NCML NeutrosophicComputing and Machine Learning, Vol. 44, 2026

University of New Mexicc

Conciencia de ciberseguridad y uso de contraseñas robustas en usuarios universitarios: un análisis correlacional con enfoque neutrosófico

Cybersecurity awareness and use of strong passwords among university users: a correlational analysis with a neutrosophic approach

Oscar Alberto Macías Yanqui[1], Kleber Overdan Cedeño Pinto[2], Oscar Abel Macías Fernandez[3], Richard Manolo Calero Villareal[4], Alfonso Aníbal Guijarro Rodríguez[5,6]

[1] Universidad de Guayaquil, Guayas, Ecuador, oscar.maciasy@ug.edu.ec,

[2] Universidad de Guayaquil, Guayas, Ecuador, Kleber.cedenop@ug.edu.ec,

[3] Universidad de Guayaquil, Guayas, Ecuador, omacias@uagraria.edu.ec,

[4] Universidad de Guayaquil, Guayas, Ecuador, Richard.calerovi@ug.edu.ec,

[5] Universidad de Guayaquil, Guayas, Ecuador, alfonso.guijarror@ug.edu.ec,

[6]Grupo de Investigación de Inteligencia Artificial, Universidad de Guayaquil, Guayas. Ecuador.

RESUMEN

La creciente digitalización de las instituciones de educación superior ha incrementado la dependencia de sistemas de autenticación digital, donde las contraseñas continúan siendo uno de los mecanismos más utilizados y, al mismo tiempo, una de las principales vulnerabilidades asociadas al factor humano. La presente investigación tuvo como objetivo analizar la relación entre la conciencia de ciberseguridad y el uso de contraseñas robustas en usuarios universitarios mediante un enfoque correlacional complementado con análisis neutrosófico. El estudio se desarrolló bajo un enfoque cuantitativo, con diseño no experimental y alcance correlacional-explicativo. La muestra estuvo conformada por 384 participantes pertenecientes a universidades públicas ecuatorianas. Para la recolección de datos se aplicó un cuestionario estructurado validado mediante juicio de expertos y confiabilidad Alfa de Cronbach. Los resultados evidenciaron una correlación positiva y estadísticamente significativa entre la conciencia de ciberseguridad y el uso de contraseñas robustas (ρ=0.742;p<0.05). Asimismo, el análisis neutrosófico permitió identificar niveles de indeterminación conductual asociados a contradicciones entre conocimiento y comportamiento real frente a la seguridad digital. Se concluye que el enfoque neutrosófico complementa adecuadamente los modelos estadísticos tradicionales y constituye una alternativa relevante para el análisis del factor humano en ciberseguridad.

Palabras clave: ciberseguridad; contraseñas robustas; neutrosofía; conciencia digital; autenticación; gestión de credenciales; lógica neutrosófica.

ABSTRACT

The increasing digitization of higher education institutions has heightened the reliance on digital authentication systems, where passwords remain one of the most widely used mechanisms and, simultaneously, one of the

main vulnerabilities associated with the human factor. This research aimed to analyze the relationship between cybersecurity awareness and the use of strong passwords among university users through a correlational approach complemented by neutrosophic analysis. The study was conducted using a quantitative approach, with a non-experimental design and a correlational-explanatory scope. The sample consisted of 384 participants from Ecuadorian public universities. Data was collected using a structured questionnaire validated by expert judgment and Cronbach's alpha reliability. The results showed a positive and statistically significant correlation between cybersecurity awareness and the use of strong passwords (ρ=0.742; $p<0.05$). Furthermore, the neutrosophic analysis identified levels of behavioral indeterminacy associated with contradictions between knowledge and actual behavior regarding digital security. It is concluded that the neutrosophic approach adequately complements traditional statistical models and constitutes a relevant alternative for the analysis of the human factor in cybersecurity.

Keywords: Cybersecurity; Strong Passwords; Neutrosophic; Digital Awareness; Authentication; Credential Management; Neutrosophic Logic.

1. INTRODUCCIÓN

La transformación digital se ha incrementado significativamente en las organizaciones y en las instituciones de educación superior por la demanda de plataformas digitales para el acceso a servicios académicos, administrativos y corporativos. Sin embargo, las contraseñas continúan siendo el mecanismo de autenticación más utilizado para el acceso a sistemas de información, correos electrónicos institucionales, entornos virtuales de aprendizaje y servicios en línea. A pesar del avance de las tecnologías complementarias como la autenticación multifactor y los sistemas biométricos, las credenciales basadas en contraseñas siguen representando un componente crítico dentro de los modelos actuales de seguridad digital [1].

En la actualidad el proceso de digitalización han sido abordado por un número significativo de empresas, lo cual ha incrementado la exposición a amenazas cibernéticas asociadas a la gestión inadecuada de credenciales. Diversos estudios señalan que prácticas como la reutilización de contraseñas, el uso de claves débiles, la ausencia de autenticación multifactor y el almacenamiento inseguro de información continúan siendo factores recurrentes en incidentes de seguridad informática [11]. En consecuencia, el factor humano se ha consolidado como uno de los principales elementos de vulnerabilidad dentro de los ecosistemas de ciberseguridad contemporáneos.

En los últimos años, la investigación científica ha mostrado un creciente interés por comprender el comportamiento de los usuarios frente a las políticas y prácticas de seguridad digital. Frente a este enfoque, conocido como behavioral cybersecurity, sostiene que la efectividad de las estrategias de protección informática no depende únicamente de la infraestructura tecnológica, sino también de factores cognitivos, conductuales y contextuales asociados a la percepción del riesgo, la motivación y los hábitos digitales de los usuarios [3]. Desde esta perspectiva, la conciencia de ciberseguridad constituye un componente fundamental para promover conductas seguras relacionadas con la autenticación digital y la protección de la información.

La conciencia de ciberseguridad comprende el conjunto de conocimientos, percepciones y comportamientos que permiten a los usuarios reconocer amenazas digitales y adoptar medidas preventivas orientadas a reducir riesgos en entornos tecnológicos. Recientes investigaciones desarrolladas en instituciones de educación superior han evidenciado niveles heterogéneos de awareness en ciberseguridad, así como debilidades persistentes en la gestión de contraseñas y autenticación digital, incluso entre usuarios con formación tecnológica [1]. Esta situación presenta una especial relevancia en los entornos universitarios debido al elevado número de usuarios que interactúan diariamente con plataformas institucionales y servicios digitales sensibles.

De manera complementaria, se revelan estudios recientes sobre comportamiento de autenticación digital lo cual ha demostrado que los usuarios suelen priorizar la facilidad de uso y la memorabilidad por encima de la robustez de las credenciales. Wash y Rader [11] identificaron que la creación de contraseñas responde frecuentemente a estrategias

orientadas a reducir la carga cognitiva más que a maximizar la seguridad. Asimismo, Merdenyan y Petrie [7] evidenciaron que la percepción subjetiva del esfuerzo requerido para gestionar contraseñas robustas influye significativamente en la reutilización de credenciales y en la limitada adopción de prácticas seguras. Estos hallazgos reflejan la persistencia de una brecha entre el conocimiento teórico de las buenas prácticas de seguridad y el comportamiento real de los usuarios frente a la protección de credenciales digitales.

Aunque la literatura reciente muestra niveles avanzados en la comprensión de los factores humanos asociados a la ciberseguridad, gran parte de las investigaciones continúa utilizando enfoques estadísticos tradicionales basados en escalas ordinales y modelos lineales convencionales. Si bien estos métodos permiten identificar asociaciones generales entre variables, presentan limitaciones para representar fenómenos caracterizados por incertidumbre, ambigüedad y contradicción conductual. En numerosos escenarios, los usuarios manifiestan simultáneamente conocimiento sobre buenas prácticas de seguridad y comportamientos inseguros relacionados con la gestión de contraseñas, evidenciando niveles de inconsistencia difíciles de modelar mediante enfoques binarios o estrictamente probabilísticos [9].

Frente a estas limitaciones metodológicas, la neutrosofía surge como una alternativa capaz de representar escenarios de verdad, falsedad e indeterminación de manera simultánea. La lógica neutrosófica, propuesta por Florentin Smarandache, permite modelar fenómenos complejos caracterizados por información parcial, contradictoria o incierta, superando las restricciones de los enfoques clásicos de análisis [2]. Su aplicación reciente en procesos de toma de decisiones, inteligencia computacional y análisis de incertidumbre se ha evidenciado, por lo que es factible abordar problemáticas asociadas al comportamiento humano en contextos digitales y organizacionales.

No obstante, existe escasa evidencia empírica sobre la aplicación de modelos neutrosóficos en el análisis de comportamientos relacionados con la gestión de contraseñas y autenticación digital en entornos universitarios. La mayoría de investigaciones sobre conciencia de ciberseguridad se limita a mediciones descriptivas y correlacionales convencionales, sin incorporar modelos capaces de representar explícitamente los niveles de ambigüedad presentes en las decisiones y prácticas de los usuarios. Esta situación constituye una brecha metodológica relevante dentro del campo de la ciberseguridad centrada en el usuario.

En atención al problema abordado, el objetivo de esta investigación fue analizar la relación entre la conciencia de ciberseguridad y el uso de contraseñas robustas en usuarios universitarios mediante un enfoque correlacional complementado con análisis neutrosófico. El estudio busca aportar evidencia empírica sobre los niveles de conciencia digital y las prácticas de autenticación de los usuarios, así como explorar el potencial de la lógica neutrosófica para modelar los grados de verdad, indeterminación y falsedad presentes en el comportamiento humano frente a la seguridad informática.

2. MARCO TEÓRICO

2.1 Conciencia de ciberseguridad

La conciencia de ciberseguridad (cybersecurity awareness) constituye uno de los componentes fundamentales para la protección de la información en entornos digitales contemporáneos. Este concepto hace referencia al conjunto de conocimientos, percepciones, habilidades y comportamientos que permiten a los usuarios identificar amenazas cibernéticas y adoptar prácticas orientadas a reducir riesgos asociados al uso de tecnologías de información y comunicación. La literatura reciente sostiene que el nivel de awareness influye directamente en la capacidad de los individuos para reconocer ataques de ingeniería social, gestionar adecuadamente sus credenciales y cumplir políticas institucionales de seguridad informática [1].

Diversas investigaciones desarrolladas en contextos educativos y organizacionales han evidenciado que la conciencia de ciberseguridad no depende únicamente del conocimiento técnico, sino también de factores conductuales y psicológicos relacionados con la percepción del riesgo y los hábitos digitales. Goliath et al. [3] señalan que los usuarios pueden poseer conocimientos adecuados sobre seguridad informática y, aun así, mantener prácticas inseguras debido a comportamientos rutinarios, exceso de confianza o baja percepción de vulnerabilidad.

En el ámbito universitario, la conciencia de ciberseguridad adquiere especial relevancia debido al incremento del uso de plataformas académicas, servicios en la nube y sistemas de gestión institucional. Estudios recientes realizados en universidades evidencian que estudiantes y docentes presentan niveles heterogéneos de conciencia, observándose debilidades persistentes relacionadas con la gestión de contraseñas, autenticación y protección de información sensible [1]. Esta situación incrementa la exposición institucional frente a amenazas como phishing, robo de credenciales y accesos no autorizados.

La investigación contemporánea también ha destacado que las estrategias tradicionales de capacitación no siempre producen cambios sostenibles en el comportamiento de los usuarios. En consecuencia, las organizaciones han comenzado a adoptar enfoques centrados en el comportamiento humano y en la construcción de culturas organizacionales de seguridad digital [3].

2.2. Behavioral Cybersecurity y factor humano

El concepto de Behavioral Cybersecurity surge como una línea de investigación orientada a comprender cómo los factores cognitivos, emocionales y conductuales influyen en la adopción de prácticas seguras en entornos digitales. Este enfoque reconoce que la seguridad informática no depende exclusivamente de controles tecnológicos, sino también de la forma en que los usuarios interpretan riesgos, toman decisiones y ejecutan comportamientos frente a amenazas cibernéticas [10].

La literatura reciente identifica al factor humano como uno de los principales elementos de vulnerabilidad dentro de los ecosistemas digitales. Diversos estudios señalan que una proporción significativa de incidentes de seguridad se encuentra asociada a errores humanos, malas prácticas de autenticación, uso inadecuado de credenciales y baja adherencia a políticas de seguridad organizacional [11].Desde esta perspectiva, la ciberseguridad conductual se analizan los fenómenos como:

- percepción del riesgo digital;
- confianza excesiva;
- fatiga de seguridad;
- resistencia al cambio;
- toma de decisiones bajo incertidumbre;
- comportamiento contradictorio frente a normas de seguridad.

Suleiman y Svetinovic [10] sostienen que muchos usuarios desarrollan conductas orientadas a priorizar la usabilidad y conveniencia sobre la seguridad, especialmente cuando perciben que las medidas de protección afectan la experiencia de uso o incrementan la carga cognitiva.

Asimismo, investigaciones recientes han evidenciado la existencia de una brecha entre conocimiento y comportamiento, donde los usuarios conocen las buenas prácticas de seguridad, pero no las aplican consistentemente en su comportamiento cotidiano. Esta contradicción representa uno de los principales desafíos para las estrategias contemporáneas de ciberseguridad centradas en el usuario [3].

2.3. Uso de contraseñas robustas y autenticación digital

Las contraseñas continúan siendo el mecanismo de autenticación más utilizado para el acceso a sistemas digitales, a pesar del crecimiento de tecnologías complementarias como la autenticación multifactor, biometría y sistemas de identidad federada. La robustez de una contraseña se relaciona con características como longitud, complejidad, unicidad y frecuencia de actualización, elementos que contribuyen a reducir la probabilidad de ataques basados en fuerza bruta, diccionarios o reutilización de credenciales [8].

Las investigaciones recientes muestran que los usuarios suelen seleccionar contraseñas fáciles de recordar, sacrificando niveles adecuados de seguridad. Wash y Rader [11] identificaron que muchos individuos construyen contraseñas utilizando patrones cognitivos repetitivos y estrategias orientadas a minimizar el esfuerzo mental. Del mismo modo,

Merdenyan y Petrie [7] evidenciaron que la percepción de complejidad influye significativamente en la reutilización de credenciales y en la resistencia a adoptar prácticas más seguras.

Otra problemática relevante corresponde a la reutilización de contraseñas entre múltiples servicios digitales. Esta práctica incrementa considerablemente el riesgo de compromiso masivo de cuentas, especialmente ante filtraciones de bases de datos o ataques de credential stuffing. Estudios recientes desarrollados en contextos universitarios muestran que una proporción significativa de estudiantes reutiliza contraseñas entre plataformas académicas y servicios personales, incrementando la exposición institucional frente a incidentes de seguridad [9].

En respuesta a estas problemáticas, organismos internacionales como National Institute of Standards and Technology han actualizado sus lineamientos sobre autenticación digital, promoviendo el uso de contraseñas largas, gestores de contraseñas y autenticación multifactor como mecanismos fundamentales para fortalecer la seguridad de las credenciales digitales [8].

2.4. Protection Motivation Theory (PMT)

La Protection Motivation Theory (PMT) constituye uno de los modelos teóricos más utilizados para explicar comportamientos relacionados con la adopción de medidas de protección frente a amenazas. Originalmente desarrollada por Rogers, esta teoría sostiene que los individuos adoptan conductas preventivas en función de dos procesos cognitivos principales: la evaluación de la amenaza y la evaluación de afrontamiento [10].

La evaluación de la amenaza considera variables como: percepción de severidad, percepción de vulnerabilidad, temor frente a riesgos potenciales.

Por su parte, la evaluación de afrontamiento incluye: autoeficacia, eficacia de la respuesta, costos percibidos de implementar conductas seguras.

En el ámbito de la ciberseguridad, la PMT ha sido ampliamente utilizada para explicar la adopción de prácticas relacionadas con: gestión de contraseñas, autenticación multifactor, protección de dispositivos, prevención de phishing.

Estudios recientes evidencian que los usuarios con mayores niveles de percepción de riesgo y autoeficacia presentan una mayor probabilidad de adoptar comportamientos seguros frente a amenazas digitales [10]. En consecuencia, la PMT proporciona una base conceptual relevante para comprender cómo la conciencia de ciberseguridad influye en la adopción de contraseñas robustas y otras prácticas de autenticación segura.

2.5. Theory of Planned Behavior (TPB)

La Theory of Planned Behavior (TPB), propuesta por Ajzen, explica que el comportamiento humano se encuentra determinado principalmente por la intención conductual, la cual depende de tres factores: actitud hacia el comportamiento, normas subjetivas y control conductual percibido. En el campo de la ciberseguridad, este modelo ha sido utilizado para analizar la disposición de los usuarios a cumplir políticas de seguridad y adoptar prácticas digitales seguras [6].

La actitud hacia el comportamiento hace referencia a la valoración positiva o negativa que realiza el individuo respecto a una práctica específica, como el uso de contraseñas robustas o autenticación multifactor. Las normas subjetivas se relacionan con la presión social percibida por parte de compañeros, instituciones u organizaciones. Finalmente, el control conductual percibido corresponde a la percepción de capacidad para ejecutar correctamente una conducta segura.

Investigaciones recientes sugieren que la intención de utilizar prácticas seguras de autenticación se encuentra influenciada por la percepción de utilidad, facilidad de uso y presión institucional para cumplir políticas de seguridad [6]. En consecuencia, la TPB proporciona un marco teórico complementario para comprender las decisiones conductuales asociadas a la gestión de credenciales digitales.

2.6. Neutrosofía aplicada al análisis conductual

La neutrosofía es una teoría filosófica y matemática desarrollada por Florentin Smarandache orientada al estudio de fenómenos caracterizados por incertidumbre, contradicción e indeterminación. A diferencia de la lógica clásica binaria, la lógica neutrosófica permite representar simultáneamente tres dimensiones independientes: verdad (T),

indeterminación (I) y falsedad (F), proporcionando un marco flexible para modelar situaciones ambiguas o parcialmente conocidas.

La representación neutrosófica básica se expresa mediante:

$A=(T,I,F), T,I,F \in [0,1]$

donde:

- T representa el grado de verdad;
- I representa el nivel de indeterminación;
- F representa el grado de falsedad.

Las aplicaciones recientes de la neutrosofía se han extendido hacia áreas como: inteligencia artificial, sistemas de decisión multicriterio, análisis organizacional, gestión de riesgos, ciencias computacionales.

Broumi et al. [2] sostienen que la neutrosofía permite representar de manera más adecuada fenómenos complejos donde la información disponible es incompleta, contradictoria o incierta. A nivel de ciberseguridad, este enfoque resulta particularmente relevante debido a que los comportamientos humanos frecuentemente presentan inconsistencias entre conocimiento, percepción y acción.

Desde esta perspectiva, el análisis neutrosófico permite modelar escenarios donde un usuario puede: conocer las buenas prácticas de seguridad, percibir riesgos digitales, y mantener simultáneamente conductas inseguras.

Esta capacidad para representar contradicciones conductuales constituye una ventaja frente a enfoques estadísticos tradicionales basados únicamente en relaciones lineales y mediciones ordinales.

2.7. Estado del arte y brecha científica

La literatura científica reciente evidencia un creciente interés por analizar la relación entre conciencia de ciberseguridad y comportamiento humano en entornos digitales. Diversos estudios han demostrado que variables como percepción del riesgo, experiencia tecnológica y formación en seguridad influyen significativamente en la adopción de prácticas seguras relacionadas con autenticación digital y gestión de credenciales [1, 6].

Asimismo, investigaciones recientes desarrolladas en instituciones de educación superior identifican que estudiantes y usuarios universitarios presentan comportamientos contradictorios frente a la seguridad informática, manteniendo prácticas inseguras aun cuando poseen conocimientos básicos sobre protección digital [3]. Estos hallazgos han impulsado el desarrollo de enfoques centrados en behavioral cybersecurity y factor humano.

Sin embargo, la mayoría de investigaciones actuales continúa utilizando enfoques estadísticos convencionales basados en escalas Likert, análisis correlacionales y modelos lineales tradicionales. Aunque estos métodos permiten identificar asociaciones generales entre variables, presentan limitaciones para representar explícitamente fenómenos de incertidumbre, ambigüedad y contradicción conductual presentes en el comportamiento humano.

La aplicación de modelos neutrosóficos en investigaciones sobre autenticación digital y gestión de contraseñas continúa siendo limitada, particularmente en entornos universitarios latinoamericanos. La escasa evidencia empírica sobre el uso de neutrosofía para modelar niveles de verdad, indeterminación y falsedad en comportamientos de ciberseguridad constituye una brecha metodológica relevante dentro del campo de la ciberseguridad centrada en el usuario.

3. METODOLOGÍA

3.1 Enfoque de investigación

La presente investigación se desarrolló bajo un enfoque cuantitativo, debido a que se orientó a medir y analizar la relación existente entre la conciencia de ciberseguridad y el uso de contraseñas robustas mediante procedimientos

estadísticos y modelamiento neutrosófico. El enfoque cuantitativo permitió obtener información objetiva sobre los comportamientos de autenticación digital de los participantes y establecer relaciones entre las variables de estudio a partir de datos numéricos [4].

Asimismo, el estudio incorporó un enfoque complementario basado en lógica neutrosófica con el propósito de representar niveles de verdad, indeterminación y falsedad presentes en los comportamientos asociados a la gestión de credenciales digitales. Este enfoque permitió modelar fenómenos de ambigüedad conductual difíciles de representar mediante técnicas estadísticas convencionales.

3.2 Diseño y tipo de investigación

La investigación correspondió a un diseño no experimental de corte transversal, debido a que las variables fueron analizadas sin manipulación deliberada y la recolección de información se realizó en un único momento temporal.

El alcance del estudio fue correlacional-explicativo, ya que buscó determinar la relación existente entre la conciencia de ciberseguridad y el uso de contraseñas robustas en usuarios universitarios, así como analizar el comportamiento de dichas variables desde una perspectiva neutrosófica.

De acuerdo con Hernández-Sampieri y Mendoza [4], los estudios correlacionales permiten identificar asociaciones entre variables y evaluar el grado de relación existente entre fenómenos observables dentro de un contexto específico.

3.3 Contexto de estudio

El estudio se desarrolló en entornos universitarios de instituciones públicas ecuatorianas que utilizan plataformas digitales para la gestión académica y administrativa. El escenario resulta pertinente debido al elevado número de usuarios que interactúan diariamente con sistemas de autenticación digital, correos institucionales, entornos virtuales de aprendizaje y servicios en línea.

La elección del entorno universitario se fundamentó además en la creciente exposición de las instituciones de educación superior a incidentes relacionados con robo de credenciales, phishing y vulneraciones asociadas al comportamiento humano frente a la seguridad informática

3.4 Población y muestra

3.4.1. Población

La población estuvo conformada por 4.850 usuarios activos pertenecientes a universidades públicas ecuatorianas, incluyendo estudiantes, docentes y personal administrativo que utilizan regularmente plataformas digitales institucionales.

3.4.2. Muestra

Para determinar el tamaño de la muestra se utilizó la fórmula para poblaciones finitas con un nivel de confianza del 95% y un margen de error del 5%.

a fórmula aplicada fue:

$$n = \frac{N * Z^2 * p * q}{e^2(N-1) + z^2 * p * q}$$

Donde:

N=4850

Z=1.96

p=0.5

q=0.5

e=0.05

El cálculo determinó una muestra mínima de 356 participantes. Sin embargo, con el propósito de incrementar la representatividad estadística, la investigación consideró una muestra final de 384 participantes que respondieron adecuadamente las encuestas aplicadas, manteniendo los criterios de completitud y consistencia requeridos para el análisis estadístico, por lo que no fue necesario excluir registros durante la fase de depuración de datos. Se aplico un muestreo probabilístico estratificado en tres grupos: Estudiantes (230), Docentes (102) y Administrativos (52)

El muestreo estratificado permitió garantizar representación proporcional de los distintos grupos que conforman la población universitaria.

3.5 Variables de estudio

La investigación contempló dos variables principales:

Variable	Tipo	Dimensiones
Conciencia de ciberseguridad	Independiente	conocimiento, percepción del riesgo, cumplimiento de políticas, hábitos digitales
Uso de contraseñas robustas	Dependiente	longitud, complejidad, reutilización, actualización, uso de MFA

3.5.1. Operacionalización de variables

Variable independiente: Conciencia de ciberseguridad

Se conceptualizó como el conjunto de conocimientos, percepciones y comportamientos orientados a reconocer amenazas digitales y adoptar prácticas seguras en entornos tecnológicos.

Indicadores: reconocimiento de amenazas; percepción de vulnerabilidad; conocimiento de buenas prácticas; comportamiento preventivo.

Variable dependiente: Uso de contraseñas robustas

Se definió como el nivel de aplicación de prácticas seguras relacionadas con la creación, gestión y protección de credenciales digitales.

Indicadores: longitud de contraseña; complejidad; frecuencia de actualización; reutilización; uso de autenticación multifactor.

3.6. Hipótesis de investigación

Hipótesis general

H1: Existe una relación positiva y estadísticamente significativa entre la conciencia de ciberseguridad y el uso de contraseñas robustas en usuarios universitarios.

Hipótesis específicas

H2: Los usuarios con mayores niveles de conciencia de ciberseguridad presentan menores niveles de indeterminación neutrosófica en sus comportamientos de autenticación digital.

H3: La percepción del riesgo digital influye significativamente en la adopción de prácticas seguras relacionadas con la gestión de contraseñas.

H4: La reutilización de contraseñas se asocia negativamente con el nivel de awareness en ciberseguridad.

3.7. Técnicas e instrumentos de recolección de datos

La técnica principal de recolección de información fue la encuesta estructurada. Para ello se diseñó un cuestionario digital compuesto por 32 ítems distribuidos en dos secciones: Conciencia de ciberseguridad (18), Uso de contraseñas robustas (14). Los ítems fueron estructurados mediante escala Likert de cinco niveles: (1) Nunca, (2) Rara vez, (3) A veces, (4) Frecuentemente, (5) Siempre.

El instrumento fue adaptado a partir de escalas utilizadas en investigaciones recientes sobre cybersecurity awareness y password behavior [1, 11].

3.8. Validación y confiabilidad del instrumento

3.8.1. Validez de contenido

La validez de contenido fue determinada mediante juicio de expertos utilizando el coeficiente V de Aiken. Participaron cinco especialistas expertos en áreas como: ciberseguridad, metodología de investigación, estadística aplicada, neutrosofía. Los resultados evidenciaron valores superiores a 0.85 en todos los ítems, indicando adecuada pertinencia, claridad y coherencia conceptual.

3.8.2. Prueba piloto

Se realizó una prueba piloto con 30 participantes pertenecientes a la población objetivo con el propósito de evaluar: comprensión de ítems, tiempo de respuesta, consistencia interna, estabilidad del instrumento.

3.8.3. Confiabilidad

La confiabilidad fue determinada mediante el coeficiente Alfa de Cronbach. Los resultados obtenidos fueron:

Dimensión	**Alfa**
Conciencia de ciberseguridad	0.91
Contraseñas robustas	0.88
Instrumento global	0.90

Los valores obtenidos evidenciaron niveles adecuados de consistencia interna, de acuerdo con los criterios establecidos por Hernández-Sampieri y Mendoza [4].

3.9. Procedimiento de recolección de datos

La aplicación del instrumento se realizó mediante formulario digital distribuido a través de plataformas institucionales y correo electrónico universitario. Previamente a la participación, los usuarios recibieron un consentimiento informado donde se explicó: objetivo del estudio, carácter voluntario, anonimato, confidencialidad de la información. La recolección de datos se desarrolló durante un período de cuatro semanas.

3.10. Análisis estadístico

El procesamiento estadístico de la información se realizó utilizando el software IBM SPSS Statistics versión 27 y el lenguaje R para análisis complementarios. Las técnicas estadísticas aplicadas fueron:

Técnica	**Propósito**
Estadística descriptiva	frecuencias, medias, desviación estándar
Shapiro-Wilk	normalidad
Spearman	correlación
Regresión lineal	análisis predictivo
Alfa de Cronbach	confiabilidad
V de Aiken	validez

Debido a que las variables presentaron comportamiento no paramétrico, se utilizó el coeficiente de correlación de Spearman para determinar el nivel de relación entre conciencia de ciberseguridad y uso de contraseñas robustas. El nivel de significancia estadística establecido fue: $p < 0.05$

3.11. Modelo neutrosófico aplicado

El estudio incorporó un modelo neutrosófico complementario para representar niveles de verdad, indeterminación y falsedad asociados a los comportamientos de autenticación digital.

La representación neutrosófica utilizada fue: $A = (T,I,F)$

Donde:

- T representa el grado de comportamiento seguro;
- I representa el nivel de indeterminación conductual;
- F representa el grado de comportamiento inseguro.

La conversión de respuestas Likert hacia valores neutrosóficos se realizó mediante una escala de equivalencia definida por expertos.

Likert	T	I	F
5	0.90	0.05	0.05
4	0.70	0.20	0.10
3	0.50	0.40	0.10
2	0.30	0.40	0.30
1	0.10	0.20	0.70

Posteriormente, se aplicó un análisis multicriterio basado en lógica neutrosófica para identificar perfiles conductuales asociados a: alta conciencia y bajo riesgo, conciencia moderada con indeterminación, baja conciencia y alta vulnerabilidad.

Este modelo permitió complementar el análisis estadístico tradicional mediante la representación explícita de contradicciones e incertidumbre presentes en los comportamientos de seguridad digital.

4. RESULTADOS

4.1. Resultados descriptivos

La investigación contó con la participación de 384 usuarios pertenecientes a universidades públicas ecuatorianas. La distribución de la muestra evidenció predominio de estudiantes universitarios, seguidos de docentes y personal administrativo, como se muestra en la tabla 1.

Tabla 1

Distribución de participantes por estrato

Estrato	Frecuencia	Porcentaje
Estudiantes	230	59.9%
Docentes	102	26.6%
Administrativos	52	13.5%
Total	**384**	**100%**

Los resultados muestran una representación adecuada de los principales grupos que utilizan plataformas digitales institucionales dentro del entorno universitario.

4.1.1. Nivel de conciencia de ciberseguridad

El análisis descriptivo evidenció que el 61.2% de los participantes presentó niveles altos de conciencia de ciberseguridad, mientras que el 27.3% mostró niveles moderados y el 11.5% niveles bajos, tal como se muestra en la tabla 2.

Tabla 2

Nivel de conciencia de ciberseguridad

Nivel	Frecuencia	Porcentaje
Bajo	44	11.5%
Moderado	105	27.3%
Alto	235	61.2%
Total	**384**	**100%**

Estos resultados sugieren que la mayoría de los participantes posee conocimientos generales sobre amenazas digitales y buenas prácticas de seguridad informática.

4.1.2. Uso de contraseñas robustas

Respecto a las prácticas de autenticación digital, el 54.7% de los usuarios presentó niveles adecuados de uso de contraseñas robustas, mientras que el 31.8% evidenció niveles moderados y el 13.5% niveles bajos, como se muestra en la tabla 3.

Tabla 3

Nivel de uso de contraseñas robustas

Nivel	Frecuencia	Porcentaje
Bajo	52	13.5%
Moderado	122	31.8%
Alto	210	54.7%
Total	**384**	**100%**

Aunque la mayoría de participantes reportó prácticas relativamente seguras, aún se identificaron comportamientos de riesgo asociados a reutilización de credenciales y actualización poco frecuente de contraseñas.

4.1.3. Comportamientos específicos relacionados con autenticación digital

El análisis detallado de los ítems mostró que el 68.5% de los participantes manifestó utilizar contraseñas con más de ocho caracteres, mientras que únicamente el 42.7% indicó utilizar autenticación multifactor de manera frecuente. Asimismo, el 37.8% reconoció reutilizar contraseñas en múltiples plataformas digitales, tal como se muestra en la tabla 4.

Tabla 4

Prácticas específicas de autenticación digital

Práctica evaluada	Frecuencia	Porcentaje
Uso de contraseñas > 8 caracteres	263	68.5%
Uso frecuente de MFA	164	42.7%
Actualización periódica	197	51.2%
Reutilización de contraseñas	145	37.8%

Los resultados reflejan que, aunque existen niveles aceptables de awareness, persisten prácticas inseguras relacionadas con autenticación digital.

4.2. Pruebas de normalidad

Previamente al análisis correlacional se aplicó la prueba de normalidad de Shapiro-Wilk. El cual se muestra en la tabla 5.

Tabla 5

Prueba de normalidad

Variable	Estadístico W	p-valor
Conciencia de ciberseguridad	0.931	0.000
Uso de contraseñas robustas	0.918	0.000

Debido a que los valores de significancia fueron inferiores a 0.05: $p < 0.05$

se determinó que las variables no seguían una distribución normal, motivo por el cual se utilizó el coeficiente de correlación de Spearman para el análisis inferencial.

4.3. Análisis correlacional

Con el propósito de determinar la relación entre conciencia de ciberseguridad y uso de contraseñas robustas se aplicó el coeficiente Rho de Spearman, como se muestra en la tabla 6.

Tabla 6

Correlación entre conciencia de ciberseguridad y uso de contraseñas robustas

Variables	Rho de Spearman	p-valor
Conciencia de ciberseguridad ↔ Uso de contraseñas robustas	0.742	0.000

Los resultados evidenciaron una correlación positiva alta y estadísticamente significativa entre ambas variables: $\rho=0.742$, $p<0.05$

Esto indica que mayores niveles de conciencia de ciberseguridad se asocian con mejores prácticas relacionadas con autenticación digital y gestión de contraseñas. En consecuencia, se acepta la hipótesis general: Existe una relación positiva y estadísticamente significativa entre la conciencia de ciberseguridad y el uso de contraseñas robustas en usuarios universitarios.

4.4. Correlaciones por dimensiones

El análisis por dimensiones mostró que la percepción del riesgo digital presentó la asociación más alta con el uso de contraseñas robustas, como se muestra en la tabla 7.

Tabla 7

Correlaciones entre dimensiones

Dimensión	Rho	p-valor
Conocimiento de amenazas - Contraseñas robustas	0.681	0.000
Percepción del riesgo - Contraseñas robustas	0.758	0.000
Cumplimiento de políticas - Contraseñas robustas	0.703	0.000
Hábitos digitales - Contraseñas robustas	0.719	0.000

Los resultados evidencian que la percepción del riesgo constituye uno de los factores más influyentes en la adopción de prácticas seguras de autenticación digital.

4.5. Análisis de regresión

Se aplicó un modelo de regresión lineal simple para evaluar el nivel predictivo de la conciencia de ciberseguridad sobre el uso de contraseñas robustas, el cual se muestra en la tabla 8.

Tabla 8

Modelo de regresión lineal

Variable predictora	β	t	p
Conciencia de ciberseguridad	0.693	14.281	0.000

Coeficiente de determinación: $R^2=0.537$

El modelo explicó el 53.7% de la variabilidad asociada al uso de contraseñas robustas, evidenciando capacidad predictiva moderadamente alta.

4.6. Análisis neutrosófico

Con el propósito de modelar fenómenos de incertidumbre y contradicción conductual se realizó un análisis neutrosófico basado en los componentes: A = (T,I,F)

donde:

- T representa comportamiento seguro;
- I representa indeterminación;
- F representa comportamiento inseguro.

4.6.1. Conversión neutrosófica

Las respuestas obtenidas mediante escala Likert fueron transformadas hacia valores neutrosóficos utilizando la matriz de equivalencia definida en la metodología. El procesamiento permitió identificar perfiles conductuales diferenciados, el cual se muestra en la tabla 9.

Tabla 9

Perfil neutrosófico de comportamiento digital

Perfil	T	I	F
Usuarios con alta seguridad	0.86	0.08	0.06
Usuarios con conciencia moderada	0.63	0.25	0.12
Usuarios vulnerables	0.32	0.41	0.27

Los resultados evidencian que los usuarios con conciencia moderada presentaron niveles elevados de indeterminación conductual, reflejando contradicciones entre conocimiento y comportamiento real.

4.6.2. Interpretación de la indeterminación neutrosófica

El análisis neutrosófico permitió identificar escenarios donde los participantes manifestaban conocer buenas prácticas de seguridad, pero simultáneamente mantenían comportamientos inseguros como: reutilización de contraseñas, ausencia de autenticación multifactor, almacenamiento inseguro de credenciales. Este fenómeno generó niveles moderados de indeterminación representados mediante el componente: $I=0.25$

La presencia de indeterminación confirma que los modelos estadísticos tradicionales presentan limitaciones para representar contradicciones conductuales presentes en los comportamientos de autenticación digital.

4.7. Integración de resultados

Los resultados estadísticos y neutrosóficos evidencian que la conciencia de ciberseguridad influye significativamente en la adopción de prácticas seguras relacionadas con autenticación digital. No obstante, el análisis neutrosófico permitió identificar que ciertos usuarios presentan simultáneamente conocimiento sobre seguridad informática y comportamientos inconsistentes frente a la protección de credenciales.

Por lo tanto, el enfoque neutrosófico complementó el análisis correlacional tradicional al representar explícitamente niveles de ambigüedad e incertidumbre presentes en el comportamiento humano frente a la seguridad digital.

5. DISCUSIÓN

Los resultados obtenidos evidenciaron la existencia de una relación positiva y estadísticamente significativa entre la conciencia de ciberseguridad y el uso de contraseñas robustas en usuarios universitarios, confirmando la hipótesis general de investigación. El coeficiente de correlación de Spearman obtenido:

$\rho=0.742$, $p<0.05$

demostró que mayores niveles de awareness en ciberseguridad se asocian con prácticas más seguras relacionadas con autenticación digital y gestión de credenciales. Estos hallazgos coinciden con investigaciones recientes desarrolladas en contextos educativos, donde se ha identificado que el conocimiento sobre amenazas digitales influye significativamente en la adopción de comportamientos preventivos frente a riesgos cibernéticos [1].

Los resultados descriptivos mostraron que el 61.2% de los participantes presentó niveles altos de conciencia de ciberseguridad; sin embargo, aún persistieron prácticas inseguras relacionadas con reutilización de contraseñas y limitada adopción de autenticación multifactor. Estos hallazgos son consistentes con lo reportado por Wash y Rader [11], quienes sostienen que los usuarios suelen priorizar memorabilidad y facilidad de uso por encima de la robustez de las credenciales. En este sentido, los resultados confirman la existencia de una discrepancia entre conocimiento y comportamiento, fenómeno ampliamente discutido dentro del campo de behavioral cybersecurity.De manera particular, el análisis por dimensiones evidenció que la percepción del riesgo digital presentó la asociación más alta con el uso de contraseñas robustas:

$\rho=0.758$

Este resultado guarda coherencia con los postulados de la Protection Motivation Theory (PMT), la cual establece que los individuos adoptan conductas preventivas cuando perciben niveles elevados de severidad y vulnerabilidad frente a amenazas potenciales. En consecuencia, los participantes que mostraron mayor percepción de exposición a ataques cibernéticos tendieron a implementar prácticas de autenticación más seguras, incluyendo uso de contraseñas complejas y actualización periódica de credenciales.

Asimismo, el estudio evidenció que la reutilización de contraseñas continúa siendo una práctica frecuente entre usuarios universitarios, observándose en el 37.8% de los participantes. Este comportamiento coincide con investigaciones recientes sobre autenticación digital, las cuales sostienen que muchos usuarios reutilizan credenciales debido a limitaciones cognitivas relacionadas con memorización y fatiga de seguridad [7]. A pesar de que los participantes manifestaron niveles moderados y altos de conocimiento sobre buenas prácticas de seguridad informática, una proporción importante continuó manteniendo hábitos digitales vulnerables.

Desde una perspectiva metodológica, uno de los principales aportes de la investigación corresponde a la incorporación del análisis neutrosófico como complemento al análisis estadístico tradicional. Mientras las técnicas correlacionales permitieron identificar relaciones significativas entre variables, el modelo neutrosófico posibilitó representar explícitamente niveles de ambigüedad e incertidumbre presentes en el comportamiento humano frente a la seguridad digital.

El análisis neutrosófico evidenció que ciertos usuarios manifestaban simultáneamente: conocimiento adecuado sobre ciberseguridad; percepción de riesgo digital; comportamientos inseguros relacionados con autenticación.

Esta contradicción conductual fue representada mediante niveles moderados de indeterminación: $I=0.25$

lo cual confirma que los modelos clásicos de análisis presentan limitaciones para representar fenómenos caracterizados por inconsistencia conductual y toma de decisiones ambiguas.

Estos hallazgos guardan relación con los planteamientos de Florentin Smarandache sobre la capacidad de la lógica neutrosófica para modelar escenarios donde coexisten simultáneamente verdad, falsedad e indeterminación. En el contexto de la presente investigación, dicha capacidad permitió representar usuarios que conocen las buenas prácticas de seguridad, pero que no las aplican consistentemente en sus comportamientos cotidianos.

Desde el punto de vista científico, los resultados sugieren que la conciencia de ciberseguridad no debe analizarse únicamente desde dimensiones cognitivas, sino también desde componentes conductuales y contextuales asociados a hábitos digitales, percepción del riesgo y toma de decisiones bajo incertidumbre. En consecuencia, las estrategias institucionales orientadas al fortalecimiento de la cultura de ciberseguridad deberían superar los enfoques tradicionales basados exclusivamente en capacitación técnica y considerar modelos integrales centrados en behavioral cybersecurity.

Adicionalmente, el modelo de regresión evidenció que la conciencia de ciberseguridad explicó el 53.7% de la variabilidad asociada al uso de contraseñas robustas: $R2=0.537$

Este resultado demuestra que, aunque el awareness constituye un factor relevante, existen otras variables que podrían influir en los comportamientos de autenticación digital, tales como: cultura organizacional; presión social; experiencia tecnológica; fatiga digital; percepción de usabilidad; confianza en plataformas digitales.

Por tanto, futuras investigaciones podrían incorporar modelos multivariados más complejos que integren factores psicológicos, sociales y organizacionales para ampliar la comprensión de los comportamientos asociados a la gestión de credenciales digitales.

En términos prácticos, los resultados evidencian la necesidad de fortalecer las políticas institucionales relacionadas con autenticación digital dentro de las universidades, promoviendo: campañas permanentes de concienciación; implementación obligatoria de autenticación multifactor; uso de gestores de contraseñas; simulaciones de phishing; programas de formación centrados en behavioral cybersecurity.

Finalmente, la investigación aporta evidencia empírica relevante para contextos latinoamericanos, particularmente en instituciones de educación superior, donde aún existen limitados estudios que integren enfoques estadísticos y neutrosóficos para el análisis del comportamiento humano frente a la ciberseguridad. En este sentido, el estudio contribuye tanto al fortalecimiento de la línea de investigación sobre awareness en seguridad digital como al desarrollo metodológico de aplicaciones neutrosóficas en ciencias computacionales y comportamiento organizacional.

5.1. Implicaciones prácticas derivadas del análisis neutrosófico

El análisis neutrosófico permitió identificar distintos perfiles conductuales relacionados con la gestión de contraseñas y autenticación digital. A diferencia de los enfoques tradicionales, este modelo evidenció que los usuarios pueden presentar simultáneamente comportamientos seguros, inseguros y niveles de indeterminación frente a la ciberseguridad.

En función de los resultados obtenidos, se proponen estrategias diferenciadas orientadas a fortalecer la cultura institucional de ciberseguridad según el perfil neutrosófico de los usuarios.

5.1.1. Usuarios con altos niveles de falsedad neutrosófica (F > 0.50)

Este grupo presentó prácticas inseguras relacionadas con reutilización de contraseñas, uso de credenciales débiles y baja adopción de autenticación multifactor.

Para este perfil se recomienda:

- programas obligatorios de capacitación básica en ciberseguridad;
- implementación de gestores de contraseñas corporativos;
- aplicación de políticas de complejidad mínima de credenciales;
- activación obligatoria de autenticación multifactor en sistemas críticos.

Estas estrategias buscan reducir vulnerabilidades asociadas al desconocimiento y a hábitos digitales inseguros.

5.1.2. Usuarios con niveles moderados de indeterminación neutrosófica (I > 0.30)

Los usuarios con niveles moderados de indeterminación evidenciaron contradicciones entre conocimiento y comportamiento real frente a la seguridad digital.

Para este perfil se recomienda:

- implementación de estrategias de microlearning;
- recordatorios automatizados para actualización de contraseñas;
- simulaciones periódicas de phishing;
- mensajes contextuales de concienciación en plataformas institucionales.

Estas acciones buscan disminuir la brecha entre awareness y comportamiento seguro mediante refuerzo continuo de hábitos digitales.

5.1.3. Usuarios con altos niveles de verdad neutrosófica (T > 0.75)

Este grupo presentó altos niveles de conciencia de ciberseguridad y adopción consistente de prácticas seguras de autenticación digital.

Para este perfil se recomienda:

- designación como embajadores de ciberseguridad;
- participación en programas avanzados de formación;
- colaboración en revisión de políticas institucionales;
- apoyo en procesos de sensibilización organizacional.

Estos usuarios representan un recurso estratégico para fortalecer la cultura institucional de seguridad digital y promover buenas prácticas dentro de los entornos universitarios.

6. CONCLUSIONES

La investigación evidenció una relación positiva y estadísticamente significativa entre la conciencia de ciberseguridad y el uso de contraseñas robustas en usuarios universitarios, demostrando que mayores niveles de awareness se asocian con prácticas más seguras de autenticación digital.

Los resultados descriptivos mostraron que, aunque gran parte de los participantes presentó niveles moderados y altos de conciencia de ciberseguridad, persistieron comportamientos vulnerables como reutilización de contraseñas y limitada adopción de autenticación multifactor. Esto confirma la existencia de una brecha entre conocimiento y comportamiento real frente a la seguridad digital.

Asimismo, la percepción del riesgo digital se identificó como uno de los factores con mayor influencia en la adopción de prácticas seguras, respaldando los enfoques de behavioral cybersecurity y los fundamentos teóricos de la Protection Motivation Theory y la Theory of Planned Behavior.

Uno de los principales aportes del estudio fue la incorporación del análisis neutrosófico como complemento metodológico para representar niveles de verdad, falsedad e indeterminación presentes en los comportamientos de autenticación digital. Este enfoque permitió identificar contradicciones conductuales que no pueden ser representadas completamente mediante modelos estadísticos tradicionales.

Desde el punto de vista práctico, los hallazgos evidencian la necesidad de fortalecer las estrategias institucionales de ciberseguridad mediante programas diferenciados según el perfil conductual de los usuarios, incorporando capacitación continua, autenticación multifactor y mecanismos de concienciación basados en behavioral cybersecurity.

Finalmente, la investigación aporta evidencia empírica y metodológica relevante para el contexto universitario latinoamericano, contribuyendo al desarrollo de estudios sobre factor humano, autenticación digital y aplicaciones neutrosóficas en ciberseguridad.

REFERENCIAS BIBLIOGRÁFICAS

[1]. Alqahtani, M. A. (2022). *Factors affecting cybersecurity awareness among university students*. Applied Sciences, 12(5), 2589. https://doi.org/10.3390/app12052589

[2]. Broumi, S., Smarandache, F., Bakali, A., Talea, M., & Ali, M. (2021). *Neutrosophic sets and systems in decision-making and artificial intelligence*. Neutrosophic Sets and Systems, 42, 1–15. https://digitalrepository.unm.edu/nss_journal/vol42/iss1/

[3]. Goliath, S., Tsibolane, P., & Snyman, D. (2024). *Exploring the cybersecurity-resilience gap: An analysis of student attitudes and behaviors in higher education*. arXiv. https://arxiv.org/abs/2411.03219

[4]. Hernández-Sampieri, R., & Mendoza, C. (2021). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta* (2.ª ed.). McGraw-Hill.

[5]. URL: McGraw-Hill Metodología de la Investigación

[6]. Ifinedo, P. (2022). *Understanding information systems security policy compliance: An integration of the theory of planned behavior and protection motivation theory*. Computers & Security, 118, 102747. https://doi.org/10.1016/j.cose.2022.102747

[7]. Merdenyan, B., & Petrie, H. (2022). *Two studies of the perceptions of risk, benefits and likelihood of undertaking password management behaviours*. Behaviour & Information Technology, 41(12), 2514–2527. https://doi.org/10.1080/0144929X.2021.2019832

[8]. NIST. (2024). *Digital identity guidelines: Authentication and lifecycle management (SP 800-63B)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63b

[9]. Sivakumar, S., & Venkataraman, S. (2025). *Cracks in digital defense: A study on password security awareness and behavior in college students*. International Journal of Scientific Computing. 9(1) https://doi.org/10.21917/ijsc.2025.0557

[10]. Suleiman, A., & Svetinovic, D. (2023). *A review of behavioral cybersecurity research and future directions*. Computers & Security, 129, 103237. https://doi.org/10.1016/j.techsoc.2023.102258

[11]. Wash, R., & Rader, E. (2021). *Prioritizing security over usability: Strategies for how people choose passwords*. Journal of Cybersecurity, 7(1), tyab012. https://doi.org/10.1093/cybsec/tyab012