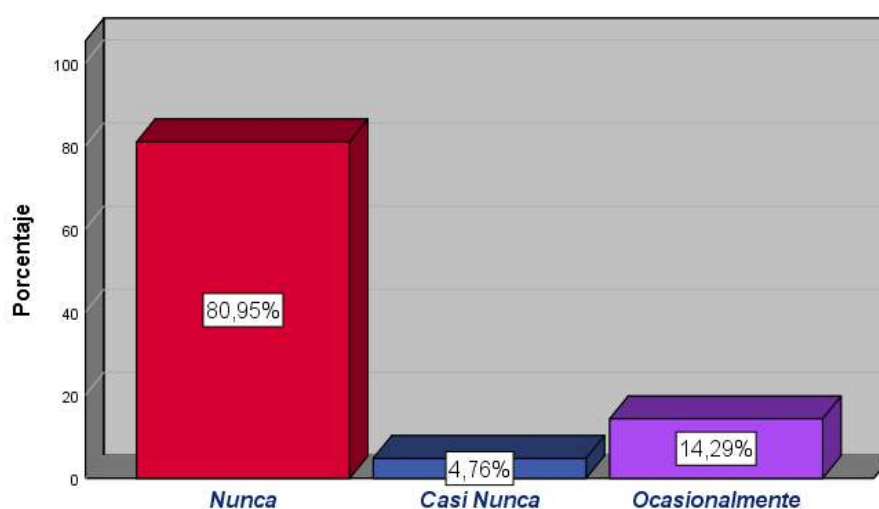
Figura 29 - Recepción de información educativa sobre ciberseguridad y derechos digitales por parte de las autoridades.

En la Tabla 29, el 95.2% de los encuestados indicó que **nunca** recibe información educativa sobre ciberseguridad y derechos digitales, mientras que un 4.8% señaló que **casi nunca** recibe este tipo de información. Estos datos revelan una grave deficiencia en las campañas educativas promovidas por las autoridades.

Tabla 30*Acceso a formación en ciberseguridad y protección de derechos digitales.*

		Frecuen cia	Porcent aje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	110	45,9	81,0	81,0
	Casi Nunca	6	2,7	4,8	85,7
	Ocasionalme nte	19	8,1	14,3	100,0
	Total	135	56,8	100,0	

Fuente: De investigación propia.

*Figura 30 - Acceso a formación en ciberseguridad y protección de derechos digitales.*

La **Tabla 30** refleja que el 81% de los encuestados **nunca** ha tenido acceso a formación en ciberseguridad y derechos digitales, mientras que un 14.3% indicó que **ocasionalmente** ha accedido a este tipo de formación. Estos resultados destacan la necesidad urgente de programas de capacitación accesibles.

Tabla 31

Participación en talleres o cursos sobre seguridad en línea como estrategia preventiva.

		Frecuen cia	Porcent aje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	135	100,0	100,0	100,0
Total		135			

Fuente: De investigación propia.

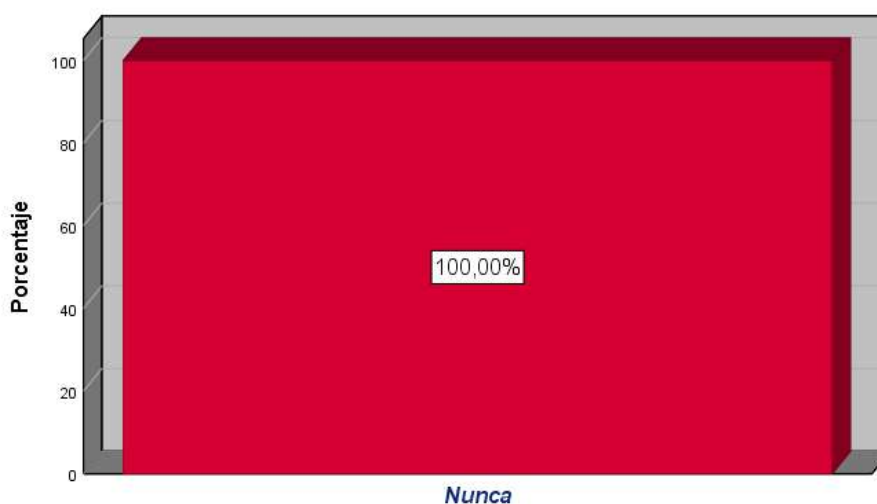


Figura 31 - Participación en talleres o cursos sobre seguridad en línea como estrategia preventiva.

En la Tabla 31, se observa que el 100% de los encuestados manifestó que **nunca** ha participado en talleres o cursos sobre seguridad en línea como estrategia preventiva. Estos resultados evidencian la falta total de oportunidades accesibles o programas efectivos que permitan a la población capacitarse en temas de seguridad digital, lo cual puede contribuir a una mayor vulnerabilidad ante los delitos informáticos.

Tabla 32

Importancia de la educación sobre seguridad en línea para reducir los delitos informáticos.

		Frecuen cia	Porcent aje	Porcentaje válido	Porcentaje acumulado
Válido	Casi siempre	44	18,9	33,3	33,3
	Siempre	91	37,8	66,7	100,0
	Total	135	56,8	100,0	

Fuente: De investigación propia.

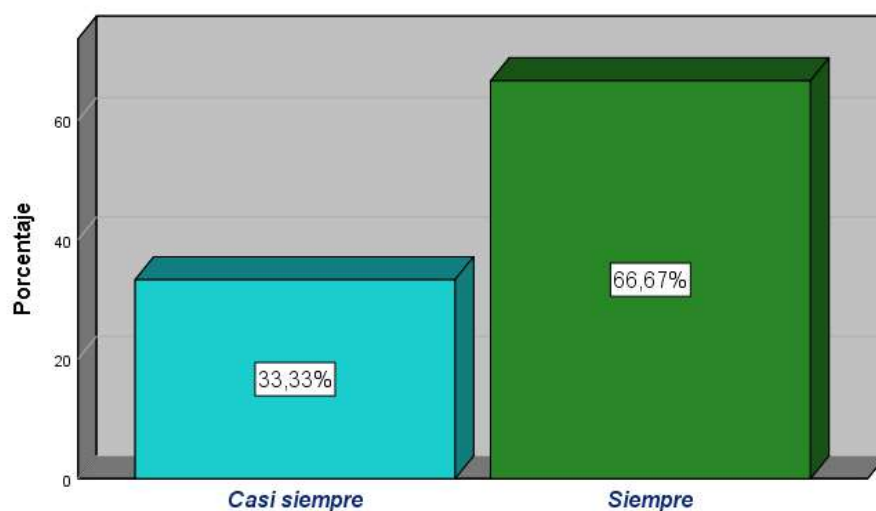


Figura 32 - Importancia de la educación sobre seguridad en línea para reducir los delitos informáticos.

En la **Tabla 32**, se destaca que el 66.7% de los encuestados consideró que la educación sobre seguridad en línea **siempre** es importante para reducir los delitos informáticos, mientras que un 33.3% indicó que esto ocurre **casi siempre**. Estos resultados reflejan un consenso positivo sobre la relevancia de la educación digital como herramienta preventiva, lo cual debería motivar a las autoridades a fortalecer y promover programas educativos en este ámbito.

Tabla 33

Uso de recursos en línea como medio para aprender sobre seguridad digital.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	45	18,9	33,3	33,3
	Casi Nunca	19	8,1	14,3	47,6
	Casi siempre	52	21,6	38,1	85,7
	Siempre	19	8,1	14,3	100,0
	Total	135	56,8	100,0	

Fuente: De investigación propia.

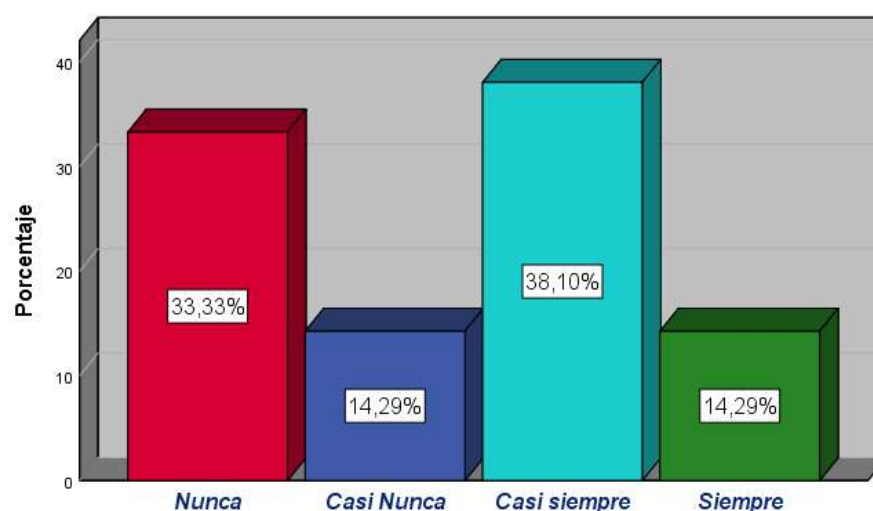


Figura 33 - Uso de recursos en línea como medio para aprender sobre seguridad digital.

La **Tabla 33** revela que el 33.3% de los encuestados **nunca** utiliza recursos en línea para aprender sobre seguridad digital, seguido de un 14.3% que señaló que **casi nunca** lo hace. Sin embargo, un 38.1% indicó que lo hace **casi siempre**, y un 14.3% mencionó que **siempre** utiliza estos recursos. Estos resultados muestran una división en la población, donde una parte reconoce el valor de los recursos en línea, mientras que otra no los utiliza, posiblemente por desconocimiento o falta de acceso.

Tabla 34*Inclusión de la educación sobre derechos digitales en los currículos escolares.*

		Frecuen cia	Porcent aje	Porcentaje válido	Porcentaje acumulado
Válido	Siemp re	135	100,0	100,0	100,0
Total		135			

Fuente: De investigación propia.

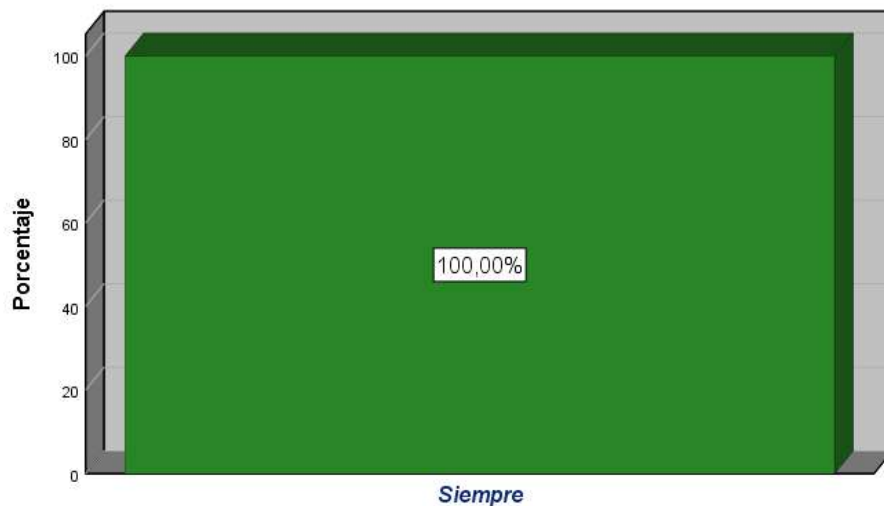


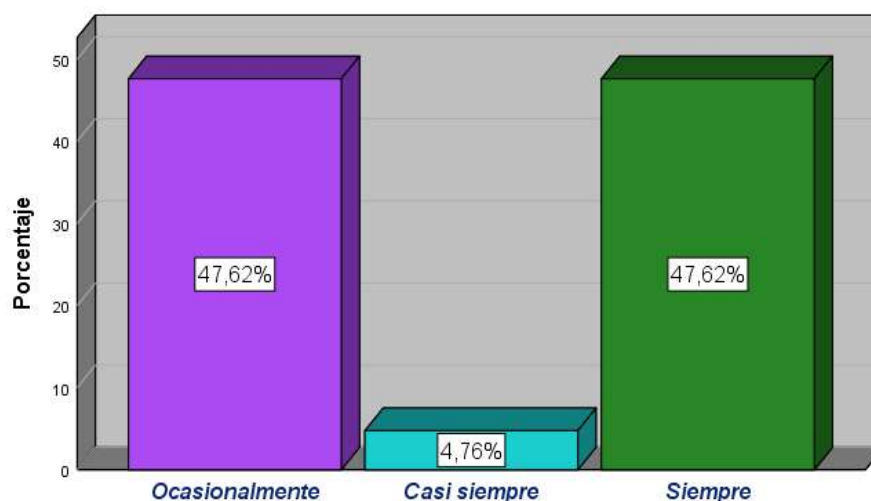
Figura 34 - Inclusión de la educación sobre derechos digitales en los currículos escolares.

En la Tabla 34, el 100% de los encuestados respondió que la educación sobre derechos digitales debe **siempre** estar incluida en los currículos escolares. Este consenso total refleja una percepción clara de que la formación desde edades tempranas es crucial para desarrollar habilidades y conocimientos que permitan a los ciudadanos protegerse en entornos digitales y prevenir vulneraciones.

Tabla 35*Preocupación por el acceso no autorizado a información personal en línea.*

		Frecuen cia	Porcent aje	Porcentaje válido	Porcentaje acumulado
Válido	Ocasionalme nte	65	27,0	47,6	47,6
	Casi siempre	5	2,7	4,8	52,4
	Siempre	65	27,0	47,6	100,0
	Total	135	56,8	100,0	

Fuente: De investigación propia.

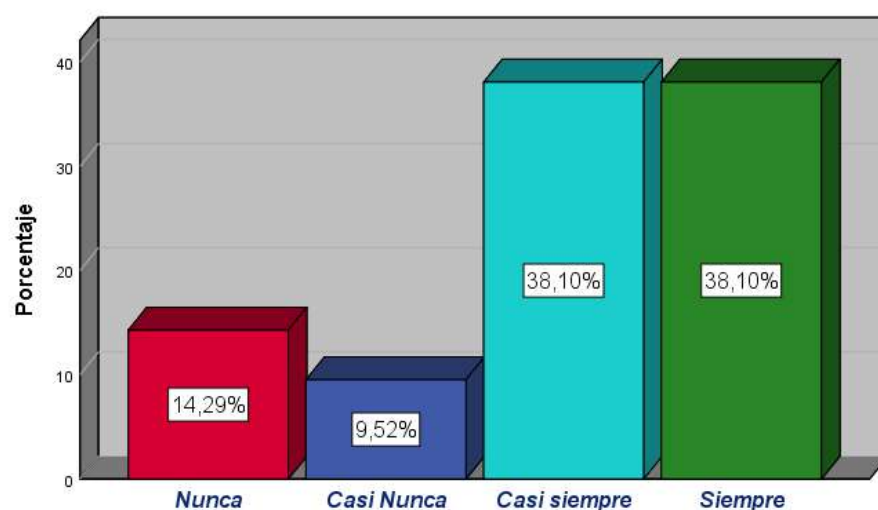
*Figura 35 - Preocupación por el acceso no autorizado a información personal en línea.*

La **Tabla 35** indica que el **47.6%** de los encuestados manifestó que **ocasionalmente** le preocupa el acceso no autorizado a su información personal en línea. Por otro lado, un **4.8%** señaló que esto ocurre **casi siempre**, y otro **47.6%** respondió que **siempre** tiene esta preocupación. Estos resultados demuestran que la mayoría de las personas tiene una percepción constante de riesgo en cuanto a la protección de sus datos personales en entornos digitales.

Tabla 36*Uso de mecanismos que garanticen la confidencialidad de la información personal.*

		Frecuen cia	Porcent aje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	18	8,1	14,3	14,3
	Casi Nunca	13	5,4	9,5	23,8
	Casi siempre	52	21,6	38,1	61,9
	Siempre	52	21,6	38,1	100,0
	Total	135	56,8	100,0	

Fuente: De investigación propia.

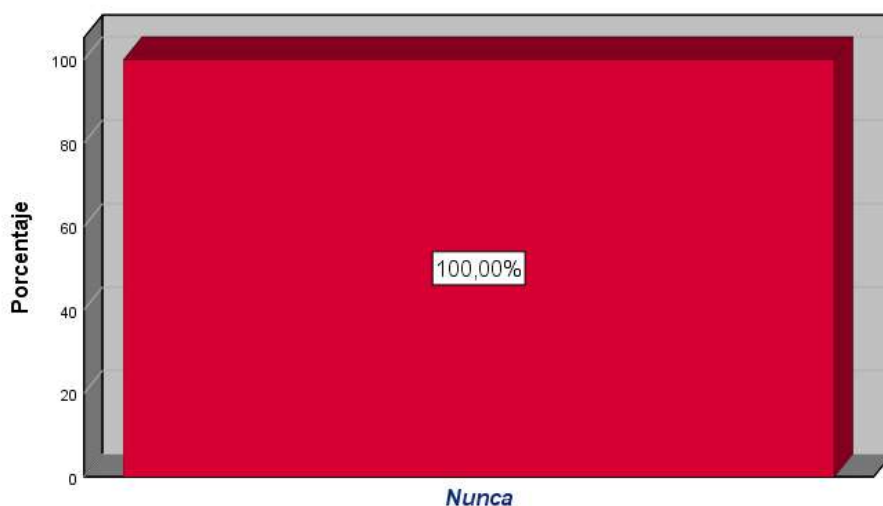
*Figura 36 - Uso de mecanismos que garanticen la confidencialidad de la información personal.*

En la Tabla 36, un 14.3% de los encuestados respondió que **nunca** utiliza mecanismos para proteger la confidencialidad de su información, seguido de un 9.5% que indicó que **casi nunca** lo hace. Por otro lado, un 38.1% señaló que **casi siempre** toma estas medidas, y un porcentaje igual, 38.1%, afirmó que lo hace **siempre**. Esto sugiere que, aunque existe un grupo considerablemente prevenido, aún hay personas que no implementan prácticas básicas de protección.

Tabla 37*Experiencia de divulgación no autorizada de información confidencial.*

		Frecuen cia	Porcent aje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	135	100,0	100,0	100,0
	a				
Total		135			

Fuente: De investigación propia.

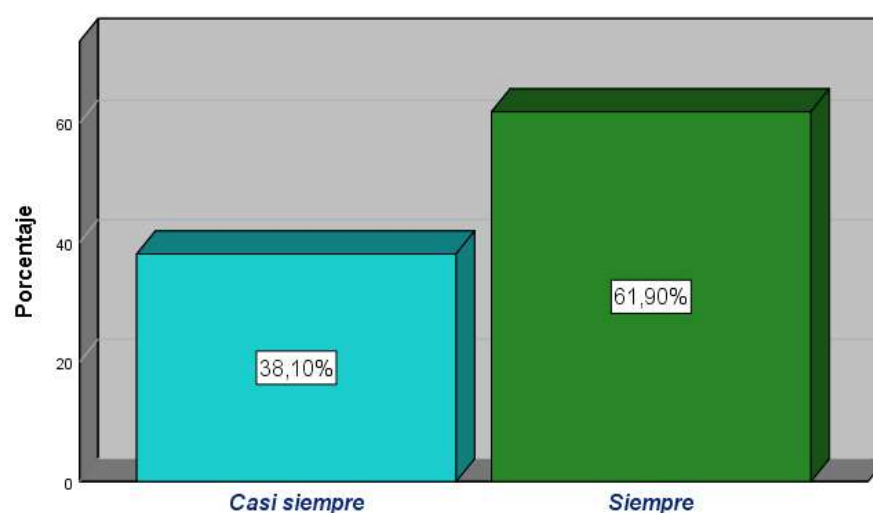
*Figura 37 - Experiencia de divulgación no autorizada de información confidencial.*

En la Tabla 37, el 100% de los encuestados respondió que **nunca** ha tenido experiencias de divulgación no autorizada de información confidencial. Esto podría indicar una percepción positiva respecto a la protección de la información personal, aunque también podría estar relacionada con un desconocimiento sobre posibles vulneraciones.

Tabla 38*Confianza en las plataformas digitales para proteger la confidencialidad de los datos.*

		Frecuen cia	Porcent aje	Porcentaje válido	Porcentaje acumulado
Válido	Casi siempre	52	21,6	38,1	38,1
	Siempre	83	35,1	61,9	100,0
	Total	135	56,8	100,0	

Fuente: De investigación propia.

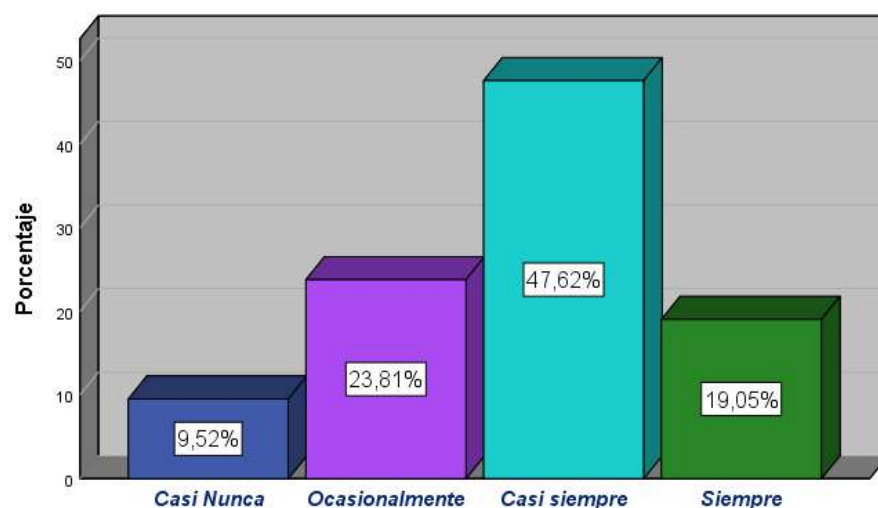
*Figura 38 - Confianza en las plataformas digitales para proteger la confidencialidad de los datos.*

En la **Tabla 38**, un **38.1%** de los encuestados expresó que **casi siempre** confía en que las plataformas digitales protegerán la confidencialidad de sus datos, mientras que un **61.9%** respondió que **siempre** confía en ellas. Estos resultados sugieren un alto grado de confianza en las plataformas digitales, lo cual es alentador, aunque esta confianza debe ser respaldada por medidas de seguridad eficaces para evitar vulneraciones.

Tabla 39*Sensación de seguridad al compartir información personal en entornos digitales.*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Casi Nunca	13	5,4	9,5	9,5
	Ocasionalmente	31	13,5	23,8	33,3
	Casi siempre	65	27,0	47,6	81,0
	Siempre	26	10,8	19,0	100,0
Total		135	100,0		

Fuente: De investigación propia.

*Figura 39 - Sensación de seguridad al compartir información personal en entornos digitales.*

En la **Tabla 39**, el **9.5%** indicó que **casi nunca** se siente seguro al compartir información personal en línea, seguido de un **23.8%** que manifestó que esto ocurre **ocasionalmente**. Por otro lado, un **47.6%** respondió que **casi siempre** se siente seguro, y un **19%** indicó que **siempre** tiene esta sensación. Estos datos reflejan una percepción mixta en torno a la seguridad digital, destacando la necesidad de fortalecer la confianza de los usuarios mediante prácticas seguras.

Tabla 40

Implementación de medidas para proteger la confidencialidad de la información en redes sociales.

		Frecuen cia	Porcent aje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	18	8,1	14,3	14,3
	Casi Nunca	91	37,8	66,7	81,0
	Ocasionalme nte	26	10,8	19,0	100,0
	Total	135	56,8	100,0	

Fuente: De investigación propia.

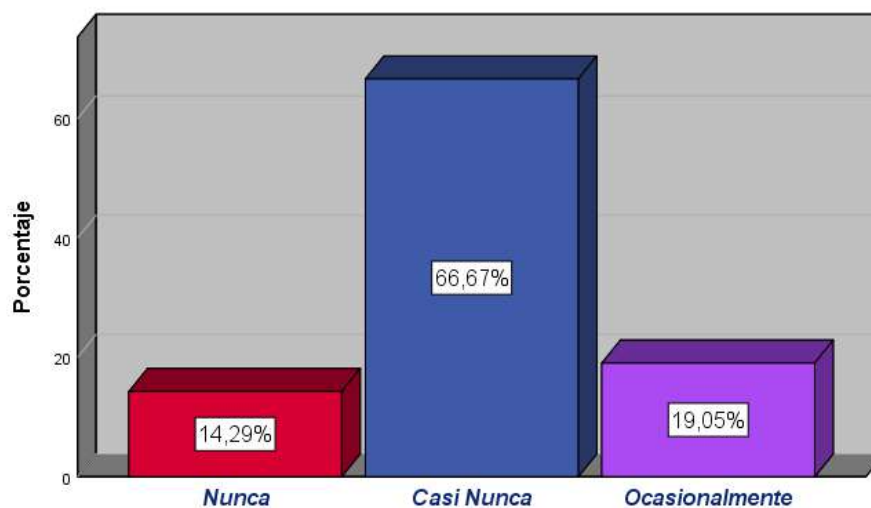


Figura 40 - Implementación de medidas para proteger la confidencialidad de la información en redes sociales.

En la **Tabla 40**, el **14.3%** de los encuestados indicó que **nunca** implementa medidas para proteger la confidencialidad de su información en redes sociales, mientras que un **66.7%** señaló que **casi nunca** lo hace. Finalmente, un **19%** mencionó que lo hace **ocasionalmente**, lo cual evidencia la necesidad de fomentar prácticas seguras y constantes en el uso de redes sociales.

Tabla 41

Revisión regular de las políticas de privacidad de las aplicaciones utilizadas.

		Frecuen cia	Porcent aje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	104	43,2	76,2	76,2
	Casi Nunca	31	13,5	23,8	100,0
	Total	135	56,8	100,0	

Fuente: De investigación propia.

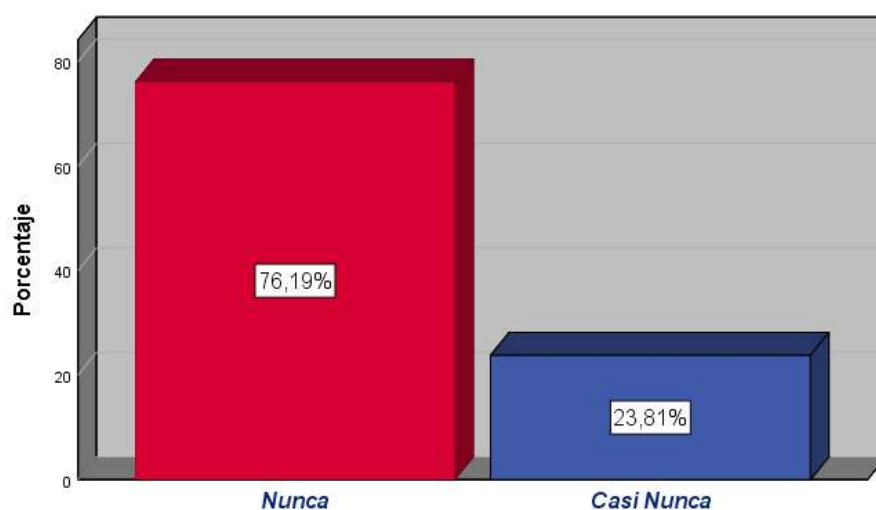


Figura 41 - Revisión regular de las políticas de privacidad de las aplicaciones utilizadas.

La **Tabla 41** muestra que el **76.2%** de los encuestados **nunca** revisa las políticas de privacidad de las aplicaciones que utiliza, mientras que un **23.8%** indicó que **casi nunca** lo hace. Estos resultados revelan una práctica preocupante que podría exponer a los usuarios a riesgos innecesarios debido al desconocimiento de cómo se gestionan sus datos personales en las plataformas digitales.

Tabla 42

Frecuencia con la que se experimenta divulgación no autorizada de información personal.

		Frecuen	Porcent	Porcentaje	Porcentaje acumulado
		cia	aje	válido	
Válido	Nunca	135	100,0	100,0	100,0
	Total	135			

Fuente: De investigación propia.

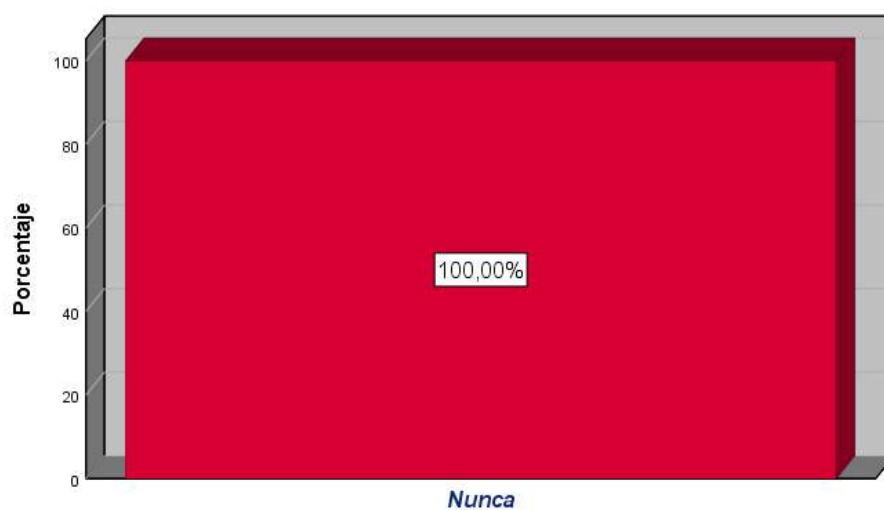


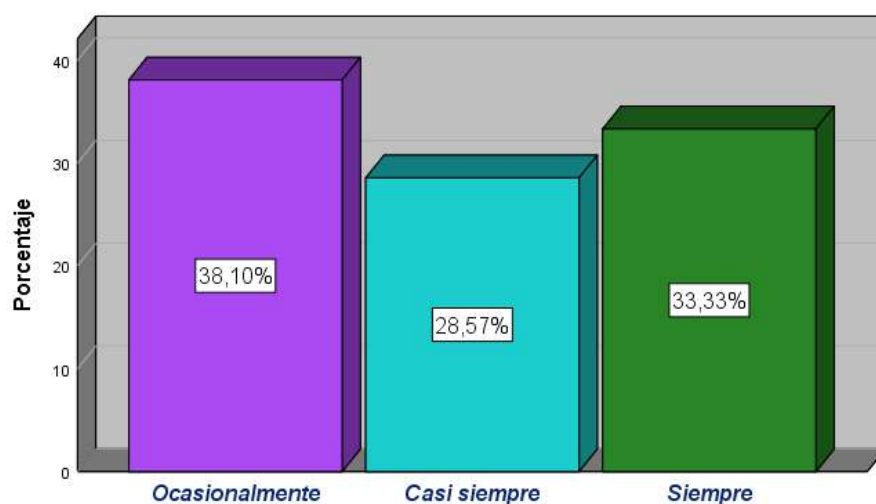
Figura 42 - Frecuencia con la que se experimenta divulgación no autorizada de información personal.

En la Tabla 42, el 100% de los encuestados manifestó que **nunca** ha experimentado divulgación no autorizada de información personal. Aunque el dato es positivo, también podría reflejar una falta de conocimiento sobre incidentes de este tipo, lo que subraya la necesidad de educar a la población sobre cómo identificar y prevenir estas situaciones.

Tabla 43*Preocupación por la modificación no autorizada de información digital.*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Ocasionalmente	52	21,6	38,1	38,1
	Casi siempre	39	16,2	28,6	66,7
	Siempre	44	18,9	33,3	100,0
	Total	135	56,8	100,0	

Fuente: De investigación propia.

*Figura 43 - Preocupación por la modificación no autorizada de información digital.*

En la Tabla 43, el 38.1% señaló que **ocasionalmente** le preocupa la modificación no autorizada de su información digital, seguido de un 28.6% que manifestó que esta preocupación ocurre **casi siempre**. Por otro lado, un 33.3% respondió que **siempre** le preocupa. Esto refleja un nivel considerable de inquietud entre los usuarios respecto a la integridad de su información digital y la necesidad de medidas para garantizar su protección.

Tabla 44

Implementación de medidas para proteger la integridad de la información personal en línea.

		Frecuen	Porcent	Porcentaje	Porcentaje
		cia	aje	válido	acumulado
Válido	Nunca	19	8,1	14,3	14,3
	Casi Nunca	84	35,1	61,9	76,2
	Ocasionalme nte	32	13,5	23,8	100,0
	Total	135	56,8	100,0	

Fuente: De investigación propia.

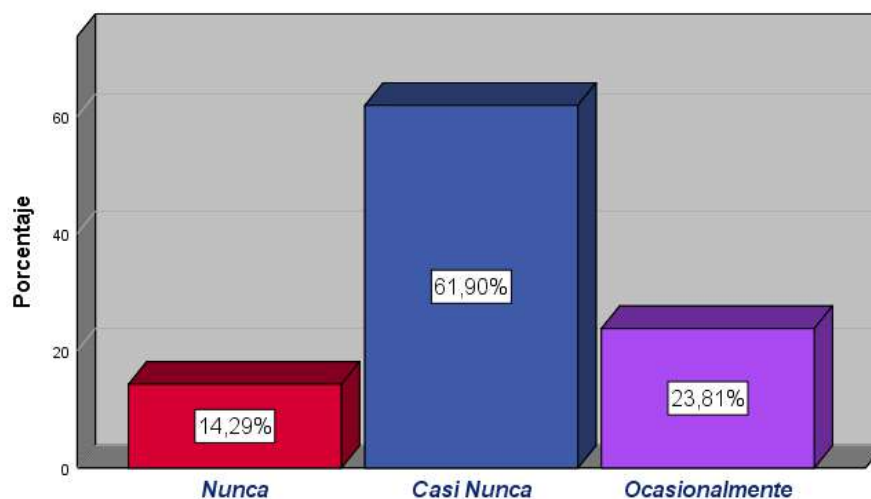


Figura 44 - Implementación de medidas para proteger la integridad de la información personal en línea.

En la Tabla 44, el 14.3% manifestó que **nunca** implementa medidas para proteger la integridad de su información personal, mientras que un 61.9% señaló que lo hace **casi nunca**. Un 23.8% indicó que **ocasionalmente** implementa estas medidas. Estos resultados reflejan un bajo nivel de prevención entre los usuarios, lo que podría incrementar el riesgo de manipulación de sus datos en línea.

Tabla 45

Detección de cambios no autorizados en datos personales o profesionales.

		Frecuen	Porcent	Porcentaje	Porcentaje acumulado
		cia	aje	válido	
Válido	Nunca	135	100,0	100,0	100,0
Total		135			

Fuente: De investigación propia.

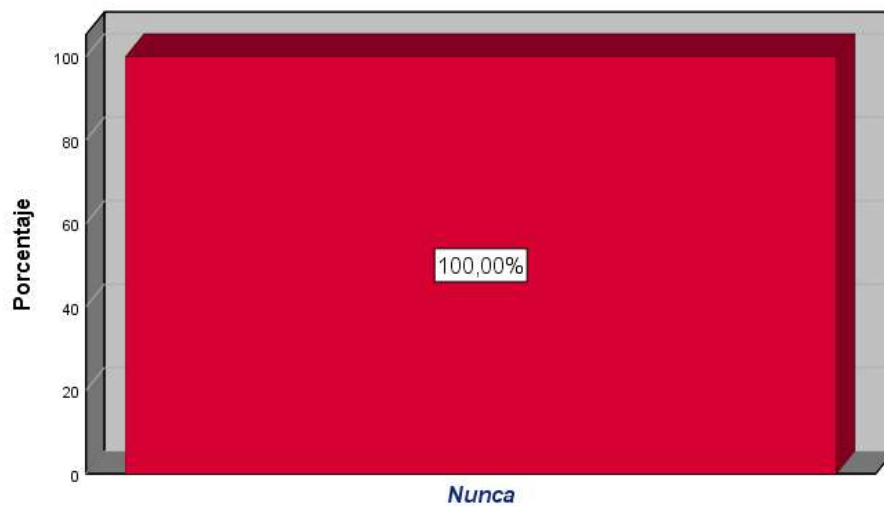


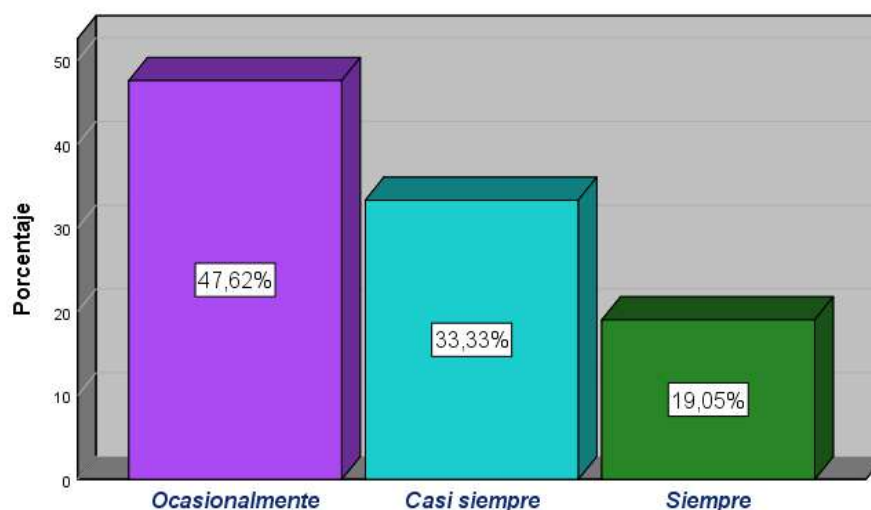
Figura 45 - Detección de cambios no autorizados en datos personales o profesionales.

En la Tabla 45, el 100% de los encuestados indicó que **nunca** ha detectado cambios no autorizados en sus datos personales o profesionales. Esto podría reflejar una percepción de seguridad o una falta de monitoreo activo de la información, lo que deja abierta la posibilidad de vulneraciones no detectadas.

Tabla 46*Confianza en las plataformas digitales para mantener la integridad de la información.*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Ocasionalmente	65	27,0	47,6	47,6
	Casi siempre	44	18,9	33,3	81,0
	Siempre	26	10,8	19,0	100,0
	Total	135	56,8	100,0	

Fuente: De investigación propia.

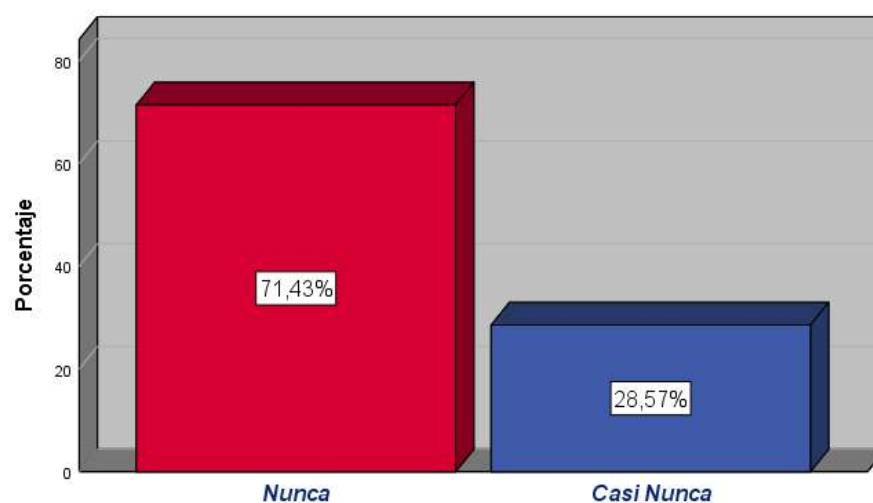
*Figura 46 - Confianza en las plataformas digitales para mantener la integridad de la información.*

En la **Tabla 46**, el **47.6%** respondió que **ocasionalmente** confía en que las plataformas digitales mantendrán la integridad de la información, seguido de un **33.3%** que indicó que esto ocurre **casi siempre**. Un **19%** manifestó que confía **siempre**, mostrando una percepción mixta respecto a la fiabilidad de las plataformas en la protección de la información.

Tabla 47*Verificación de la exactitud de la información recibida en línea.*

		Frecuen cia	Porcent aje	Porcentaje válido	Porcentaje acumulado
Válido	Nunca	96	40,5	71,4	71,4
	Casi Nunca	39	16,2	28,6	100,0
	Total	135	56,8	100,0	

Fuente: De investigación propia.

*Figura 47 - Verificación de la exactitud de la información recibida en línea.*

En la **Tabla 47**, el **71.4%** señaló que **nunca** verifica la exactitud de la información recibida en línea, mientras que un **28.6%** manifestó que lo hace **casi nunca**. Esto refleja una falta de hábito en la verificación de datos, lo cual puede contribuir a la propagación de información incorrecta y a la manipulación de los usuarios en entornos digitales.

Tabla 48

Identificación de información incorrecta o manipulada en cuentas o dispositivos digitales.

		Frecuen	Porcent	Porcentaje	Porcentaje acumulado
		cia	aje	válido	
Válido	Nunca	135	100,0	100,0	100,0
Total		135			

Fuente: De investigación propia.

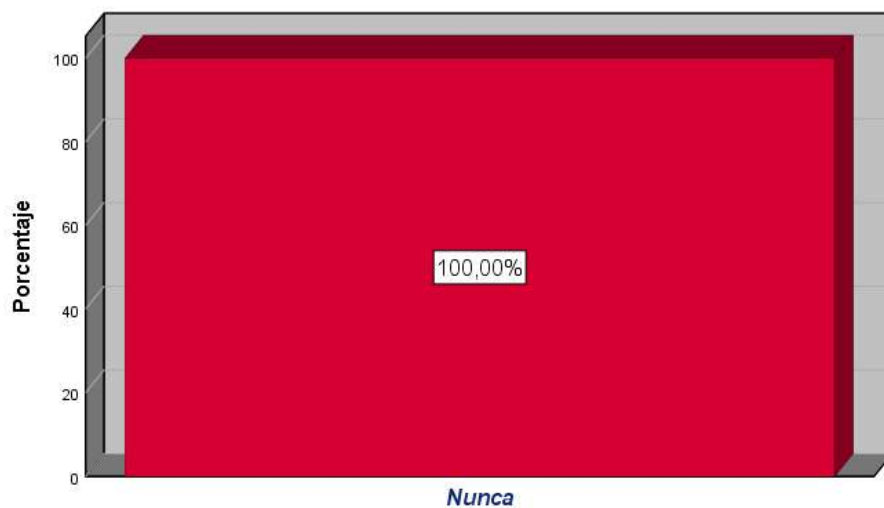


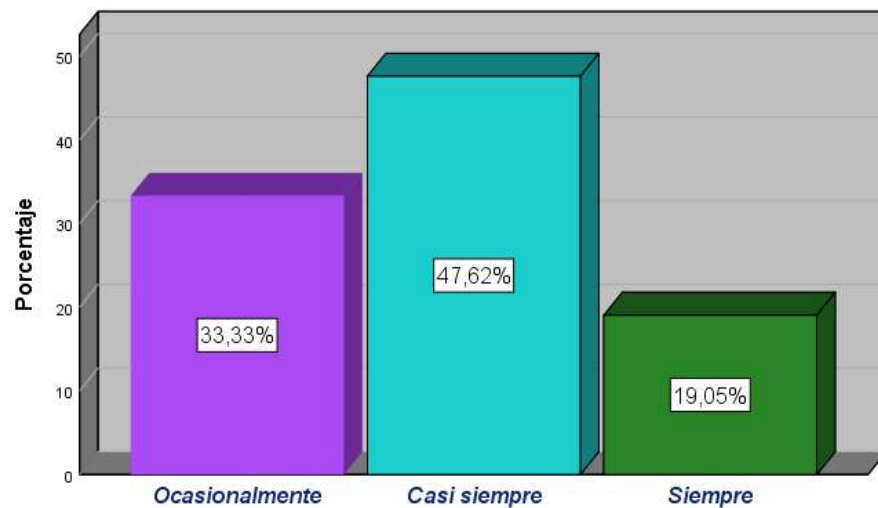
Figura 48 - Identificación de información incorrecta o manipulada en cuentas o dispositivos digitales.

En la Tabla 48, el 100% de los encuestados respondió que **nunca** ha identificado información incorrecta o manipulada en sus dispositivos digitales, lo que podría reflejar una falta de monitoreo activo o desconocimiento sobre cómo detectar posibles alteraciones en la información personal.

Tabla 49*Aseguramiento de que la información compartida en línea sea veraz.*

		Frecuen cia	Porcent aje	Porcentaje válido	Porcentaje acumulado
Válido	Ocasionalme nte	44	18,9	33,3	33,3
	Casi siempre	65	27,0	47,6	81,0
	Siempre	26	10,8	19,0	100,0
	Total	135	56,8	100,0	

Fuente: De investigación propia.

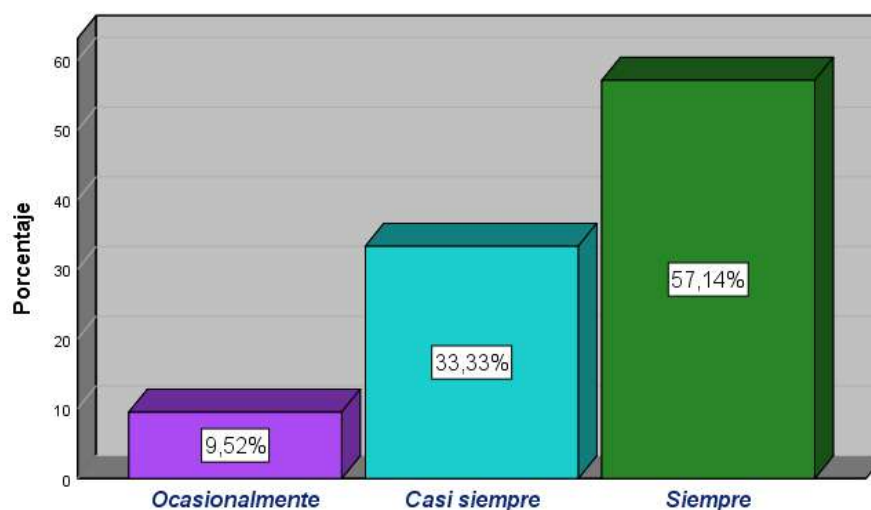
*Figura 49 - Aseguramiento de que la información compartida en línea sea veraz.*

La **Tabla 49** muestra que el **33.3%** indicó que **ocasionalmente** asegura que la información compartida en línea sea veraz, seguido de un **47.6%** que lo hace **casi siempre** y un **19%** que lo hace **siempre**. Esto sugiere que, aunque una parte de los encuestados toma medidas para garantizar la veracidad de su información, aún existe una proporción significativa que no lo hace de manera regular.

Tabla 50*Dificultad para detectar la manipulación de datos en entornos digitales.*

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Ocasionalmente	13	5,4	9,5	9,5
	Casi siempre	44	18,9	33,3	42,9
	Siempre	78	32,4	57,1	100,0
	Total	135	56,8	100,0	

Fuente: De investigación propia.

*Figura 50 - Dificultad para detectar la manipulación de datos en entornos digitales.*

En la Tabla 50, el 9.5% señaló que **ocasionalmente** encuentra difícil detectar la manipulación de datos en entornos digitales, mientras que un 33.3% indicó que esto ocurre **casi siempre**. Finalmente, un 57.1% afirmó que **siempre** tiene esta dificultad, lo que refleja una gran necesidad de desarrollar habilidades de detección y análisis crítico para identificar manipulaciones en la información digital.

4.2 Contratación de hipótesis

La contratación de la hipótesis general se realiza mediante análisis descriptivo de los resultados obtenidos a través del cuestionario aplicado a los estudiantes del Instituto de Idiomas de la UNJFSC. Dado que la investigación no formuló problemas específicos ni hipótesis específicas, la contratación se concentra en verificar si los datos empíricos permiten sostener la necesidad y pertinencia de criterios operativos de ciberseguridad basados en la cultura de autoprotección ciudadana para contribuir a la mitigación preventiva de delitos informáticos.

Los resultados evidencian que la población encuestada utiliza herramientas digitales de manera frecuente, pero no siempre adopta prácticas sistemáticas de seguridad, tales como actualización de mecanismos de protección, uso de contraseñas seguras, revisión de privacidad, verificación de fuentes, protección de datos personales y reconocimiento de intentos de fraude o suplantación digital. Esta situación confirma la existencia de una brecha entre el uso cotidiano de tecnologías digitales y la formación de hábitos de autoprotección, lo que incrementa la vulnerabilidad frente a delitos informáticos.

En ese sentido, la hipótesis general queda corroborada en términos descriptivos y propositivos, pues los hallazgos permiten afirmar que la accesibilidad cognitiva de la información preventiva, la sostenibilidad práctica de los hábitos digitales seguros, la proporcionalidad económica de las medidas de protección, la educación digital continua y la adopción de prácticas básicas de verificación, confidencialidad e integridad constituyen criterios necesarios para fortalecer la cultura de autoprotección ciudadana. No obstante, la investigación no demuestra una reducción estadística efectiva de denuncias o incidencia delictiva, debido a que no se aplicó un diseño experimental ni un estudio longitudinal antes-después. Por ello, la mitigación se entiende como reducción de vulnerabilidad y fortalecimiento de condiciones preventivas frente a riesgos informáticos.

Capítulo V : DISCUSIÓN

Los resultados obtenidos en la presente investigación permiten sostener que la problemática de los delitos informáticos en la ciudad de Huacho no puede ser comprendida únicamente desde una perspectiva tecnológica o jurídica, sino que exige una aproximación integral que incorpore de manera prioritaria el componente humano y conductual de la ciberseguridad. En efecto, el análisis de los datos evidencia que, si bien la población utiliza de forma frecuente herramientas digitales para actividades financieras, comerciales, educativas y de comunicación, aún persisten importantes debilidades relacionadas con la protección de la información personal, la verificación de contenidos digitales y la identificación de amenazas informáticas. Esta situación demuestra que el crecimiento de la digitalización no ha sido acompañado por un desarrollo proporcional de competencias orientadas a la autoprotección ciudadana, generando un escenario de vulnerabilidad que favorece la comisión de delitos informáticos.

Los hallazgos permiten advertir que una proporción significativa de los participantes presenta limitaciones para aplicar medidas de protección relacionadas con la confidencialidad, integridad y disponibilidad de la información, principios fundamentales de la ciberseguridad. La escasa verificación de la autenticidad de la información recibida, la reducida implementación de mecanismos de protección de datos personales y la dificultad para detectar posibles alteraciones o manipulaciones de la información constituyen indicadores que reflejan una débil cultura de seguridad digital. Desde una perspectiva práctica, ello significa que los ciudadanos continúan expuestos a diversas modalidades de ciberdelincuencia, tales como el phishing y otras formas de ingeniería social que se aprovechan de los errores humanos antes que de las vulnerabilidades tecnológicas.

Estos resultados guardan estrecha relación con los fundamentos teóricos desarrollados en la investigación. En ese sentido, la teoría de la ciberseguridad humana sostiene que el usuario constituye simultáneamente el principal factor de riesgo y el principal mecanismo de defensa dentro del ecosistema digital. Esta afirmación adquiere especial relevancia al analizar la realidad observada, pues se evidencia que el conocimiento básico sobre la existencia de amenazas informáticas no resulta suficiente para garantizar comportamientos seguros. La experiencia demuestra que muchos usuarios conocen la existencia de riesgos digitales, pero continúan desarrollando prácticas inseguras debido a la confianza excesiva, la falta de hábitos preventivos o la percepción errónea de que difícilmente serán víctimas de un ataque informático. Por consiguiente, la protección

efectiva no depende exclusivamente del acceso a la información, sino de la capacidad de transformar ese conocimiento en conductas permanentes de autoprotección.

En relación con los antecedentes analizados, los resultados obtenidos coinciden con lo señalado por Albarrán y Campos (2024), quienes concluyeron que el reconocimiento de los riesgos asociados al entorno digital no siempre genera modificaciones significativas en el comportamiento de los usuarios. De manera similar, los hallazgos confirman que la percepción de inseguridad en internet no necesariamente conduce a la adopción de medidas preventivas concretas. Esta situación evidencia que la formación en ciberseguridad debe trascender los enfoques meramente informativos para orientarse hacia el fortalecimiento de competencias prácticas y hábitos de protección sostenibles en el tiempo.

Asimismo, los resultados son consistentes con los aportes de Jancachagua Vera (2021), quien demostró que la efectividad de los ataques de phishing depende en gran medida del nivel de capacitación y concientización de las personas. En efecto, la investigación permite corroborar que la vulnerabilidad frente a los delitos informáticos no se encuentra determinada únicamente por aspectos técnicos, sino también por factores conductuales relacionados con la toma de decisiones del usuario. Desde esta perspectiva, la cultura de autoprotección ciudadana adquiere una importancia estratégica, ya que permite disminuir significativamente las posibilidades de éxito de los ciberdelincuentes mediante la adopción de prácticas básicas de seguridad digital.

Del mismo modo, los resultados obtenidos encuentran respaldo en los planteamientos de Correa Coronel (2022), quien concluyó que la ciberseguridad posee una incidencia significativa en la protección de los datos personales. En el contexto de la presente investigación, esta relación se manifiesta claramente al observar que las deficiencias en la aplicación de medidas de seguridad incrementan la exposición de los ciudadanos a diversas formas de afectación patrimonial y vulneración de la privacidad. En consecuencia, se reafirma la necesidad de fortalecer las capacidades de protección digital desde el ámbito ciudadano, especialmente en contextos locales donde la expansión tecnológica avanza con mayor rapidez que la educación en ciberseguridad.

Por otro lado, los hallazgos también permiten confirmar los planteamientos de Santos (2023), quien sostiene que las respuestas exclusivamente normativas resultan insuficientes para enfrentar eficazmente la criminalidad informática. Si bien el ordenamiento jurídico peruano cuenta con mecanismos legales para sancionar conductas tipificadas en la Ley N.º 30096, la realidad demuestra que la represión penal por sí sola no constituye una solución integral frente al problema. La naturaleza dinámica, transnacional y altamente especializada

de los delitos informáticos exige que las estrategias de prevención adquieran un rol prioritario dentro de las políticas de seguridad digital. En consecuencia, la participación activa de la ciudadanía se convierte en un elemento indispensable para fortalecer los mecanismos de protección frente a las amenazas emergentes del ciberespacio.

Desde una perspectiva criminológica, los resultados también pueden interpretarse a la luz de la teoría de las actividades rutinarias, según la cual la ocurrencia del delito depende de la convergencia entre un delincuente motivado, un objetivo adecuado y la ausencia de un guardián eficaz. En el ámbito digital, esta ausencia de vigilancia suele materializarse en la falta de conocimientos, habilidades y conductas preventivas por parte de los usuarios. Por ello, cuando la ciudadanía carece de criterios básicos para identificar amenazas, verificar información o proteger sus credenciales, se incrementan considerablemente las oportunidades para la comisión de delitos informáticos. En cambio, cuando los individuos desarrollan competencias de autoprotección, se reduce la probabilidad de victimización y se fortalece la capacidad de resistencia frente a los ataques cibernéticos.

En atención a lo expuesto, los resultados obtenidos permiten validar la hipótesis general de la investigación, de modo que la aplicabilidad de la ciberseguridad basada en la cultura de autoprotección ciudadana constituye un mecanismo viable para contribuir a la mitigación de los delitos informáticos en la ciudad de Huacho. Los datos empíricos demuestran que la principal necesidad no radica exclusivamente en la incorporación de nuevas herramientas tecnológicas, sino en el fortalecimiento de capacidades humanas que permitan a los ciudadanos actuar de manera preventiva frente a los riesgos digitales.

Finalmente, los resultados obtenidos deben interpretarse dentro de los límites metodológicos del estudio. La investigación no pretende sustituir los mecanismos penales de persecución del delito informático ni demostrar estadísticamente una reducción efectiva de denuncias, sino aportar criterios preventivos de ciberseguridad ciudadana a partir del diagnóstico de prácticas, percepciones y vulnerabilidades digitales observadas en la población encuestada. En tal sentido, la cultura de autoprotección ciudadana se presenta como un complemento necesario del marco normativo penal, en la medida en que permite actuar antes de la consumación del daño y reducir condiciones de exposición frente a modalidades como fraude informático, suplantación de identidad, acceso no autorizado y manipulación de datos personales.

Capítulo VI : CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

6.1.1 Primera conclusión

Se determinó que los criterios de aplicabilidad de ciberseguridad basada en la cultura de autoprotección ciudadana deben estructurarse sobre la accesibilidad cognitiva de la información preventiva, la sostenibilidad práctica de los hábitos digitales seguros, la proporcionalidad económica de las medidas de protección, la educación digital continua y la adopción de prácticas básicas de verificación, confidencialidad e integridad de la información. Estos criterios permiten orientar la mitigación preventiva de delitos informáticos en Huacho, especialmente frente a riesgos asociados al fraude informático, suplantación de identidad, acceso no autorizado y manipulación de datos personales.

6.1.2 Segunda conclusión

El diagnóstico realizado evidenció que el uso frecuente de herramientas digitales no garantiza, por sí mismo, una cultura de autoprotección ciudadana. La población encuestada presenta prácticas preventivas desiguales respecto del uso de contraseñas seguras, actualización de mecanismos de seguridad, revisión de privacidad, verificación de fuentes y protección de datos personales, lo que revela una brecha entre alfabetización digital operativa y alfabetización digital preventiva.

6.1.3 Tercera conclusión

La mitigación de delitos informáticos no puede depender exclusivamente de la respuesta penal posterior al hecho, debido a que muchas modalidades delictivas se consuman mediante engaño, descuido, confianza excesiva o falta de hábitos preventivos del usuario. Por ello, la cultura de autoprotección ciudadana constituye un componente preventivo necesario para reducir condiciones de vulnerabilidad frente a riesgos digitales.

6.1.4 Cuarta conclusión

Los resultados de la investigación permiten sostener que la educación digital continua, la formación en derechos digitales, la verificación crítica de información y la protección de datos personales deben ser consideradas medidas prioritarias dentro de cualquier estrategia local de ciberseguridad ciudadana. Estas medidas resultan especialmente relevantes en entornos educativos donde los usuarios poseen familiaridad con plataformas digitales, pero no necesariamente cuentan con criterios suficientes de autoprotección.

6.1.5 Quinta conclusión

La investigación permite concluir que los criterios propuestos no demuestran una reducción estadística efectiva de la incidencia de delitos informáticos, debido a que el estudio no tuvo diseño experimental ni longitudinal. Sin embargo, sí permiten establecer una base preventiva razonable para disminuir la vulnerabilidad digital de los usuarios y orientar futuras políticas, programas o campañas locales de ciberseguridad ciudadana en Huacho.

6.2 Recomendaciones

6.2.1 Primera recomendación

Se recomienda que las instituciones educativas de Huacho incorporen programas periódicos de formación en ciberseguridad ciudadana, orientados no solo al uso de herramientas digitales, sino principalmente a la prevención de fraudes, protección de datos personales, verificación de fuentes, reconocimiento de suplantación de identidad y adopción de hábitos seguros en línea.

6.2.2 Segunda recomendación

Se recomienda que la Universidad Nacional José Faustino Sánchez Carrión, a través de sus áreas académicas y administrativas pertinentes, promueva campañas internas de autoprotección digital dirigidas a estudiantes, docentes y personal administrativo, tomando como base criterios de accesibilidad cognitiva, sostenibilidad práctica y proporcionalidad económica.

6.2.3 Tercera recomendación

Se recomienda que las autoridades locales, instituciones educativas, comisarías y entidades públicas desarrollen materiales preventivos sencillos, comprensibles y de bajo costo, orientados a explicar las principales modalidades de delitos informáticos y las medidas básicas que los ciudadanos pueden adoptar para reducir su exposición al riesgo.

6.2.4 Cuarta recomendación

Se recomienda fortalecer la articulación entre prevención ciudadana y marco jurídico penal, de modo que la Ley de Delitos Informáticos no sea entendida únicamente como instrumento sancionador posterior al daño, sino también como punto de partida para impulsar políticas educativas y preventivas frente a la criminalidad digital.

6.2.5 Quinta recomendación

Se recomienda que futuras investigaciones amplíen la población de estudio hacia otros sectores de Huacho, tales como comerciantes, adultos mayores, usuarios de banca digital, estudiantes universitarios de distintas facultades y servidores públicos, con la finalidad de contrastar los criterios propuestos en grupos poblacionales diversos y fortalecer la generalización de los hallazgos.

Capítulo VII : REFERENCIAS

- Justia México.** (2026). Delitos informáticos. <https://mexico.justia.com/derecho-penal/delitos-informaticos/>
- Revista Sinergia Académica.** (2026). Conciencia y cultura de ciberseguridad en estudiantes universitarios en entornos de educación virtual. Sinergia Académica. <https://sinergiaacademica.com/index.php/sa/article/download/897/1825/3503>
- Wikipedia.** (2026). Ciudadanía digital. En Wikipedia, la enciclopedia libre. Recuperado de https://es.wikipedia.org/wiki/Ciudadan%C3%ADa_digital
- Alvear Tobar, E. J., & Casa Murillo, W. G.** (2025). La educación digital y su rol en la prevención ante la ciberdelincuencia juvenil en Ecuador https://repositorio.uisek.edu.ec/handle/123456789/5530?utm_.
- GPS Penal.** (2025, 6 de noviembre). *Delitos informáticos en España: cómo se investigan y qué penas tienen.* <https://gpspenal.com/2025/11/06/delitos-informaticos-en-espana/>
- La República.** (2025, 16 de agosto). *Delitos informáticos aumentaron 129% en los últimos dos años.* <https://larepublica.pe/sociedad/2025/08/16/delitos-informaticos-aumentaron-129-en-los-ultimos-dos-anos-ciberdelitos-hnews-381968>
- La República.** (2025, 18 de mayo). *Ciberataques: Perú supera el millón de delitos informáticos cometidos dentro del sector empresarial, ¿cómo prevenirlo?* <https://larepublica.pe/economia/2025/05/18/ciberataques-peru-supera-el-millon-de-delitos-informaticos-cometidos-dentro-del-sector-empresarial-como-prevenirlo-atmp-565470>
- Ministerio de Educación de Chile.** (2025). *¿Qué es la ciudadanía digital? Ciudadanía Digital Mineduc.* <https://ciudadaniadigital.mineduc.cl/que-es-la-ciudadania-digital/>
- Panda Seguridad.** (2025). *La cultura de la ciberseguridad es fundamental para reducir los riesgos informáticos en las empresas.* <https://www.pandasecurity.com/es/mediacenter/cultura-ciberseguridad-reducir-riesgos-informaticos-empresas/>
- RPP Noticias.** (2025). *Ciberdelincuencia en Perú aumentó un 40% en 2024: más de 42 mil denuncias por delitos informáticos.* <https://rpp.pe/peru/actualidad/fraudes-digitales-y-suplantacion-de-identidad-alarman-cifras-de-la-pnp-revelan-el-impacto-de-la-ciberdelincuencia-en-peru-noticia-1620466>

- Secretaría de Gobierno y Transformación Digital.** (2025). *Estrategia Nacional de Ciberseguridad 2026-2028*. Gobierno del Perú.
- Asociación Iberoamericana de Derecho Comparado.** (2024). *Ciberdelitos y delitos informáticos*. AIDCA. <https://aidca.org/ridca5-penalycriminologia-amato-ciberdelitos-y-delitos-informaticos/>
- Dexia Abogados.** (2024). *Los delitos informáticos en el Código Penal*. <https://www.dexiaabogados.com/blog/delitos-informaticos/>
- eBIZ Noticias.** (2024). *El alto costo de la cibercriminalidad*. <https://ebiz.pe/noticias/el-alto-costo-de-la-cibercriminalidad-un-especial-de-ebiz-noticias/>
- Juris.pe.** (2024). *Modifican diversos delitos informáticos para sancionar la ciberdelincuencia*. DL 1614. <https://juris.pe/blog/modifican-diversos-delitos-informaticos-sancionar-ciberdelincuencia-decreto-legislativo-1614/>
- Marcasur.** (2024). *Recientes mejoras a la Ley de Delitos Informáticos en el Perú*. <https://marcasur.com/noticia/recientes-mejoras-a-la-ley-de-delitos-informaticos-en-el-peru>
- Mazuelos Abogados.** (2024). *Comentarios al Decreto Legislativo N.º 1614: Modificaciones a los delitos informáticos*. <https://mazuelosabogados.com.pe/comentarios-al-decreto-legislativo-n-o-1614-modificaciones-a-los-delitos-informaticos/>
- Revista de Investigación Educativa de la REDIECH.** (2024). *Ciberseguridad en instituciones de educación superior: Un análisis desde la perspectiva de la teoría de la motivación de protección*. IE Revista de Investigación Educativa de la REDIECH. https://revistas.rediech.org/index.php/ie_rie_rediech/article/view/2271
- Rufián Albarrán, M. & Varela Campos, E.** (2024) *Análisis de la Privacidad y Seguridad en las Redes Sociales en un Mundo de Ciberdelitos* <https://repositorio.comillas.edu/jspui/handle/11531/120?offset=40>
- S2Grupo.** (2024). *Cómo fomentar una cultura de ciberseguridad en la empresa*. <https://s2grupo.es/como-fomentar-una-cultura-de-ciberseguridad-en-la-empresa/>
- Seguridadtecnia.** (2024, 15 de marzo). *Ciberseguridad conductual y la línea entre lo lógico y lo físico*. https://www.seguritecnia.es/tecnologias-y-servicios/ciberseguridad/ciberseguridad-conductual-y-la-delgada-linea-entre-lo-logico-y-lo-fisico_20240315.html

- Cajigas Moreano, L. J., & Pérez Chirinos, G. L.** (2023). *La incidencia de las nuevas tecnologías en el delito de fraude informático y su aplicación en la Ley N.º 30096 en el Perú*. Tesis de grado, Universidad Andina del Cusco. https://alicia.concytec.gob.pe/vufind/Record/UACI_57323fcf10dd71024ce700e52e3386ff
- Congreso de la República del Perú.** (2023). *Decreto Legislativo N° 1614, Decreto Legislativo que modifica la Ley N° 30096, Ley de Delitos Informáticos, para prevenir y hacer frente a la ciberdelincuencia*. Diario Oficial El Peruano. <https://busquedas.elperuano.pe/dispositivo/NL/2246611-13>
- Defensoría del Pueblo.** (2023). *Informe Defensorial N° 001-2023-DP/ADHPD: La ciberdelincuencia en el Perú*. <https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf>
- ENISA Agencia de la Unión Europea para la Ciberseguridad** (2023). *Informe sobre el panorama de amenazas*. <https://www.enisa.europa.eu/publications/threat-landscape-2023>
- Santos, M. D.** (2023). *Marco regulatorio de la ciberseguridad y ciberdefensa dentro de la sociedad de la información y el conocimiento. Respuestas del Estado ecuatoriano en el periodo 2013-2022*. Repositorio Institucional UASB. <https://repositorio.uasb.edu.ec/bitstream/10644/9076/1/T3975-MRI-Santos-Marco.pdf>
- Banco Interamericano de Desarrollo.** (2022). *Ciudadanía digital: ¿tenemos derechos y deberes en el espacio online?* <https://www.iadb.org/es/blog/educacion/ciudadania-digital-tenemos-derechos-y-deberes-en-el-espacio-online>
- Computer Weekly.** (2022). *Los 7 elementos de una cultura de ciberseguridad empresarial*. <https://www.computerweekly.com/es/cronica/Los-7-elementos-de-una-cultura-de-ciberseguridad-empresarial>
- Correa Coronel, M. M.** (2022). *Ciberseguridad y su incidencia en el tratamiento de datos personales en una Municipalidad distrital de Lima Sur, 2021*. Tesis de maestría, Universidad César Vallejo. https://alicia.concytec.gob.pe/vufind/Record/UCVV_7b08f45d5d387ee11cc9935bd18720f9

- Organización Internacional de Normalización.** (2022). *Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de gestión de la seguridad de la información - Requisitos* (ISO/IEC 27001:2022). <https://www.iso.org/standard/27001>
- Instituto Nacional de Estadística e Informática.** (2021). *Estadísticas de criminalidad y seguridad ciudadana: Abril-Junio 2021*. https://www.inei.gob.pe/media/MenuRecursivo/boletines/estadisticas_de_criminalidad_seguridad_ciudadana_abr-jun2021.pdf
- Jancachagua Vera, J. W.** (2021). *Mejoramiento de la seguridad de la información para reducir los ciberataques del tipo phishing en una entidad financiera*. Tesis de grado, Universidad Tecnológica del Perú. https://alicia.concytec.gob.pe/vufind/Record/UTPD_f8ca306ab965872f4f67120adb0bf77f
- IUS360.** (2020). *Delitos informáticos: Cuáles son los principales fraudes informáticos que se pueden cometer a través del E-Commerce*. <https://ius360.com/delitos-informaticos-cuales-son-los-principales-fraudes-informaticos-que-se-pueden-cometer-a-traves-del-e-commerce-oscar-zevallos-prado/>
- Organización de los Estados Americanos.** (2020). *El Convenio de Budapest sobre el Cibercrimen y su impacto en las Américas*. <https://www.oas.org/es/>
- PWC España.** (2020). *Cómo crear una cultura de ciberseguridad sólida en tu empresa*. <https://www.pwc.es/es/publicaciones/transformacion-digital/estado-cultura-ciberseguridad.html>
- Saldaña, J.** (2020). *Derechos digitales y la autodeterminación informativa en el siglo XXI*. *Revista Ius Et Praxis*, 26(1), 115-136.
- Unión Internacional de Telecomunicaciones UIT.** (2020). *Guía de la UIT para el desarrollo de una Estrategia Nacional de Ciberseguridad*. Oficina de Desarrollo de las Telecomunicaciones de la UIT. https://www.itu.int/pub/D-STR-CYB_GUIDE.01-2020
- Schneier, B.** (2019). *Haga clic aquí para matarlos a todos: Seguridad y supervivencia en un mundo hiperconectado*.
- W. W. Norton & Company. Cain, A. A., Edwards, M. E. y Still, J. D.** (2018). *An exploratory study of cyber hygiene behaviors and knowledge*. *Journal of Information Security and Applications*, 42, 36-45. <https://doi.org/10.1016/j.jisa.2018.08.002>

- Caro John, J. A.** (2018). *Cibercrimen y derecho penal: Análisis de la Ley de Delitos Informáticos* (2.^a ed.). Jurista Editores.
- Instituto Nacional de Estándares y Tecnología.** (2018). *Framework for Improving Critical Infrastructure Cybersecurity (Versión 1.1)*.
- Departamento de Comercio de Estados Unidos. Provan, D., & Lemon, O.** (2018). *Factores humanos en ciberseguridad: Una revisión de la literatura. International Journal of Human-Computer Studies*, 118, 45-54.
<https://doi.org/10.1016/j.ijhcs.2018.06.004>
- Scielo Chile.** (2018). *Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos*. https://www.scielo.cl/scielo.php?pid=S0718-00122018000100159&script=sci_arttext
- Stallings, W.** (2018). *Fundamentos de seguridad de redes: Aplicaciones y estándares* (6.^a ed.). Pearson.
- Whitman, M. E. y Mattord, H. J.** (2018). *Principios de la seguridad de la información* (6.^a ed.).
- Cengage Learning. Téllez Valdés, J.** (2017). *Derecho informático* (5.^a ed.). McGraw-Hill Interamericana.
- Whitman, ME, & Mattord, HJ** (2017). *Principios de seguridad de la información* (5.^a ed.). Cengage Learning.
- Kott, A., & Arnold, C.** (2016). *Ciberdefensa y conocimiento de la situación*. Springer International Publishing. <https://doi.org/10.1007/978-3-319-41310-6>
- Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D. y Polak, P.** (2015). *What do systems users have to fear? Using Fear Appeals to engender threats and fear that motivate protective security behaviors. MIS Quarterly*, 39(4), 837-864.
<https://doi.org/10.25300/MISQ/2015/39.4.5>
- Hadžiosmanović, D., et al.** (2015). *Medición del factor humano en la ciberseguridad. Talleres de Seguridad y Privacidad IEEE 2015*, 130-137.
<https://doi.org/10.1109/SPW.2015.31>
- Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P.** (2014). *Metodología de la investigación* (6.^a ed.). McGraw-Hill Education.
- Sommestad, T., Karlzén, H., y Hallberg, J.** (2014). *The effectiveness of security awareness training. Information Management & Computer Security*, 22(2), 24-38.

- Torres Pozo, A. R.** (2014). *La problemática de la función investigatoria del delito de fraude informático en el Perú. Tesis de grado*, Universidad César Vallejo. https://alicia.concytec.gob.pe/vufind/Record/UCVV_5bee2bdf89de86818429b31d29da29ce/Details
- Congreso de la República del Perú.** (2013). *Ley N° 30096, Ley de Delitos Informáticos*. Diario Oficial El Peruano. <https://busquedas.elperuano.pe/normaslegales/ley-de-delitos-informaticos-ley-n-30096-1003117-1/>
- Reyns, B. W.** (2013). *Online routines and identity theft victimization: Further expanding routine activity theory with respect to cybercrime*. *Deviant Behavior*, 34(2), 142-153. <https://doi.org/10.1080/01639625.2012.707550>
- Von Solms, R., & Van Niekerk, J.** (2013). *De la seguridad de la información a la ciberseguridad*. *Computers & Security*, 38, 83-84. <https://doi.org/10.1016/j.cose.2013.04.004>
- Furnell, S., y Clarke, N.** (2012). *Power to the people? The evolving recognition of human aspects of security*. *Computers & Security*, 31(8), 983-988. <https://doi.org/10.1016/j.cose.2012.08.004>
- Pfleeger, CP y Caputo, DD** (2012). *El factor humano en la ciberseguridad*. *IT Professional*, 14 (1), 43-46. <https://doi.org/10.1109/MITP.2012.11>
- Pfleeger, CP y Pfleeger, SL** (2012). *Seguridad en la informática (5ª ed.)*. Prentice Hall.
- Vara Horna, A. A.** (2012). *Desde la idea hasta la sustentación: Siete pasos para una tesis exitosa*.
- Universidad de San Martín de Porres. Bernal, C. A.** (2010). *Metodología de la investigación: Administración, economía, humanidades y ciencias sociales (3.ª ed.)*.
- Pearson Educación. Téllez Valdés, J.** (2009). *Derecho informático (4.ª ed.)*. McGraw-Hill.
- Meliá, JL** (2007). *Seguridad basada en el comportamiento*. Universitat de València. https://www.uv.es/~meliajl/Papers/2007JLM_SBC.pdf
- Kruger, H. A. y Kearney, W. D.** (2006). *A prototype for assessing information security awareness*. *Computers & Security*, 25(4), 289-296. <https://doi.org/10.1016/j.cose.2006.02.008>
- Yar, M.** (2005). *The novelty of cybercrime: An assessment in light of routine activity theory*. *European Journal of Criminology*, 2(4), 407-427. <https://doi.org/10.1177/147737080556656>
- Mitnick, K. D. y Simon, W. L.** (2002). *El arte de la decepción: Los secretos de la ingeniería social detrás del hackeo*. Wiley Publishing.

- Zaffaroni, E. R.** (2000). *Derecho penal: Parte general*. Ediar.
- Ajzen, I.** (1991). *The theory of planned behavior*. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- Davis, F. D.** (1989). *Perceived usefulness, perceived ease of use, and user acceptance of information technology*. *MIS Quarterly*, 13(3), 319-340. <https://doi.org/10.2307/249008>
- Sweller, J.** (1988). *Cognitive load during problem solving: Effects on learning*. *Cognitive Science*, 12(2), 257-285. https://doi.org/10.1207/s15516709cog1202_4
- Petty, R. E., & Cacioppo, J. T.** (1986). *The elaboration likelihood model of persuasion*. *Advances in Experimental Social Psychology*, 19, 123-205. [https://doi.org/10.1016/S0065-2601\(08\)60214-2](https://doi.org/10.1016/S0065-2601(08)60214-2)
- Rogers, R. W.** (1983). *Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation*. En J. Cacioppo & R. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153-176). Guilford Press.
- Weinstein, N. D.** (1980). *Unrealistic optimism about future life events*. *Journal of Personality and Social Psychology*, 39(5), 806-820. <https://doi.org/10.1037/0022-3514.39.5.806>
- Cohen, L. E., & Felson, M.** (1979). *Social change and crime rate trends: A routine activity approach*. *American Sociological Review*, 44(4), 588-608. <https://doi.org/10.2307/2094589>
- Kahneman, D., & Tversky, A.** (1979). *Prospect theory: An analysis of decision under risk*. *Econometrica*, 47(2), 263-291. <https://doi.org/10.2307/1914185>
- Rogers, R. W.** (1975). *A protection motivation theory of fear appeals and attitude change*. *The Journal of Psychology*, 91(1), 93-114. <https://doi.org/10.1080/00223980.1975.9915803>
- 3 dígitos.** (sf). *El análisis conductual (Behavioral Analysis) como protección en ciberseguridad*. <https://www.3digits.es/blog/análisis-conductual-analisis-conductual.html>
- Gálvez Monteagudo Abogados.** (s.f.). *Delitos informáticos en Perú: evolución legal y desafíos*. <https://galvezmonteagudo.pe/delitos-informaticos-peru-normativa-retos/>
- Gobierno de Canarias.** (sf). *Concepto y alcance de ciudadanía digital*. Gobierno de Canarias. https://www3.gobiernodecanarias.org/medusa/contenidosdigitales/FormacionTIC/cdtic2014/04cd/11_concepto_y_alcance_de_ciudadana_digital.html

Instituto Nacional de Ciberseguridad de España. (s.f.). *Guía de ciberseguridad para el ciudadano.* <https://www.incibe.es/ciudadania>

Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado. (sf). *Cultura de ciberseguridad. Ministerio de Educación y Formación Profesional de España.*
https://descargas.intef.es/cedec/proyectoedia/FP/digitalizacion/contenidos/operacion_ciberseguridad/cultura_de_ciberseguridad.html

Ministerio del Interior de España. (sf). *Autoprotección: Guía de información al ciudadano. Dirección General de Protección Civil y Emergencias.*
https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/proteccion-civil/Guia_de_informacion_autoproteccion_126230971.pdf

Monografías Plus. (sf). *Autoprotección ciudadana.*
<https://www.monografias.com/docs/Autoproteccion-ciudadana-F3FJGC3R99JP>

Observatorio de Economía de la Conducta. (s.f.). *Ciberseguridad conductual.*
<https://observatorioeconomiaconducta.org/ciberseguridad-conductual/>

Real Academia Española. (s.f.). *Cultura. En Diccionario de la lengua española.*
Recuperado de <https://dle.rae.es/cultura>

Universidad de La Laguna. (s.f.). *Los delitos informáticos en el código penal español.*
Repositorio Institucional ULL.
<https://riull.ull.es/xmlui/bitstream/handle/915/27983/Los%20delitos%20informaticos%20en%20el%20codigo%20penal%20espanol..pdf>



**UNIVERSIDAD NACIONAL
“JOSÉ FAUSTINO SÁNCHEZ CARRIÓN”
ESCUELA DE DERECHO Y CIENCIAS POLÍTICAS**



BORRADOR DE TESIS

**Determinación de criterios sobre aplicabilidad de ciberseguridad basada en la
cultura de autoprotección ciudadana para lograr mitigar delitos informáticos,
Huacho, 2025**

Espero su colaboración respondiendo con responsabilidad y honestidad el presentante cuestionario. Se agradece no dejar ninguna pregunta sin contestar además será de manera confidencial y estrictamente para fines de investigación:

Objetivo: es recopilar información, para tener conocimiento sobre la “Determinación de criterios sobre aplicabilidad de ciberseguridad basada en la cultura de autoprotección ciudadana para lograr mitigar delitos informáticos, Huacho, 2025”

Marque con un aspa (X) cualquiera de las alternativas a, b, c, d o e

Instrucciones: A continuación, se formula preguntas de diferentes tipos, le cuidadosamente cada una, identifique la respuesta que considere correcta y escriba un aspa (x) sobre ella.

Para cada Items se considera la escala de 1 a 5 donde:

1. Nunca	2. Casi nunca	3. Ocasionalmente	4. Casi siempre	5. Siempre
----------	---------------	-------------------	-----------------	------------

EDAD	a) 18 - 28 b) 28 - 38 c) 38 - 48 d) 48 - 58 e) 58 – más
SEXO	a) Masculino b) Femenino

Mitigación de delitos informáticos	1	2	3	4	5
1. Dimensión: Exposición a riesgos informáticos					
1. ¿Ha experimentado accesos no autorizados a sus dispositivos o sistemas informáticos?					
2. ¿Ha tenido problemas con la seguridad de su sistema informático en el último año?					
3. ¿Ha sufrido pérdida o alteración de información debido a ataques informáticos?					
4. ¿Realiza revisiones regulares para garantizar la seguridad de sus sistemas informáticos?					
5. ¿Con qué frecuencia actualiza el software de seguridad en sus dispositivos?					
6. ¿Con qué frecuencia utiliza contraseñas seguras y únicas para sus cuentas en línea?					
7. ¿Con qué frecuencia realiza copias de seguridad de sus datos importantes?					
8. ¿Con qué frecuencia se informa sobre las amenazas cibernéticas actuales?					
2. Dimensión: Riesgo de fraude y suplantación digital					
1. ¿Ha sido víctima de fraude informático relacionado con sus datos personales?					
2. ¿Sus datos han sido robados o utilizados sin su consentimiento?					
3. ¿Ha notado intentos de suplantación de identidad digital utilizando sus datos personales?					
4. ¿Toma medidas activas para proteger sus datos informáticos de posibles amenazas?					
5. ¿Con qué frecuencia revisa la configuración de privacidad de sus cuentas en redes sociales?					
6. ¿Con qué frecuencia se siente preocupado por el uso indebido de sus datos personales en línea?					
7. ¿Con qué frecuencia comparte información personal sensible en línea (como su dirección o número de teléfono)?					
8. ¿Con qué frecuencia verifica la autenticidad de las fuentes de información antes de compartir datos en línea?					

Criterios de aplicabilidad de ciberseguridad basada en la cultura de autoprotección ciudadana	1	2	3	4	5
1. Dimensión: Prácticas de autoprotección digital					
1. ¿Considera que las autoridades locales implementan medidas eficaces para proteger sus derechos digitales?					
2. ¿Siente que las leyes actuales sobre derechos digitales le protegen adecuadamente?					
3. ¿Ha participado en alguna iniciativa gubernamental para la protección de sus derechos digitales?					
4. ¿Confía en las herramientas tecnológicas que usa para prevenir la vulneración de sus derechos digitales?					
5. ¿Con qué frecuencia se informa sobre las leyes que protegen sus derechos digitales?					
6. ¿Con qué frecuencia considera que las leyes actuales son efectivas para proteger sus derechos en línea?					
7. ¿Con qué frecuencia ha sentido que sus derechos digitales han sido vulnerados?					
8. ¿Con qué frecuencia cree que las autoridades deberían hacer más para educar a la población sobre sus derechos digitales?					
2. Dimensión: Cultura educativa y participación preventiva					
1. ¿Conoce las medidas de seguridad necesarias para protegerse de ataques cibernéticos?					
2. ¿Sabe cómo identificar posibles vulneraciones a sus derechos digitales?					
3. ¿Recibe información educativa sobre ciberseguridad y derechos digitales por parte de las autoridades?					
4. ¿Ha recibido algún tipo de formación sobre ciberseguridad y protección de derechos digitales?					
5. ¿Con qué frecuencia ha participado en talleres o cursos sobre seguridad en línea?					
6. ¿Con qué frecuencia considera que la educación sobre seguridad en línea es importante para prevenir delitos informáticos?					
7. ¿Con qué frecuencia utiliza recursos en línea para aprender sobre seguridad digital?					
8. ¿Con qué frecuencia cree que las escuelas deberían incluir la educación sobre derechos digitales en su currículo?					

Criterios de aplicabilidad de ciberseguridad basada en la cultura de autoprotección ciudadana	1	2	3	4	5
3. Dimensión: Conocimiento preventivo en ciberseguridad					
1. ¿Le preocupa que personas no autorizadas puedan acceder a su información personal en línea?					
2. ¿Utiliza mecanismos para garantizar que solo personas autorizadas accedan a su información confidencial?					
3. ¿Ha experimentado la divulgación de su información confidencial sin su consentimiento?					
4. ¿Confía en que las plataformas digitales que utiliza mantendrán la confidencialidad de su información?					
5. ¿Con qué frecuencia se siente seguro al compartir información personal en línea?					
6. ¿Con qué frecuencia toma medidas para proteger la confidencialidad de su información en redes sociales?					
7. ¿Con qué frecuencia revisa las políticas de privacidad de las aplicaciones que utiliza?					
8. ¿Con qué frecuencia ha experimentado la divulgación no autorizada de su información personal?					
4. Dimensión: Verificación y gestión responsable de la información					
1. ¿Le preocupa que su información digital sea modificada sin su consentimiento?					
2. ¿Toma medidas para asegurar que su información personal en línea no sea manipulada?					
3. ¿Ha detectado cambios no autorizados en sus datos personales o profesionales?					
4. ¿Confía en la integridad de la información que maneja en las plataformas digitales?					
5. ¿Con qué frecuencia verifica la exactitud de la información que recibe en línea?					
6. ¿Con qué frecuencia ha notado información incorrecta o manipulada en sus cuentas o dispositivos?					
7. ¿Con qué frecuencia toma medidas para asegurarse de que la información que comparte en línea sea veraz?					
8. ¿Con qué frecuencia cree que es fácil para los usuarios detectar la manipulación de datos en línea?					

ANEXO (MATRIZ DE CONSISTENCIA)

PROBLEMA	OBJETIVO	HIPOTESIS	VARIABLES	INDICADORES	METODOLOGÍA
Problema General ¿Cuáles son los criterios operativos para diseñar e implementar un modelo de ciberseguridad basado en la cultura de autoprotección ciudadana que permita reducir la incidencia de delitos informáticos en Huacho en el año 2025?	Objetivo General Determinar los criterios operativos para el diseño e implementación de un modelo de ciberseguridad fundamentado en la cultura de autoprotección ciudadana, con el fin de reducir la incidencia de delitos informáticos en Huacho durante el año 2025.	Hipótesis General Si se determinan como criterios operativos de aplicabilidad de la ciberseguridad basada en la cultura de autoprotección ciudadana la accesibilidad cognitiva de la información preventiva, la sostenibilidad práctica de los hábitos digitales seguros, la proporcionalidad económica de las medidas de protección, la educación digital continua y la adopción de prácticas básicas de verificación, confidencialidad e integridad de la información, entonces se favorecerá la mitigación de los delitos informáticos en Huacho durante el año 2025, mediante la reducción de la vulnerabilidad ciudadana frente a riesgos como el fraude informático, la suplantación de identidad, el acceso no autorizado y la manipulación de datos personales.	Variable independiente Criterios de aplicabilidad de ciberseguridad basada en la cultura de autoprotección ciudadana. <i>Dimensiones</i> ➤ Conocimiento preventivo en ciberseguridad. ➤ Prácticas de autoprotección digital. ➤ Verificación y gestión responsable de la información. ➤ Cultura educativa y participación preventiva. ➤ Criterios operativos de aplicabilidad.	Identificación de amenazas cibernéticas actuales. Uso de contraseñas seguras y diferenciadas. Verificación de autenticidad de fuentes digitales. Acceso a formación en ciberseguridad y derechos digitales. Accesibilidad cognitiva de las medidas preventivas.	Población: 435 estudiantes del Instituto de Idiomas de la UNJFSC. Muestra: 135 estudiantes Tipo de Investigación: Aplicada Nivel: Descriptivo-propositivo con alcance explicativo limitado Enfoque: Cuantitativo con apoyo jurídico-documental Estilo: Analítica Diseño: No experimental, transversal Técnica: Encuesta Instrumento: Cuestionario aplicado a estudiantes del Instituto de Idiomas de la Universidad Nacional José Faustino Sánchez Carrión.
Problemas Específicos No se formulan problemas específicos, debido a que la investigación se estructura a partir de un problema general único. Los objetivos específicos cumplen función metodológica instrumental y no constituyen subproblemas autónomos.	Objetivos Específicos • Diagnosticar el nivel de conocimientos y prácticas de autoprotección digital existentes en la comunidad. • Describir las modalidades de delitos informáticos y riesgos digitales más relevantes para el contexto de estudio. • Establecer criterios de aplicabilidad de la ciberseguridad para la prevención de dichos riesgos. • Proponer medidas de fortalecimiento de la cultura de autoprotección ciudadana	Hipótesis Específicas No se formulan hipótesis específicas, debido a que no se han planteado problemas específicos autónomos. La contrastación se realizará respecto de la hipótesis general.	Variable dependiente Mitigación de delitos informáticos. <i>Dimensiones</i> ➤ Exposición a riesgos informáticos. ➤ Riesgo de fraude y suplantación digital. ➤ Protección de derechos digitales y datos personales. ➤ Confidencialidad e integridad de la información.	Experiencia de accesos no autorizados a dispositivos o cuentas. Experiencia de fraude informático vinculado con datos personales. Percepción de vulneración de derechos digitales. Implementación de medidas para proteger información confidencial.	