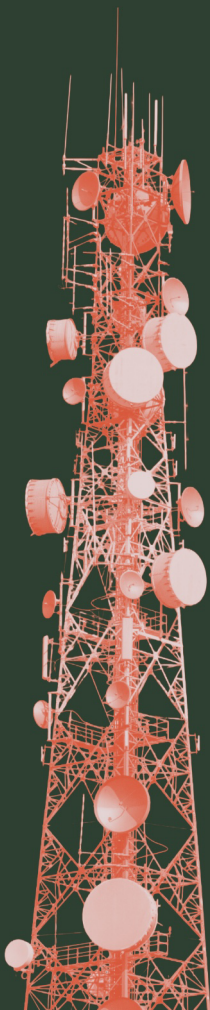
José Armando Tiznado Ubillus, Carmen Lucila Infante Saavedra,
Carlos Alberto Castro Carreño, Andrés Augustin Castillo Moscol,
Carlos Alberto Raymundo García

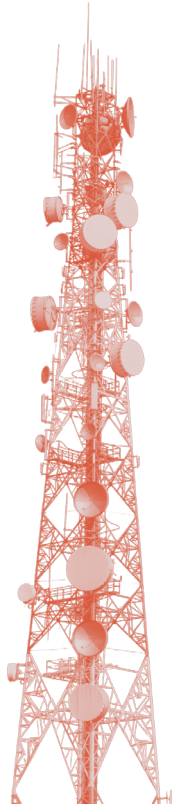
# CÓDIGO VULNERABLE

*La paradoja de la seguridad móvil en la era digital*



ATIK editorial

Colección Ingeniería



José Armando Tiznado Ubillus, Carmen Lucila Infante Saavedra,
Carlos Alberto Castro Carreño, Andrés Augustin Castillo Moscol,
Carlos Alberto Raymundo García

# Código vulnerable

*La paradoja de la seguridad móvil en la era digital*

**Atik** Editorial

E15D N49-59 y Olivos, San Isidro. Código postal 170515.
Quito, Ecuador
**Atik** *Editorial, es una iniciativa del Centro de Investigaciones CICSHAL y está a cargo del departamento de Comunicación y Difusión Científica.*
**www.atikeditorial.com**

**(APA 7)**

Tiznado Ubillus, J. A., Infante Saavedra, C. L., Castro Carreño, C. A., Castillo Moscol, A. A., y Raymundo García, C. A. (2026). *Código vulnerable. La paradoja de la seguridad móvil en la era digital*. Atik Editorial. https://doi.org/10.46652/atikbook23

El presente libro tienen el aval del Centro de Investigaciones en Ciencias y Humanidades desde América Latina - CICSHAL.


Título: Código vulnerable. La paradoja de la seguridad móvil en la era digital

Primera Edición: 2026



Editorial: Atik Editorial

Materia Dewey: 005 - Programación. programas. datos de computadores

Clasificación Thema: UBJ - Aspectos éticos y sociales de las tecnologías de las información | UR - Seguridad informática | URQ - Cortafuegos

Público objetivo: Profesional/Académico

BISAC: COM060040

Colección: Ingeniería

Soporte: Digital

Formato: Epub (.epub)/PDF (.pdf)

Publicado: 2026-02-13

ISBN: 978-9907-807-02-8

Disponible para su descarga gratuita en http://atikeditorial.com

Esta publicación es una obra derivada que surge de la tesis de maestría titulada "Riesgo y Seguridad en los Dispositivos Móviles en Estudiantes de la Carrera de Desarrollo de Software en el SENATI, 2019 ", defendida por José Armando Tiznado Ubillus en la Universidad César Vallejo (Perú) en el año 2019. Bajo la coordinación del propio autor de la tesis, un equipo de investigadores ha ampliado, profundizado y actualizado el trabajo original mediante un proceso colaborativo, dando lugar a este libro.

This publication is a derivative work originating from the master's thesis titled "Riesgo y Seguridad en los Dispositivos Móviles en Estudiantes de la Carrera de Desarrollo de Software en el SENATI, 2019 ", defended by José Armando Tiznado Ubillus at the Universidad César Vallejo (Perú) in 2019. Under the coordination of the thesis author himself, a team of researchers has expanded, deepened, and updated the original work through a collaborative process, resulting in this book.

# AVAL DE REVISIÓN POR PARES

El presente libro constituye el resultado de un riguroso proceso de investigación académica, cuya calidad metodológica y solidez argumental han sido validadas mediante un sistema de revisión por pares externos implementado bajo el protocolo de doble ciego, bajo la supervisión del Centro de Investigaciones en Ciencias y Humanidades desde América Latina (CICSHAL). Como garantía de transparencia y rigor científico, los informes de evaluación realizados por los especialistas designados se conservan en el archivo institucional de la editorial, a disposición de las instancias que así lo requieran.

This book is the result of a rigorous academic research process, whose methodological quality and argumentative solidity have been validated through an external peer-review system implemented under a double-blind protocol, under the supervision of the Center for Research in Sciences and Humanities from Latin America (CICSHAL). As a guarantee of transparency and scientific rigor, the evaluation reports prepared by the designated specialists are preserved in the publisher's institutional archives, available to any party that may require them.

info@atikeditorial.com

ATIK editorial

# AUTORES

*AUTHORS*

**José Armando Tiznado Ubillus**
Universidad Nacional Mayor San Marcos | Lima | Perú
https://orcid.org/0000-0003-0505-510X
jose.tiznado@unmsm.edu.pe
drjtiznado@gmail.com
Candidato a Doctor en Ingeniería de Sistemas e Informática por la UNMSM y Magíster en Ingeniería de Sistemas con mención en Tecnologías de la Información, con una trayectoria consolidada en investigación científica e innovación tecnológica, orientada a la generación de conocimiento aplicado. Docente en instituciones de prestigio, articula la formación académica con la práctica profesional en desarrollo de software y tecnologías de información, y participa activamente en la publicación de artículos científicos en su especialidad.

**Carmen Lucila Infante Saavedra**
Universidad Nacional de Piura | Piura | Perú
https://orcid.org/0000-0002-5772-8807
cinfantes@unp.edu.pe
Ingeniero Industrial con orientación en Sistemas e Informática, Magister en Informática, Doctora en Tecnologías de Información y Comunicación, Doctoranda en Administración de Empresas, Certificada por la Universidad de Liverpool en el curso Adaptación e implementación de cursos virtuales, asesora y jurado de tesis de pregrado y posgrado, miembro del equipo de Semilleros de Investigación y docente principal hace 25 años de la Universidad Nacional de Piura

**Carlos Alberto Castro Carreño**
Universidad Tecnológica del Perú | Piura | Perú
https://orcid.org/0000-0001-7136-4774
ccastroca@utp.edu.pe
carlos_dir_tumbes@hotmail.com
Ingeniero Informático por la Universidad Nacional de Piura, Magister en Administración con Mención Gerencia Gubernamental por la Universidad Nacional de Piura, con estudios concluidos de doctorado en Administración en la Universidad Alas Peruanas.

**Andrés Augustin Castillo Moscol**
Universidad Nacional de Piura | Piura | Perú
https://orcid.org/0000-0002-8361-9225
acastillom@unp.edu.pe
andresaugustincastillomoscol@gmail.com
Licenciado en Matemática Pura, Magister en Matemática Aplicada y con estudios doctoral concluidos en Ingeniera Industrial de la Universidad Nacional de Piura. Docente con 20 años de Experiencia en Pre-Grado de la Universidad Nacional de Piura

**Carlos Alberto Raymundo García**
Universidad Nacional de Piura | Piura | Perú
https://orcid.org/0000-0001-8130-4636
craymundog@unp.edu.pe
charlesray39@hotmail.com
Licenciado en Física por la Universidad Nacional de Piura, Maestría en Matemática Aplicada por la Universidad Nacional de Piura, Doctorado en la Universidad Nacional de  Piura, docente adscrito al departamento de física de la Universidad Nacional de Piura

## RESUMEN

Este libro examina la paradoja central de nuestra era digital, donde la dependencia universal de los dispositivos móviles coexiste con una exposición creciente a riesgos informáticos. A partir de un caso de estudio en una institución educativa técnica, se analiza la relación crítica entre diversas amenazas cibernéticas, como el malware y las vulnerabilidades en aplicaciones, y los pilares fundamentales de la seguridad móvil, que son la confidencialidad, la integridad y la autenticación. La obra propone un enfoque metodológico para medir y gestionar estos riesgos, ofreciendo una guía esencial para proteger la información personal y financiera en el ecosistema móvil, con especial énfasis en plataformas de alta penetración como Android.

Palabra clave:
Seguridad móvil, riesgos informáticos, dispositivos móviles, vulnerabilidades, análisis de riesgos.

## ABSTRACT

This book examines the central paradox of our digital age, where universal dependence on mobile devices coexists with a growing exposure to information security risks. Based on a case study in a technical educational institution, it analyzes the critical relationship between various cyber threats, such as malware and application vulnerabilities, and the fundamental pillars of mobile security: confidentiality, integrity, and authentication. The work proposes a methodological approach to measure and manage these risks, offering an essential guide to protecting personal and financial information in the mobile ecosystem, with special emphasis on high-penetration platforms such as Android.

Keywords:
Mobile security, information risks, mobile devices, vulnerabilities, risk analysis.

# RESUMO

Este livro examina o paradoxo central da nossa era digital, em que a dependência universal dos dispositivos móveis coexiste com uma exposição crescente a riscos informáticos. A partir de um estudo de caso em uma instituição de ensino técnico, analisa-se a relação crítica entre diversas ameaças cibernéticas, como malware e vulnerabilidades em aplicações, e os pilares fundamentais da segurança móvel, que são a confidencialidade, a integridade e a autenticação. A obra propõe uma abordagem metodológica para medir e gerir esses riscos, oferecendo um guia essencial para proteger a informação pessoal e financeira no ecossistema móvel, com especial ênfase em plataformas de alta penetração, como o Android.

Palavras-chave:
Segurança móvel, riscos informáticos, dispositivos móviles, vulnerabilidades, análise de riscos.

# CONTENIDO

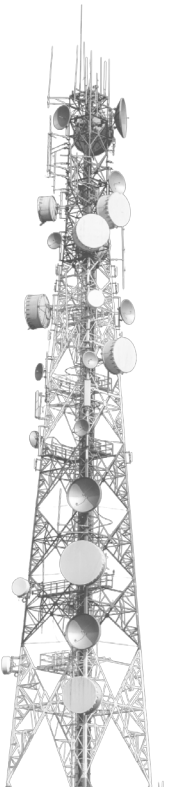
## LISTA DE TABLAS



## LISTA DE FIGURAS

**Código vulnerable**

*La paradoja de la seguridad móvil en la era digital*



# CAPÍTULO 1
# EL ADVENIMIENTO DE LA ERA DIGITAL Y SU DOBLE FILO

Los cimientos de la era digital contemporánea se remontan a los albores de la computación, un período marcado por invenciones paradigmáticas como la máquina concebida por Alan Turing, pieza fundamental para descifrar el código Enigma durante la Segunda Guerra Mundial. Este hito no solo representó un triunfo criptográfico sin precedentes, sino que también sentó las bases conceptuales para entender cómo la tecnología puede ser instrumentalizada tanto para la protección como para la intrusión de sistemas complejos. La transición desde esas máquinas monolíticas y especializadas hacia los dispositivos de cómputo personalizados y, finalmente, a la omnipresencia de los teléfonos inteligentes, ha sido exponencial. Sin embargo, esta evolución tecnológica vertiginosa ha dado lugar a una paradoja fundamental: la misma conectividad que potencia la productividad, la comunicación y el acceso al conocimiento también genera una superficie de ataque exponencialmente mayor y más diversificada. Nos encontramos, así, en un siglo XXI donde la figura del cibercriminal ha evolucionado desde el hacker aislado hacia sofisticadas organizaciones y redes que operan con motivaciones financieras, geopolíticas o de sabotaje, atacando indiscriminadamente infraestructuras críticas, entidades corporativas y la privacidad individual con una eficiencia alarmante. Este ecosistema de amenazas digitales ha transformado la seguridad de la información de un problema técnico periférico a una cuestión central de riesgo operacional, reputacional y legal para toda organización y individuo inmerso en la vida digital.

El panorama actual está caracterizado por un volumen y una sofisticación de ciberataques sin precedentes históricos, como lo documentan diversos informes sectoriales. Un reflejo de esta escalada se encuentra en el análisis de empresas especializadas en seguridad. Por ejemplo, según Mosquera (2016), quien reporta en el diario El Mundo, la firma Panda Security señaló que "2015 ha sido el año en el que se han producido más ciberataques en todo el mundo". Esta afirmación, respaldada por una muestra de 304 millones de detecciones, ilustra una tendencia creciente donde la creación de malware se convierte en una industria subterránea. El mismo análisis detalla que "el contenido de las intimidaciones se está elevando exponencialmente debido a los Exploit Kits (trozo de código de comando), principalmente son software diseñados para la

identificación de debilidades en los celulares y para procesar código dañino para el celular" (Mosquera, 2016). Los Exploit Kits representan un ejemplo claro de la industrialización del cibercrimen, herramientas empaquetadas que automatizan la búsqueda de vulnerabilidades conocidas en dispositivos, permitiendo a actores con diversos niveles de habilidad técnica lanzar campañas de infección masiva. Esta automatización del mal reduce las barreras de entrada para la delincuencia digital, democratizando en cierto sentido la capacidad de causar daño y ampliando el radio de acción de las amenazas más allá de los objetivos tradicionales de alto valor.

La convergencia de esta amenaza industrializada con la plataforma tecnológica más penetrante del planeta, el dispositivo móvil, configura el epicentro de la problemática de seguridad contemporánea. Los teléfonos inteligentes han dejado de ser meros dispositivos de comunicación para convertirse en extensiones digitales del individuo, repositorios centralizados de su identidad digital. Como explicó Raúl Pérez, especialista de Panda Security, "los celulares y Tablet son estrechamente apetitoso para ellos, porque el poseedor de estos equipos almacena datos de casi toda su vida: como por ejemplo sus cuentas bancarias, imágenes, las zonas que han visitado, los deportes que realizan, lo que comunican frecuentemente en las redes sociales y a sus contactos" (Mosquera, 2016). Esta concentración de datos sensibles, combinada con prácticas de usuario no siempre diligentes y una superficie de ataque compleja (compuesta por el sistema operativo, las aplicaciones de terceros, la conectividad de red y los sensores físicos), convierte al móvil en el objetivo perfecto. La proyección realizada en 2016 sobre el incremento de amenazas móviles, específicamente aquellas que buscan privilegios de root o administrador, se ha materializado plenamente. La capacidad de un malware para obtener estos privilegios, como señalaba el análisis, donde "con solamente basta que los cybercriminales localicen una abertura en la seguridad para que acceda a posicionarse como el administrador" (Mosquera, 2016), implica un control casi total del dispositivo, permitiendo el robo de credenciales, el espionaje, el cifrado de datos para extorsión (ransomware) o la inclusión del dispositivo en una botnet.

**El teléfono inteligente. Un castillo con múltiples puertas entornadas**

La aparente mejora en las estadísticas de detección de malware, como las reportadas por Giusto (2018) para Android e iOS, no debe interpretarse como una reducción del riesgo inherente, sino más bien como un cambio en las dinámicas de la amenaza y una mejora en las capacidades de detección de los fabricantes de soluciones de seguridad. La reducción porcentual en las detecciones puede estar vinculada a la adopción de técnicas de ofuscación más avanzadas por parte del malware, a la migración de ataques hacia vectores menos monitorizados (como aplicaciones legítimas comprometidas o ataques a la cadena de suministro) o a la explotación de vulnerabilidades de día cero. El dato crucial que aporta Giusto (2018) es que "el 23% de los fallos publicados en 2018 existieron críticos y el 13% de ellos consentía la realización de código malicioso". Esto subraya que el núcleo del problema reside en las vulnerabilidades del software, errores de programación que, al ser descubiertos y no parcheados a tiempo, abren una ventana de oportunidad para los atacantes. La existencia de fallos críticos, aquellos que permiten un compromiso remoto o la elevación de privilegios, representa un riesgo sistémico. La recomendación concomitante, "los usuarios tienen que instalar a tiempo los parches de seguridad" (Giusto, 2018), choca frontalmente con la realidad del ecosistema móvil, caracterizado por la fragmentación en Android (donde la actualización depende del fabricante del hardware y la operadora) y por la posible reticencia del usuario a instalar actualizaciones por miedo a problemas de rendimiento o consumo de datos.

Figura 1. Vulnerabilidad en Android


Fuente: Welivessecurity: "Balance semestral de la seguridad móvil"

Esta vulnerabilidad intrínseca se vuelve particularmente alarmante al considerar la escala de adopción de la tecnología móvil. Los datos globales son elocuentes. Kemp (2018), citando estadísticas de Hootsuite, indica que "More than 200 million people achieved their 1st cell phone in 2017, and two thirds of the world's 7.6 million people now have cell phones". Esta masificación significa que miles de millones de personas, muchas de ellas con niveles dispares de alfabetización digital y conciencia sobre ciberseguridad, tienen en sus bolsillos un dispositivo que gestiona aspectos críticos de su vida. La inclusión financiera digital, por ejemplo, ha crecido a la par, con aplicaciones bancarias móviles convirtiéndose en la principal interfaz para transacciones en muchas regiones. Sin embargo, como demuestra el caso peruano reportado por El Diario La República (2018) y el Diario El Comercio (2018), este progreso es frágil. Los ataques coordinados contra el sistema bancario, como el que obligó a recomendaciones extremas como no realizar "ninguna transacción bancaria a través de internet y vía APP" (El Diario La República, 2018), exponen la interdependencia y la potencial fragilidad de los sistemas financieros digitales. Estos incidentes no son aislados; reflejan una tendencia global donde los grupos cibercriminales realizan pruebas de estrés contra infraestructuras nacionales, utilizando tácticas como el robo de credenciales vía phishing móvil, malware bancario (como el famoso Anubis o Cerberus) o ataques de denegación de servicio.

Figura 2. Digital in 2018


Fuente: Hootsuite (s.f.).

El impacto de estos sucesos trasciende lo económico para penetrar en la esfera de la confianza social y la percepción de seguridad. La rápida diseminación de información (y desinformación) a través de canales como WhatsApp durante la crisis bancaria peruana, tal como reportó el Diario El Comercio (2018) al mencionar que "la población estuvo al tanto de estos acontecimientos y fluyó bastante información por canales móviles como WhatsApp y redes sociales", introduce una variable adicional de complejidad. Las aplicaciones de mensajería, si bien son herramientas vitales para la comunicación, pueden actuar como amplificadores del pánico y vectores para la propagación de enlaces maliciosos o scams que se aprovechan de la situación de confusión. Esta conjunción de factores convierte el entorno móvil en un campo de batalla multidimensional, donde la seguridad técnica debe complementarse con la educación del usuario y la resiliencia operativa de las instituciones. Para una entidad educativa en formación profesional técnica superior cuyo compromiso es formar profesionales tecnológicamente competentes, esta realidad problemática adquiere una dimensión práctica inmediata, pues sus estudiantes no solo son usuarios potencialmente vulnerables, sino también futuros desarrolladores y administradores de los sistemas que deben proteger estas infraestructuras críticas.

## Construyendo defensas. De la teoría a la práctica en la seguridad móvil

La respuesta académica y profesional a este panorama desafiante se ha materializado en una creciente producción de investigación aplicada, tanto a nivel internacional como nacional, que busca comprender, medir y mitigar los riesgos informáticos en dispositivos móviles. Estos trabajos previos constituyen un corpus de conocimiento esencial para abordar el problema de manera sistemática y fundamentada. A nivel internacional, investigaciones como la de Rojas (2016) han puesto el foco en un eslabón crítico de la cadena: las aplicaciones financieras. Su estudio, que evaluó aplicaciones bancarias chilenas en Google Play mediante ingeniería inversa automatizada y análisis estático, reveló una tendencia preocupante hacia la solicitud de privilegios excesivos y la presencia de múltiples debilidades de programación. Este hallazgo es fundamental porque expone una falla en el modelo de seguridad por permisos, donde los usuarios, por prisa o desconocimiento, otorgan acceso extensivo a sus datos personales a aplicaciones que, en teoría, solo necesitan una funcionalidad específica. La investigación de López (2016) profundizó en la evaluación técnica de vulnerabilidades en dispositivos Android, proponiendo una metodología experimental para identificar vectores de ataque y validar la eficacia de contramedidas como los antivirus. Su trabajo reforzó la noción de que la configuración por defecto de muchos dispositivos es inadecuada y que la seguridad requiere una implementación proactiva de capas de protección que salvaguarden la confidencialidad, integridad y disponibilidad de la información, principios cardinales de la seguridad de la información.

Complementariamente, estudios como el de Erreyes (2017) abordaron la problemática desde una perspectiva metodológica y de selección de herramientas, reconociendo que la diversidad del ecosistema Android y la constante evolución de las amenazas exigen marcos de trabajo adaptables. La propuesta de una metodología para seleccionar recursos de seguridad eficientes busca empoderar al usuario final, ofreciendo criterios objetivos más allá del marketing de las soluciones comerciales. En una línea más especializada, Gar-

cía (2017) exploró el análisis forense en smartphones, una disciplina que se ha vuelto indispensable tanto para la investigación de incidentes de seguridad como para procesos legales. El desarrollo de metodologías forenses adaptadas a Android es una respuesta directa a la necesidad de obtener evidencias válidas de dispositivos que han sido blanco o herramienta de un ataque, cerrando así el ciclo de detección, respuesta y recuperación. A nivel nacional, la investigación ha transitado hacia la gestión integral del riesgo tecnológico. Los trabajos de Llontop (2018) y Otoya (2017) ejemplifican este enfoque, aplicando metodologías cuantitativas y modelos estandarizados para medir la eficiencia de la gestión de riesgos de TI en distintos contextos organizacionales, desde empresas comerciales hasta programas de desarrollo público. Estos estudios aportan una visión macro, necesaria para que las organizaciones prioricen inversiones y diseñen políticas de seguridad coherentes con sus objetivos.

De manera crucial, Huamán (2017) recordó que el eslabón más débil en la cadena de seguridad suele ser el humano, abogando por la construcción de una cultura organizacional sólida en seguridad de la información. Su propuesta de un plan de comunicaciones basado en modelos como el NIST subraya que la tecnología por sí sola es insuficiente; se requiere un cambio de comportamiento sostenido mediante la concientización y la educación continua. Esta perspectiva es vital para el ámbito educativo, donde se debe formar no solo en competencias técnicas, sino también en una ética y una mentalidad de seguridad proactiva. En conjunto, este corpus investigativo demuestra que abordar la seguridad móvil requiere un enfoque multidisciplinario que combine el análisis técnico de vulnerabilidades, la gestión estructurada del riesgo, el desarrollo de herramientas y metodologías forenses, y, de manera transversal, la promoción de una cultura de seguridad desde la base misma de la formación profesional y la práctica.

## Hacia una comprensión integral del riesgo y la seguridad digital

### De la noción básica a la gestión estratégica del riesgo

La conceptualización del riesgo informático ha evolucionado desde su percepción inicial como un término técnico hacia un constructo fundamental en la gestión organizacional moderna, con implicaciones legales, financieras y operativas profundas. Téllez (2008) contribuye a esta comprensión al enmarcar el riesgo, en un sentido amplio, como "la inseguridad o posibilidad de que suceda o se ejecute una casualidad, la cual podría estar pronosticada", precisando que, en esencia, "la palabra riesgo es la posibilidad de que ocurra un daño" (p. 158). Esta definición, aunque aparentemente simple, establece los dos pilares constitutivos de cualquier riesgo: la probabilidad de que un evento adverso ocurra y el impacto o daño potencial que dicho evento podría causar. Al aplicar esta lógica al ámbito digital, Téllez (2008) argumenta que los riesgos informáticos se refieren a esa misma incertidumbre, pero contextualizada en la posible materialización de una amenaza que cause daño a los bienes o servicios informáticos, los cuales abarcan un espectro tan amplio como los equipos informáticos, periféricos, instalaciones, proyectos, programas de cómputo, archivos, información, datos confidenciales e incluso la responsabilidad civil frente a terceros derivada de un servicio informático (p. 158). Esta enumeración destaca la naturaleza omnipresente y multifacética del riesgo en entornos tecnodependientes, donde un activo aparentemente intangible, como un archivo de datos, puede tener un valor económico y estratégico superior al del hardware que lo aloja.

La estandarización de este concepto ha sido impulsada por organismos internacionales, aportando perspectivas complementarias esenciales para su gestión práctica. La norma ISO 31000:2009, citada por Serra (2013), ofrece una visión más dinámica y orientada a los objetivos organizacionales, definiendo el riesgo como "el efecto de la incertidumbre sobre los objetivos" (p. 14). Esta formulación es poderosa porque desplaza el foco desde el daño per se hacia la interferencia con la consecución de metas, reconociendo que la incerti-

dumbre puede tener tanto consecuencias negativas como positivas (oportunidades). En el contexto de la ciberseguridad, esto implica que la gestión del riesgo no debe limitarse a una postura defensiva, sino que debe integrarse en la estrategia de negocio, evaluando cómo las decisiones tecnológicas (como la adopción de una nueva plataforma móvil en la empresa) pueden crear o mitigar incertidumbre en los objetivos de productividad, innovación o expansión de mercado. Por otro lado, la norma UNE-71504:2008, referenciada por Escrivá et al. (2013), introduce el crucial concepto de exposición, definiendo el riesgo como "el nivel de grado de exposición ante una amenaza" (p. 12). Esta perspectiva enfatiza la relación entre un activo vulnerable y una fuente de peligro, un nexo que es particularmente relevante para los dispositivos móviles, cuya exposición es constante debido a su portabilidad, conectividad multifacética y uso en contextos no controlados.

La síntesis de estas visiones conduce a un modelo relacional del riesgo, articulado claramente por Aguilera (2010), quien afirma: "Se le denomina riesgos a la supuesta presente que se puede materializar o no en una amenaza donde se aprovecha de una debilidad. No se puede decir riesgo ante una amenaza si no existe vulnerabilidades, ni tampoco si le puede decir vulnerabilidad si no existe la presencia de una amenaza" (p. 14). Esta afirmación establece la tríada fundamental de la seguridad de la información: Amenaza, Vulnerabilidad e Impacto. Una amenaza (por ejemplo, un cibercriminal que busca datos bancarios) solo se convierte en un riesgo real para una organización o individuo si existe una vulnerabilidad (por ejemplo, una aplicación móvil bancaria con un fallo de seguridad no parcheado) que pueda ser explotada, lo que a su vez generaría un impacto (pérdida financiera, fraude). La gestión, por tanto, se convierte en el arte de interrumpir esta cadena. Frente a un riesgo identificado, Aguilera (2010) postula tres cursos de acción estratégicos: aceptarlo (cuando el costo de la mitigación excede el impacto potencial), mitigarlo (aplicando controles para reducir la probabilidad o el impacto) o transferirlo (por ejemplo, mediante un seguro cibernético) (p. 14). Esta decisión no es meramente técnica, sino que requiere un análisis riguroso que considere el contexto específico de cada activo y proceso.

## El proceso de análisis de riesgos. Desglosando la complejidad

El análisis de riesgos constituye la metodología sistemática para operacionalizar estos conceptos teóricos. Según Aguilera (2010), este proceso implica "analizar y sistematizar los niveles de vulnerabilidades por cada uno de ellos que se puede presentar algunas amenazas y resaltando el valor del impacto de los ataques" (p. 12). Se trata de un ejercicio deliberado y estructurado que busca pasar de una percepción difusa de peligro a un inventario cuantificado y priorizado de riesgos específicos. El primer paso en este viaje analítico es la identificación y catalogación de los activos, definidos por Aguilera (2010) como "recursos que son perteneciente al propio sistema de la información o que tiene relación con él" (p. 12). En el ecosistema móvil contemporáneo, esta clasificación adquiere matices críticos. Los datos son, indiscutiblemente, el activo primordial; en un smartphone residen no solo datos laborales o financieros, sino también la huella digital personal completa, cuyo valor en mercados subterráneos es enorme. El software ya no se limita al sistema operativo y aplicaciones de escritorio, sino que incluye el complejo stack de apps móviles, sus SDKs (kits de desarrollo de software) y las APIs (interfaces de programación de aplicaciones) que interconectan servicios, cada una siendo un potencial vector de ataque si su desarrollo no sigue prácticas seguras (Shabtai et al., 2012).

El hardware móvil presenta desafíos únicos: es a la vez un dispositivo de consumo masivo y una potente herramienta de cómputo, con sensores (GPS, cámara, micrófono) que, si son comprometidos, convierten al teléfono en un dispositivo de vigilancia perfecto. Las redes en este contexto son inherentemente inseguras; los dispositivos se conectan alternativamente a Wi-Fi domésticos, redes corporativas, puntos de acceso públicos no confiables y redes de datos 4G/5G, multiplicando los vectores de ataque man-in-the-middle. Los soportes de almacenamiento se han virtualizado en gran medida (almacenamiento en la nube), pero la memoria física del dispositivo y las tarjetas SD externas siguen siendo objetivos. Las instalaciones como concepto se diluyen, pues el dispositivo opera en espacios físicos no controlados. El per-

sonal usuario es, en este escenario, simultáneamente el operador final y, con frecuencia, el eslabón más débil, cuyas decisiones (instalar apps de fuentes no oficiales, hacer clic en enlaces de phishing) pueden anular las mejores defensas técnicas. Finalmente, los servicios móviles, desde el correo y la mensajería instantánea hasta las plataformas de banca y comercio electrónico, concentran funcionalidad y riesgo, siendo el punto de interacción donde las amenazas buscan materializarse.

Identificados los activos, el análisis procede a evaluar las amenazas que los acechan. Aguilera (2010) describe la amenaza como un factor, ya sea humano, mecánico o ambiental, que aprovecharía una debilidad para causar daño (p. 13). En la esfera móvil, esta tipología se ha sofisticado enormemente. Además, las amenazas no son puramente digitales; el robo o pérdida física del dispositivo es una amenaza tangible que compromete todos los datos almacenados en él si no está adecuadamente protegido con cifrado y controles de acceso robustos. La intersección entre el activo (el smartphone con datos sensibles) y la amenaza (un malware de robo de información o un ladrón) define el espacio donde el riesgo se manifiesta, y su análisis permite priorizar las contramedidas.

## Dimensiones del riesgo en el contexto móvil. Una taxonomía aplicada

Para una evaluación práctica, es útil desagregar el riesgo informático en dimensiones operativas, tal como lo propone Téllez (2008). La primera dimensión, los riesgos provenientes del equipo, adquiere una nueva complejidad en dispositivos móviles. La "pérdida o cambio de mensajes" durante la transmisión (Téllez, 2008, p. 160) es hoy un riesgo crítico en comunicaciones sensibles vía apps de mensajería. La "interrupción" del servicio (Téllez, 2008, p. 160) puede deberse a ataques de denegación de servicio dirigidos a servicios en la nube de los que depende el dispositivo, o al agotamiento malicioso de la batería mediante software. La "falta de respaldo" (Téllez, 2008, p. 160) es una vulnerabilidad endémica entre usuarios móviles, que confían en la nube pero

no siempre configuran las copias de seguridad correctamente. Las "fallas de origen del equipo" (Téllez, 2008, p. 160) incluyen no solo defectos de fabricación, sino también vulnerabilidades a nivel de firmware o en componentes de hardware como el módem baseband, que pueden ser explotadas para obtener acceso profundo al sistema.

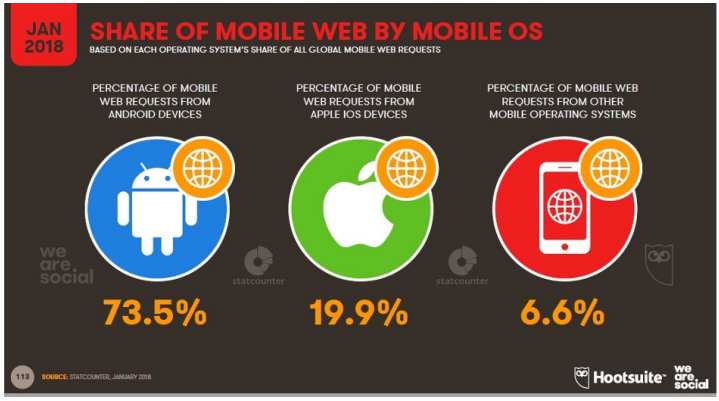
La segunda dimensión, los riesgos provenientes de los programas, es quizás la más dinámica en el ecosistema móvil. El "fraude o desfalco" (Téllez, 2008, p. 161) se ejecuta a través de apps falsas de bancos o comercios en tiendas oficiales, un problema persistente a pesar de los esfuerzos de Google y Apple. El "robo de programas" (Téllez, 2008, p. 161) se traduce en la piratería de apps, que a menudo distribuye versiones modificadas con malware. La "falta de posibilidad de recuperación" (Téllez, 2008, p. 161) es evidente cuando una app crítica pierde datos locales sin sincronización. Las "modificaciones no autorizadas" y la "alteración de secuencias" (Téllez, 2008, p. 161) son riesgos en apps que manejan transacciones o datos sensibles sin integridad criptográfica. La "deficiente validación de datos" (Téllez, 2008, p. 161) en apps móviles puede llevar a vulnerabilidades como inyección SQL móvil o cross-site scripting. La "falta de comprobación intermedia" (Téllez, 2008, p. 161) en procesos transaccionales puede permitir fraudes. Un ejemplo concreto es el estudio de Rojas (2016), que encontró debilidades de seguridad en aplicaciones bancarias chilenas, evidenciando cómo riesgos teóricos se materializan en software real usado por miles de personas.

La tercera dimensión, los riesgos relacionados con los trabajos, se extiende al uso del dispositivo móvil para fines laborales o profesionales (Bring Your Own Device–BYOD). Los "riesgos en los proyectos informáticos" (Téllez, 2008, p. 162) pueden magnificarse si se usan dispositivos no gestionados para acceder a entornos de desarrollo. Los "riesgos contra los datos" (Téllez, 2008, p. 162) son exacerbados cuando datos corporativos se almacenan o transmiten desde un dispositivo personal. La "provocación accidental o intencionada de errores" (Téllez, 2008, p. 162) por parte de un empleado usando su móvil para trabajar es un peligro constante. El "acceso indebido a los sistemas" (Téllez, 2008, p. 162) puede ocurrir si el dispositivo comprometido tiene credenciales

corporativas almacenadas. Bustelo (s.f.) amplía esta perspectiva al enfatizar los riesgos para la autenticidad, fiabilidad, integridad y usabilidad de los documentos gestionados desde dispositivos móviles (p. 16), un aspecto crucial en entornos regulados.

La cuarta y crucial dimensión son los riesgos respecto de las personas. Téllez (2008) señala acertadamente que la protección debe incorporar "la operación de concientizar en la formación y en el control de la seguridad" (p. 164). En el contexto móvil, el factor humano es determinante. La ingeniería social a través de SMS (smishing) o aplicaciones de mensajería es extremadamente efectiva. La falta de conciencia sobre permisos de apps, los riesgos de las redes Wi-Fi públicas, o la importancia de las actualizaciones, convierte al usuario en un amplificador de vulnerabilidades. Como bien señala Téllez (2008), cada persona "debe de tener conocimiento sobre los reglamentos de las claves de la seguridad" y ser advertida sobre su responsabilidad (p. 164). En un entorno educativo como una institución en formación profesional técnica superior, donde se forman futuros desarrolladores, esta dimensión es doblemente importante: se deben mitigar los riesgos a los que están expuestos como usuarios y, simultáneamente, inculcar en ellos los principios de desarrollo seguro que minimicen los riesgos que sus futuras creaciones software podrían introducir.

Figura 3. Digital in 2018




Fuente: Hootsuite (s.f.).

## Del dato a la decisión. El análisis estadístico como herramienta de descubrimiento

La culminación del riguroso proceso de recolección de datos marca el inicio de una fase igualmente crítica: el análisis estadístico, donde los números comienzan a revelar patrones, tendencias y relaciones subyacentes. Para este fin, el estudio empleará el software estadístico especializado SPSS (Statistical Package for the Social Sciences) en su versión 25, una herramienta robusta y ampliamente validada en la comunidad científica para el procesamiento y la interpretación de datos cuantitativos. La ejecución del análisis se estructura en dos etapas secuenciales y complementarias, cada una con un propósito epistemológico distinto. La primera etapa, conocida como análisis descriptivo, tiene una función exploratoria y de contextualización; consiste en aplicar un conjunto de técnicas estadísticas que resumen y describen las características básicas de los datos recolectados de la muestra. Esto implica calcular medidas de tendencia central, como la media (promedio) y la mediana, que indican el punto alrededor del cual se agrupan las respuestas para cada ítem o dimensión. Simultáneamente, se calcularán medidas de dispersión, como la desviación estándar, que cuantifican la variabilidad o heterogeneidad de las respuestas, revelando si las percepciones de los estudiantes son homogéneas o si, por el contrario, existe una amplia divergencia de opiniones y prácticas. Este análisis se complementa con la generación de representaciones gráficas, como tablas de frecuencia absoluta y relativa, e histogramas o gráficos de barras, que ofrecen una visualización inmediata e intuitiva de la distribución de los datos. El poder del análisis descriptivo reside en su capacidad para trazar un perfil detallado y matizado del grupo estudiado, permitiendo comprender, por ejemplo, cuál es el nivel promedio de percepción de riesgo asociado al malware o qué tan dispersas son las prácticas de autenticación entre los futuros desarrolladores, estableciendo así una línea base esencial para interpretar los hallazgos inferenciales posteriores.

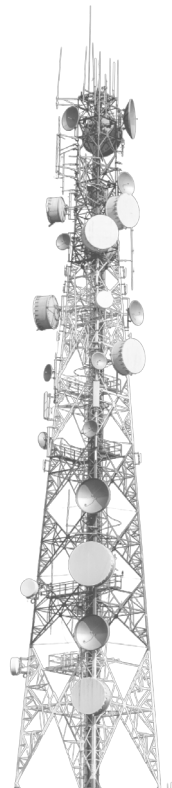
## Descifrando relaciones. La búsqueda de asociaciones significativas

Una vez caracterizada la muestra, la investigación avanza hacia su núcleo inferencial: la prueba de las hipótesis planteadas. Para ello, se recurrirá a una técnica estadística específicamente diseñada para explorar asociaciones: el coeficiente de correlación Rho de Spearman. La elección de esta prueba no paramétrica es estratégica y responde a la naturaleza de los datos obtenidos. A diferencia de su contraparte paramétrica, el coeficiente de Pearson, el Rho de Spearman no exige el supuesto de normalidad en la distribución de los datos y es particularmente adecuado para información medida en escalas ordinales, como la producida por los cuestionarios con escalas Likert de cinco puntos. Su función principal es medir la fuerza y la dirección de una asociación monotónica entre dos variables, es decir, evaluar si, a medida que aumentan los valores de una variable (por ejemplo, la percepción de riesgos provenientes de programas), tienden a aumentar (correlación positiva) o a disminuir (correlación negativa) los valores de la otra variable (por ejemplo, el nivel de seguridad percibido en integridad). El coeficiente Rho produce un valor que oscila entre -1 y +1, donde 0 indica la ausencia de asociación monotónica, los valores cercanos a +1 o -1 señalan una asociación fuerte, y el signo denota la dirección de la relación. Aplicado a este estudio, el análisis correlacional se realizará de manera sistemática, cruzando cada una de las dimensiones de la variable "Riesgos Informáticos" (riesgo de equipo, de programas, relacionado con trabajos y respecto de las personas) con cada uno de los pilares de la variable "Seguridad en Dispositivos Móviles" (confidencialidad, integridad, autenticación, no repudio).

La interpretación decisiva no recae únicamente en el valor del coeficiente Rho, sino en su significancia estadística, comúnmente evaluada a través del valor p (p-value). Este valor indica la probabilidad de que la asociación observada en la muestra se deba al mero azar, en lugar de reflejar una relación real en la población de origen. Siguiendo las convenciones científicas, se establecerá un nivel de significancia (alfa) de 0.05. Por lo tanto, si el valor p asociado a un

coeficiente Rho es menor a 0.05, se concluirá que la correlación es estadísticamente significativa, proporcionando evidencia sólida para aceptar la hipótesis específica que postula dicha relación. Por el contrario, un valor p superior a 0.05 conduciría a no rechazar la hipótesis nula de independencia entre las variables. Este riguroso proceso de contraste es lo que permitirá, de manera objetiva y fundamentada en evidencia numérica, aceptar o rechazar cada una de las hipótesis específicas, así como la hipótesis general que engloba la relación entre ambos constructos. Así, el análisis de datos trasciende la mera descripción para convertirse en un mecanismo de descubrimiento y verificación, cumpliendo el objetivo primordial de determinar la naturaleza, magnitud y significancia de los vínculos entre la exposición a riesgos digitales y la implementación de prácticas de seguridad en el ecosistema móvil de una nueva generación de profesionales de la tecnología.

# CAPÍTULO 2
# LOS PILARES METODOLÓGICOS. CONSTRUYENDO UN PUENTE ENTRE LA TEORÍA Y LA EVIDENCIA EMPÍRICA EN CIBERSEGURIDAD MÓVIL



La ejecución de todo proyecto de investigación exige una fase de clarificación y delimitación conceptual, donde las variables centrales son definidas con precisión tanto en su esencia abstracta como en su manifestación concreta. Este proceso, lejos de ser un mero requisito metodológico, constituye el cimiento sobre el cual se construye la validez interna del estudio. Permite transitar de un plano teórico, cargado de constructos y definiciones amplias, a un plano empírico y observable, donde las ideas se traducen en indicadores medibles. La labor realizada en este proyecto se orientó precisamente a ese fin: validar y articular el marco teórico mediante la descripción exhaustiva de las variables estudiadas, sus dimensiones constitutivas y los indicadores que permitirían su evaluación. Este esfuerzo de operacionalización es fundamental, ya que establece un puente inequívoco entre las preguntas de investigación y los datos que se recolectarán para responderlas, asegurando que lo que se pretende medir se corresponda fielmente con lo que conceptualmente se ha definido (Téllez, 2008).

Las variables identificadas como núcleo del análisis son dos, cada una representando un eje crítico en el ecosistema tecnológico contemporáneo. A continuación, se presentan y definen estas variables, recopiladas y sintetizadas a partir de la literatura especializada. La primera variable, "riesgos informáticos", aborda las amenazas inherentes al uso de sistemas digitales. La segunda, "seguridad en dispositivos móviles", se enfoca en los mecanismos y estados de protección específicos de la tecnología portátil. Su examen conjunto permite una comprensión holística de los desafíos de seguridad en un contexto de alta penetración de dispositivos inteligentes y conectividad permanente, un escenario particularmente relevante para profesionales en formación dentro del campo del desarrollo de software.

## Desentrañando la naturaleza del riesgo en entornos digitales

La primera variable, riesgos informáticos, requiere una comprensión profunda que vaya más allá de la percepción común de "algo que puede salir mal". Conceptualizar el riesgo en el ámbito digital implica reconocerlo como

un producto de la interacción entre vulnerabilidades técnicas, humanas y procedimentales. Según la definición canónica proporcionada por Téllez (2008), el riesgo informático se representa como "la incertidumbre o posibilidad de que suceda o se ejecute una casualidad, la cual podría estar pronosticada; en este sentido, que es permitido decir que la palabra riesgo es la posibilidad de que ocurra un daño" (p. 158). Esta conceptualización subraya dos elementos clave: la incertidumbre (el evento no es determinista) y el daño potencial (la consecuencia negativa material o inmaterial). No se trata simplemente de la existencia de una amenaza, como un virus informático, sino de la probabilidad de que esa amenaza encuentre y explote una vulnerabilidad, materializándose en un perjuicio.

Para operacionalizar esta variable multidimensional, es imperativo desagregarla en dimensiones manejables y observables. En este estudio, la variable "riesgos informáticos" se define operacionalmente a través de cuatro dimensiones principales: 1) Riesgo proveniente del equipo (hardware), que incluye fallas físicas, obsolescencia, robo o daño del dispositivo; 2) Riesgo proveniente de los programas (software), abarcando la presencia de malware (virus, ransomware, spyware), explotación de bugs, uso de software ilegítimo o desactualizado; 3) Riesgo relacionado con los trabajos, referido a la pérdida, corrupción o acceso no autorizado a los datos y productos del trabajo académico o profesional (código fuente, documentos, bases de datos); y 4) Riesgo respecto de las personas, que comprende los factores humanos como la ingeniería social (phishing), prácticas de contraseñas débiles, falta de capacitación o negligencia en el manejo de la información. La medición de estas dimensiones se realizará utilizando datos recolectados directamente de los estudiantes de la carrera de Desarrollo de Software, a través de instrumentos diseñados para evaluar su percepción, conocimiento y experiencias frente a cada una de estas categorías de riesgo.

## La seguridad móvil. Un paradigma de protección en evolución

La segunda variable, seguridad en dispositivos móviles, introduce un campo de estudio dinámico y complejo, dado el papel central que estos artefactos tienen en la vida personal y profesional. La definición conceptual ofrecida por Domingo (2011) enfatiza su naturaleza procesal y multifacética: "Cuando mencionamos la palabra seguridad es determina una lista de elementos necesario para la identificación de los niveles de protección que se está utilizando. Se tomará como modelo los distintos pasos que se tienen que ejecutar durante el proceso de una llamada telefónica conectado inalámbricamente a una red" (p. 7). Esta perspectiva es invaluable, pues en lugar de reducir la seguridad a un producto (como un antivirus), la presenta como un estado resultante de una serie de elementos y protocolos interconectados. El ejemplo de la llamada telefónica ilustra perfectamente cómo la protección debe estar integrada en cada etapa: desde la autenticación en la red, el cifrado de la comunicación, la seguridad del dispositivo que origina y recibe la llamada, hasta las políticas de la red operadora.

Operacionalizar esta variable exige, por tanto, trasladar esa "lista de elementos necesarios" a indicadores concretos. Podrían considerarse dimensiones como: seguridad en el almacenamiento (uso de cifrado del dispositivo, gestión segura de credenciales), seguridad en las comunicaciones (uso de redes Wi-Fi públicas, configuración de Bluetooth, empleo de aplicaciones de mensajería con cifrado de extremo a extremo), seguridad en la gestión de aplicaciones (hábitos de descarga desde tiendas oficiales, revisión de permisos, actualizaciones), y conciencia y prácticas del usuario (activación de bloqueo de pantalla, realización de copias de seguridad, conocimiento sobre phishing móvil). Al igual que con la variable anterior, la medición de estas dimensiones se fundamentará en los datos proporcionados por la población objetivo: los estudiantes de desarrollo de software, cuyo contacto diario con estos dispositivos y su perfil técnico los convierten en sujetos de estudio idóneos para evaluar tanto las prácticas reales como la percepción de seguridad en este

entorno. La integración del análisis de ambas variables ofrecerá una visión completa del panorama de amenazas y defensas en el ecosistema digital que estos futuros profesionales están llamados a desarrollar y, a la vez, a proteger.

Tabla 1. Operacionalización de variable Riesgo Informático

| Dimensiones | Indicadores | ítems | Escala de mediciones y valores | Niveles y rangos |
|---|---|---|---|---|
| Riesgos Provenientes del Equipos | Nivel de riesgo en resguardo de información | 1 | | (Alto) |
| | | 2 | 1 = Nunca | 21 |
| | Nivel de riesgo sin protección de seguridad | 3 | | - |
| | | 4 | 2 = A veces | 49 |
| Riesgos Provenientes de los programas | Nivel de riesgo en aplicaciones de fuentes desconocida | 5 | | |
| | | 6 | 3 = Algunas veces | (Medio) |
| | | 7 | | 50 |
| | Nivel de riesgo sin protección de Antivirus | 8 | 4 = Casi siempre | - |
| | | 9 | | 78 |
| | Nivel de riesgo en aplicaciones de tiendas no oficiales | 10 | 5 = Siempre | |
| | | 11 | | (Bajo) |
| Riesgos relacionados con los trabajos | Nivel de riesgo en almacenamiento de Información | 12 | | 79 |
| | | 13 | | - |
| | | 14 | | 105 |

| Dimensiones | Indicadores | ítems | Escala de mediciones y valores | Niveles y rangos |
|---|---|---|---|---|
| | Nivel de riesgo en almacenamiento de Memoria | 15 | | |
| | Nivel de riesgo en activación firewall | 16 | | |
| | Nivel de riesgo en conexiones a redes externa e internas | 17 | | |
| | | 18 | | |
| Riesgo respecto de las personas | Nivel de riesgo en las Política de seguridad | 19 | | |
| | | 20 | | |
| | Nivel de riesgo en protecciones de recomendaciones de seguridad | 21 | | |

Fuente: Tiznado Ubillus (2019).

## Operacionalizando la defensa. Dimensiones cuantificables de la seguridad móvil

La operacionalización de la variable seguridad en dispositivo móvil se establece mediante cuatro dimensiones fundamentales que materializan su definición conceptual: confidencialidad, integridad, autenticación y no repudio. La medición de la confidencialidad se centrará en evaluar prácticas como el uso de cifrado de almacenamiento y la gestión restrictiva de permisos de aplicaciones, asegurando que solo usuarios autorizados accedan a la información. La integridad será evaluada a través de hábitos relacionados con la procedencia del software instalado y la regularidad en la aplicación de actualizaciones de seguridad, prácticas que garantizan que los datos y sistemas no sean alterados de manera no autorizada. La dimensión de autenticación se medirá analizando los métodos de desbloqueo del dispositivo y el uso de

mecanismos de verificación de identidad robustos. Finalmente, el no repudio se operacionalizará mediante la identificación del uso de firmas digitales o certificados en aplicaciones de comunicación y transacciones, lo que busca garantizar la trazabilidad e irrevocabilidad de las acciones realizadas. La recolección de datos para estas dimensiones se realizará directamente entre los estudiantes de la carrera de desarrollo de software, quienes, debido a su perfil técnico, constituyen una población idónea para analizar las brechas entre el conocimiento teórico y las prácticas de seguridad aplicadas en su entorno tecnológico inmediato (Domingo, 2011).

Esta aproximación operacional permite trascender la mera definición conceptual y establecer un puente claro hacia la evaluación empírica, conectando directamente con la primera variable del estudio. Mientras la variable de riesgos informáticos (Téllez, 2008) identifica y categoriza las amenazas y vulnerabilidades latentes en el ecosistema digital, la variable de seguridad en dispositivos móviles se enfoca en el estado concreto de las defensas y protocolos diseñados para mitigar dichos riesgos específicamente en plataformas portátiles. La medición conjunta de ambas variables, a través de la misma población de estudiantes, posibilitará un análisis integral que no solo catalogue las amenazas percibidas, sino que también evalúe la efectividad y aplicación real de los controles de seguridad, ofreciendo así una visión dialéctica completa del panorama de ciberseguridad desde la perspectiva del futuro profesional del software.

Tabla 2. Matriz de Operacionalización de variable seguridad en dispositivo móvil

| **Dimensiones** | **Indicadores** | **Ítems** | **Escala de mediciones y valores** | **Niveles y rangos** |
|---|---|---|---|---|
| Confidencialidad | Nivel de seguridad en la protección de tu Información | 1 | | (Bajo) |
| | | 2 | 1 = Nunca | 17 |
| | | 3 | | - |

| Dimensiones | Indicadores | Ítems | Escala de mediciones y valores | Niveles y rangos |
|---|---|---|---|---|
| | Nivel de seguridad en los accesos de comunicaciones Seguras | 4 | 2 = A veces | 39 |
| | Nivel de seguridad en la confiabilidad a la nube | 5 | | (Medio) |
| | | 6 | 3 = Algunas veces | 40 |
| Integridad | Nivel de seguridad en sistema operativo | 7 | | - |
| | Nivel de seguridad en los certificados digitales | 8 | 4 = Casi siempre | 62 |
| | Nivel de permiso de seguridad | 9 | | (Alto) |
| | | 10 | 5 = Siempre | 63 |
| Autenticación | Nivel de acceso en las claves de seguridad | 11 | | - |
| | | 12 | | 85 |
| | | 13 | | |
| | | 14 | | |
| No repudio | Nivel de seguridad en firma digital | 15 | | |
| | Nivel de seguridad en enviar y compartir documentos | 16 | | |
| | | 17 | | |

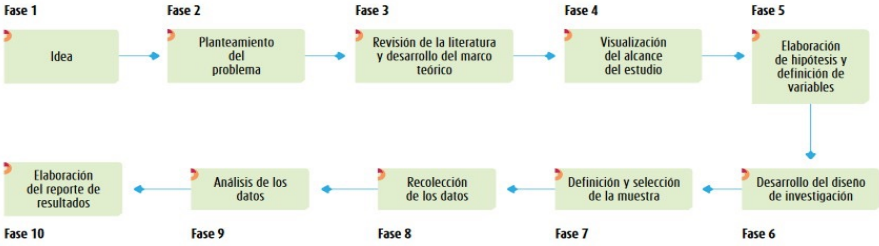
Fuente: Tiznado Ubillus (2019).

## La arquitectura metodológica. Un marco para la construcción de conocimiento

El diseño metodológico de una investigación constituye la columna vertebral intelectual que estructura toda la indagación, guiando al investigador desde la formulación de preguntas hasta la interpretación de los hallazgos.

Bernal (2010) conceptualiza este proceso, en su forma deductiva, como un camino que "reside en un proceso que inicia de unas aseveración en calidad de hipótesis y busca contradecir o mentir tales hipótesis, derivando de ellas terminaciones que deben comprobar con hechos reales" (p. 60). Esta descripción subraya la naturaleza rigurosa y contrastable del método científico, donde las proposiciones teóricas iniciales no se aceptan dogmáticamente, sino que se someten al escrutinio de la evidencia empírica. Por consiguiente, la metodología funciona como el instrumento rector que permite orientar los objetivos del estudio, operativizando las hipótesis para evaluar su validez frente a la realidad observada. Su función es fundamental para comparar, afirmar o refutar los elementos de la problemática planteada, canalizando la resolución de interrogantes a través de la recolección y análisis sistemático de datos. Para visualizar este proceso integral, resulta ilustrativo el modelo propuesto por Hernández et al. (2014), quienes desglosan la metodología para el enfoque cuantitativo en un esquema de fases sucesivas e interconectadas. Este marco, lejos de ser una mera secuencia administrativa, proporciona un mapa de navegación que garantiza la claridad en la determinación de los objetivos, la articulación coherente de las variables y la vinculación lógica entre las hipótesis iniciales y las conclusiones finales, transformando así los problemas de investigación en resultados sustentados por el análisis estadístico y la interpretación teórica.

Figura 4. Metodología para enfoque cuantitativo




Fuente: Hernández et al. (2014, p. 5).

## La búsqueda del conocimiento puro. Fundamentos de la investigación básica

La naturaleza del presente estudio se enmarca dentro del ámbito de la investigación básica, también denominada teórica, pura o fundamental. Valderrama (2013) la define como aquella que "está destinada a aportar un cuerpo organizado de conocimientos científicos y no produce necesariamente resultados de utilidad práctica inmediata. Se preocupa por recoger información de la realidad para enriquecer el conocimiento teórico, científico, orientado al descubrimiento de principios y leyes" (p. 164). Esta caracterización destaca su vocación primordial por la expansión del entendimiento abstracto y la formulación de teorías, más que por la solución aplicada de problemas concretos en un contexto específico. En sintonía con esta perspectiva, Muños (2014) sostiene que la investigación básica "pretende generar conocimiento científico sobre distintos hechos que interesan a las ciencias particulares o a la filosofía sin buscar lucro o utilidad alguna, salvo la difusión del conocimiento por el propio conocimiento" (p. 26). La convergencia en los planteamientos de ambos autores subraya el carácter desinteresado y fundamentador de este tipo de indagación. Por lo tanto, los métodos científicos empleados en esta investigación que son clasificables como teóricos, puros o fundamentales, están orientados a generar argumentos explícitos y marcos explicativos robustos que permitan comprender en profundidad los objetivos y la problemática central. Este enfoque no prejuzga la obtención de un resultado "positivo" o "negativo" en términos prácticos, sino que valora la contribución al acervo teórico sobre los riesgos informáticos y la seguridad móvil, enriqueciendo así la comprensión de estos fenómenos desde una perspectiva académica y disciplinar.

## Cartografiando el fenómeno. El nivel descriptivo de la investigación

Para lograr el objetivo de comprender y caracterizar el panorama de estudio, esta investigación adopta un nivel descriptivo. Según Danhker (1989,

citado en Hernández et al., 2006), los estudios descriptivos "buscan definir las propiedades, característica y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis" (p. 81). Esta definición enfatiza la función de "cartografía" o "fotografía" de la realidad que cumple este nivel, la cual es esencial antes de intentar explicar causas o predecir comportamientos. En un sentido complementario, Sabino (2006) señala que la investigación descriptiva "se plantea conocer grupos semejantes de fenómenos manejando criterios sistemáticos que accederán poner de manifiesto su estructura o conducta" (p. 40). La conjunción de ambas definiciones destaca dos aspectos metodológicos cruciales: la sistematización en la observación y el propósito de revelar la estructura inherente al fenómeno estudiado. En el contexto de esta tesis, el nivel descriptivo permitirá realizar un estudio detallado de la población conformada por estudiantes de la carrera de Desarrollo de Software. El propósito es caracterizar las manifestaciones, comportamientos, percepciones y prácticas de este grupo homogéneo en relación con las variables de riesgos informáticos y seguridad en dispositivos móviles. La aplicación de un instrumento de recolección de datos diseñado con criterios sistemáticos posibilitará poner de manifiesto la estructura de dichas variables dentro de la población, generando un diagnóstico claro y fundamentado que sirva como punto de partida para análisis posteriores y como contribución al conocimiento del perfil de seguridad digital de los futuros profesionales del sector tecnológico.

## Explorando vínculos. El enfoque correlacional y cuantitativo

El propósito de esta investigación trasciende la mera descripción para adentrarse en la exploración de las relaciones existentes entre sus constructos centrales. Para ello, adopta un enfoque correlacional. Hernández et al. (2010) definen este tipo de estudio como aquel que tiene "como propósito de conocer la relación o grado de agrupación que exista entre 2 o más conceptos, categorías o variables en un argumento en particular" (p. 81). En este caso, el interés se centra específicamente en determinar el grado de asociación es-

tadística entre los niveles percibidos y experimentados de "riesgos informáticos" y las prácticas e implementaciones de "seguridad en dispositivos móviles" entre los estudiantes. Un ejemplo concreto de esta relación podría explorar si una mayor percepción de riesgos asociados al malware (dimensión de software) se correlaciona con una mayor frecuencia de actualizaciones del sistema operativo (dimensión de integridad en la seguridad móvil). Este enfoque permite indagar si ambas variables coexisten de forma independiente o si, por el contrario, covarían, lo cual puede sugerir patrones de comportamiento o conciencia que merezcan un análisis más profundo, sin pretender en esta etapa establecer causalidad.

Para operacionalizar y medir estas relaciones de manera precisa y objetiva, el estudio se sustenta en un enfoque cuantitativo. Hernández et al. (2011) afirman que este enfoque "utilizar la recopilación de datos para probar hipótesis fundadas en mediciones numéricas y análisis estáticos, con la finalidad de implantar pautas de comportamiento y comprobar hipótesis" (p. 4). La elección del paradigma cuantitativo es coherente con la naturaleza de las variables operacionalizadas y con el objetivo correlacional, ya que permite transformar las dimensiones de confidencialidad, integridad, autenticación, percepción de riesgo, entre otras, en escalas numéricas (por ejemplo, escalas Likert). Esta cuantificación posibilita la aplicación de técnicas estadísticas, como el coeficiente de correlación de Pearson o Rho de Spearman, para determinar con rigor la fuerza y dirección de las relaciones postuladas, alejando la interpretación del terreno de la impresión subjetiva para ubicarla en el ámbito de la evidencia matemática.

## El diseño del estudio. Una fotografía analítica no experimental

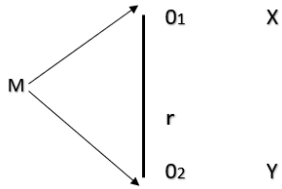
El diseño específico que articula estos elementos metodológicos es no experimental, transeccional y correlacional. Este diseño se caracteriza por basarse en la observación de los fenómenos en su estado natural, sin que el investigador intervenga para manipular o modificar las variables de estudio. Hernández et al. (2014) precisan que en los diseños no experimentales "se trata

de estudios en los que no hacemos variar intencionalmente las variables independientes para ver su efecto sobre otras variables" (p. 152). Esta característica es apropiada para la presente investigación, ya que busca capturar y analizar las percepciones y prácticas existentes en la población, sin asignar tratamientos o formar grupos de control. Dei (2006) refuerza esta idea al señalar que en la investigación no experimental, "los procedimientos más frecuente empleados son la observación y las diversas técnicas de análisis" (p. 66), siendo en este caso la encuesta el instrumento de observación sistemática elegido.

A su vez, el diseño es transeccional, lo que significa que la recolección de datos se realizará en un único momento temporal. Hernández et al. (2014) explican que los diseños transeccionales "recolectan datos en un solo momento (en un tiempo único). Tiene como propósito describir variables y analizar su incidencia e interrelación en un momento dado" (p. 154). Esta "fotografía" o corte temporal es adecuada para cumplir con los objetivos descriptivos y correlacionales planteados, ofreciendo una visión sincrónica de la situación de las variables en la población de estudio durante el período de ejecución de la investigación.

Finalmente, el componente correlacional del diseño se alinea con el propósito declarado de examinar relaciones. Hernández et al. (2014) afirman que los diseños correlacionales "describen relaciones entre dos o más categorías, conceptos o variables en un momento dado. A veces, únicamente en términos correlacionales, otras veces en función de la relación causa efecto (causales)" (p. 157). En este estudio, el esquema operativo se representa conceptualmente en la Figura 5, donde se busca establecer el coeficiente de correlación (r) entre las puntuaciones obtenidas en las dos variables medidas en una misma muestra (M): los Riesgos Informáticos (01) y la Seguridad en los Dispositivos Móviles (02).

Figura 5. Esquema de tipo de diseño.




Fuente: Tiznado Ubillus (2019).

Donde:

M : Muestra de estudio 01 : Riesgos Informáticos

02 : Seguridad en los dispositivos móviles

01 y 02 : Puntuaciones de las variables r: Correlación

Este diseño integral, por tanto, proporciona un marco metodológico robusto y coherente para explorar, describir y relacionar los constructos de interés, permitiendo responder a las preguntas de investigación con un alto grado de rigor científico y aportando una base empírica válida para la discusión y las conclusiones del estudio. La conjunción de estos elementos tales como básico, descriptivo, correlacional, cuantitativo y no experimental transeccional, configura una estrategia de indagación que equilibra la profundidad teórica con el análisis sistemático de la realidad observada en la población objetivo.

## Definiendo el campo de estudio. Población, muestra y estrategia de acceso

La sección metodológica de toda investigación empírica requiere una definición precisa de los sujetos o elementos sobre los cuales recaerá la indagación, así como de la estrategia para seleccionarlos y acceder a ellos. Este proceso, que abarca la identificación de la población, el cálculo de la muestra y la elección de la técnica de muestreo, es fundamental para garantizar que los hallazgos del estudio posean validez externa, es decir, que puedan gene-

ralizarse de manera justificada más allá del grupo inmediatamente analizado. Se procederá, por tanto, a argumentar y detallar cada uno de estos elementos constitutivos del diseño muestral de la presente tesis. La claridad en esta etapa no es un mero formalismo, sino una condición indispensable para evaluar la solvencia de las inferencias que se realizarán a partir de los datos recolectados, estableciendo los límites y el alcance de las conclusiones que se deriven del proceso investigativo.

## Población. El universo de interés conceptual

El punto de partida de cualquier diseño muestral es la delimitación conceptual y operativa de la población de estudio. Arias (2012) se refiere a la población como el "conjunto limitado o no ilimitado de varios elementos que se define con características frecuentes en las cuales se podrán ser extensiva en sus conclusiones. Esta conforma por un finito por el de los problemas y sus objetivos de la investigación" (p. 81). Esta definición destaca dos aspectos cruciales: primero, que la población está compuesta por elementos que comparten características comunes relevantes para los objetivos de estudio; y segundo, que es a este conjunto al que idealmente se desea extrapolar o extender los resultados. En el presente estudio, la población objetivo está claramente definida y delimitada: todos los estudiantes activos de la carrera de Desarrollo de Software de una institución en formación profesional técnica superior, durante el ciclo académico en el que se realiza la investigación. Para efectos de organización y posible análisis estratificado, esta población se encuentra distribuida en los semestres 2, 5 y 6 de la malla curricular. La distribución concreta de los estudiantes por semestre se presenta en la Tabla 3, la cual ofrece una visión detallada de la composición del universo de estudio y sirve como base para los subsiguientes cálculos muestrales.

Tabla 3. Distribución de estudiantes por Semestre.

| Semestre | Cantidad de estudiantes. |
|---|---|
| 2 Sem. | 30 |
| 5 Sem. | 19 |
| 6 Sem. | 17 |
| Total | 66 |

Fuente: Tiznado Ubillus (2019).

## Muestra y muestreo. La porción accesible y representativa

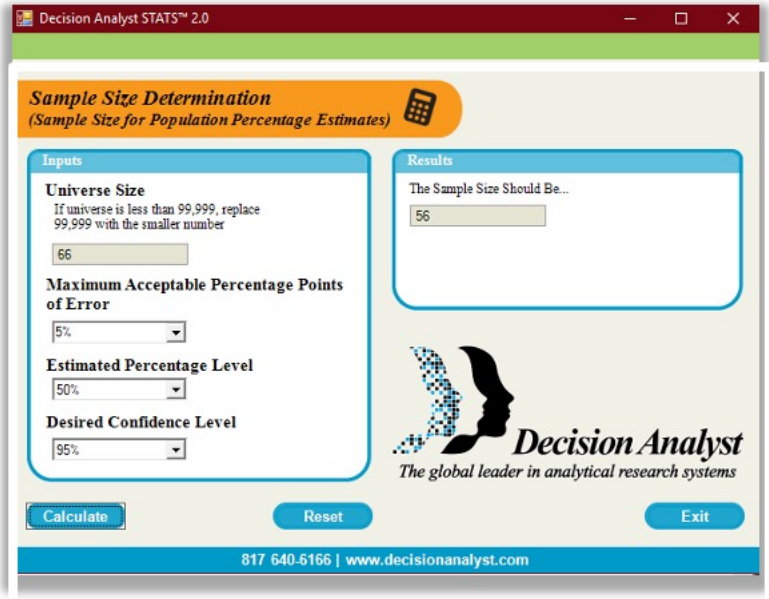
Dada la factibilidad logística y temporal, es común en la investigación social y educativa trabajar no con la población completa (censo), sino con una porción representativa de la misma, denominada muestra. Behar (2008) define la muestra como un "subgrupo de la población. Se le llamada subconjunto a los elementos que lo relaciona con el conjunto, conceptualizado a las necesidades denominado población" (p. 51). Complementariamente, Arias (2012) argumenta que la muestra "es la representación del subconjunto en un esta concreto que se utiliza de la población en un estado accesible" (p. 83). La conjunción de estas definiciones subraya la dualidad de la muestra: es un subconjunto extraído de la población, pero su valor radica en su capacidad de representar a dicha población, permitiendo que las conclusiones obtenidas a partir de ella sean inferibles al conjunto mayor, siempre que se haya seguido un procedimiento de selección adecuado.

El proceso mediante el cual se selecciona esta muestra se denomina muestreo. Para determinar el tamaño óptimo de la muestra se recurre a fórmulas estadísticas que balancean la precisión deseada, el nivel de confianza y la variabilidad esperada en la población. Tamayo (1990, citado en Valderrama, 2013) aclara que "el tamaño de la muestra podrá ser seleccionada por la subpoblación de los cuales se obtendrán los resultados de los datos para luego pueda comprobarse sobre lo verdadero o lo falso todo orientado a la hipóte-

sis en un proceso de extraer e interpretar la deducción sobre el estudio de la población" (p. 188). En este estudio, si bien inicialmente se contempló aplicar el instrumento a los 66 estudiantes que conforman la población accesible, se procedió a realizar un cálculo estadístico más riguroso para optimizar recursos sin comprometer la validez.

| Tamaño de la muestra | Precisión Error máximo aceptable | Porcentaje de estimación | Nivel de confianza |
|---|---|---|---|
| 66 estudiantes | 5% | 50% | 95% |

Figura 6. Total del tamaño de la población




Fuente: analista de decisiones STATS™ 2.0

Por consiguiente, la nueva muestra representativa estará conformada por 56 estudiantes de la carrera de Desarrollo de Software de una institución en formación profesional técnica superior, seleccionados mediante un muestreo probabilístico aleatorio simple desde el listado total de la población. Este método asegura que cada estudiante tenga una probabilidad conocida y

distinta de cero de ser seleccionado, minimizando los sesgos de selección y maximizando la representatividad de la muestra final.

## Herramientas de indagación. Técnicas e instrumentos para la recolección de datos

Una vez definido el quién (la muestra), es esencial especificar el cómo se obtendrá la información de dichos sujetos. Esto implica la elección de una técnica de recolección y el diseño de un instrumento específico que sea válido y confiable.

### *Técnica. La encuesta como ventana a las percepciones y prácticas*

Para el presente estudio, la técnica seleccionada es la encuesta por cuestionario. Esta técnica es ampliamente utilizada en investigaciones de corte cuantitativo y descriptivo-correlacional, ya que permite recopilar datos estandarizados de una muestra numerosa de manera eficiente, facilitando posteriormente la comparación y el análisis estadístico. La encuesta se aplicará de manera individual a cada uno de los 56 estudiantes que conforman la muestra final, garantizando la confidencialidad de sus respuestas. Su fortaleza reside en la capacidad de cuantificar percepciones, actitudes, conocimientos y reportes de comportamiento sobre las variables de estudio; riesgos informáticos y seguridad en dispositivos móviles, transformando constructos complejos en datos numéricos manejables.

### *Instrumento. El cuestionario y su arquitectura de medición*

El instrumento concreto que operacionalizará la técnica de la encuesta es un cuestionario estructurado. Este cuestionario, cuyo beneficio para la investigación radica en la estandarización del proceso de recolección, está

compuesto por ítems organizados en dos secciones principales, cada una correspondiente a una de las variables de estudio. Cada pregunta es politómica y ofrece cinco alternativas de respuesta que se corresponden con una escala tipo Likert. Esta escala, que típicamente va desde "Muy en desacuerdo" o "Nunca" (1) hasta "Muy de acuerdo" o "Siempre" (5), permite capturar la intensidad o frecuencia de las percepciones y prácticas de los encuestados, yendo más allá de una mera opción dicotómica (sí/no). La asignación de valores numéricos a cada alternativa es lo que posibilita el "guardado de la data" para su posterior procesamiento estadístico. La estructura detallada del instrumento, incluyendo los ítems correspondientes a cada dimensión de las variables, se presenta en las Tablas 4 y 5, las cuales ofrecen una visión clara de la ficha técnica aplicada.

Tabla 4. Ficha de instrumento – v1 riesgo informático

| | |
|---|---|
| Nombre original | Cuestionario Riesgo Informático |
| Autor | Br. Jose Armando Tiznado Ubillus |
| Año | 2019 |
| Procedencia | Lima – Perú |
| Tipo de Instrumento | Cuestionario |
| Objetivo | Recolectar información para determinar la relación entre los Riesgo Informático en una institución en formación profesional técnica superior |
| Estudiantes | Individual |
| Aplicación | Directa |
| Estructura | El instrumento consta de 21 ítems distribuidos con alternativas:<br>1: Nunca<br>2: Casi nunca<br>3: Intermedio<br>4: Casi siempre<br>5: Siempre |

Fuente: Tiznado Ubillus (2019).

Tabla 5. Ficha de instrumento – v2 Seguridad en dispositivo Móvil

| | |
|---|---|
| Nombre original | Cuestionario Seguridad en dispositivo Movil |
| Autor | Br. José Armando Tiznado Ubillus |
| Año | 2019 |
| Procedencia | Lima – Perú |
| Tipo de Instrumento | Cuestionario |
| Objetivo | Recolectar información para determinar la relación entre los Riesgo Informático en una institución en formación profesional técnica superior |
| Estudiantes | Individual |
| Aplicación | Directa |
| Estructura | El instrumento consta de 17 ítems distribuidos con alternativas:<br>1: Nunca<br>2: Casi nunca<br>3: Intermedio<br>4: Casi siempre<br>5: Siempre |

Fuente: Tiznado Ubillus (2019).

## Garantías de calidad metodológica. Validez y confiabilidad del instrumento

La utilidad de cualquier instrumento de medición depende de su capacidad para medir con exactitud (validez) y consistencia (confiabilidad) aquello que pretende medir. Sin estas propiedades psicométricas, los datos recolectados carecen de solidez interpretativa.

### *Validez. El juicio de expertos como aval de pertinencia*

Para determinar la validez de contenido del cuestionario —es decir, el grado en que sus ítems representan adecuadamente el dominio completo de

cada constructo— se recurrió a un juicio de expertos. Este procedimiento consistió en someter el instrumento a la evaluación crítica de especialistas en el área de ciberseguridad, metodología de la investigación y tecnología educativa. Estos especialistas, cuyos perfiles se detallan en la Tabla 6, evaluaron cada ítem en función de tres criterios fundamentales: (1) Claridad (si la redacción es comprensible y no ambigua), (2) Pertinencia (si el ítem mide efectivamente la dimensión a la que se asigna), y (3) Relevancia (si el ítem es importante para la evaluación del constructo). La concordancia positiva entre los expertos en estos aspectos constituye un sólido aval de la validez de contenido del instrumento, recomendando su aplicación para los fines de la investigación.

Tabla 6. Especialista para el certificarón de validez.

| DNI | Grado Académico Apellido y Nombre | Institución donde labora | Calificación |
|---|---|---|---|
| 04656793 | Doctor en Ingeniería de Sistema<br>Lezama Gonzales, Pedro Martin | UCV | Aplicable |
| 08404620 | Magister en Estadístico<br>Torres Cabanillas, Luis Alberto | UCV | Aplicable |
| 10530519 | Magister en Gestión Pública y G.<br>Arle Trujillo, Miguel Ángel | UCV | Aplicable |

Fuente: Tiznado Ubillus (2019).

## Confiabilidad. La consistencia interna a través del alfa de cronbach

La confiabilidad, que se refiere a la consistencia o estabilidad de las mediciones del instrumento, se evaluó mediante una prueba piloto. Esta prueba se aplicó a un grupo reducido de 19 estudiantes con características similares a la muestra objetivo, pero que no fueron incluidos en la muestra final. Los datos recolectados en este piloto se analizaron utilizando el coeficiente Alfa de Cronbach en el software SPSS versión 22. Este coeficiente mide la consistencia interna, es decir, el grado en que los ítems de una misma escala están

correlacionados entre sí, midiendo un constructo unidimensional. Los resultados, presentados en la Tabla 7, arrojaron valores de 0.819 para la escala de riesgos informáticos y 0.820 para la escala de seguridad en dispositivos móviles. De acuerdo con los criterios ampliamente aceptados (George & Mallery, 2016), valores de Alfa superiores a 0.70 son considerados "aceptables", y superiores a 0.80 son "buenos". Por lo tanto, se puede concluir que ambas escalas del instrumento poseen una confiabilidad interna satisfactoria para su uso en la investigación principal.

Tabla 7. Estadística de Confiabilidad

| Alfa de Cronbach | Alfa de Cronbach basada en elementos estandarizados | N de elementos |
|---|---|---|
| ,819 | ,820 | 2 |

Fuente: Software SPSS 22.

## Del dato a la interpretación. Métodos de análisis de datos

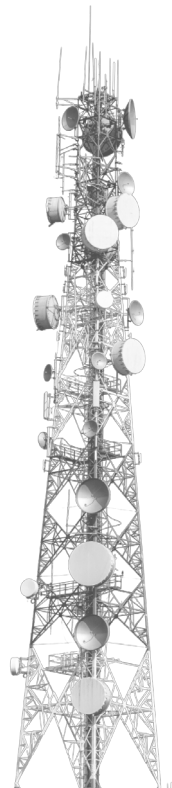
La fase final del proceso metodológico concierne a las estrategias que se emplearán para procesar, sintetizar e interpretar los datos recolectados, con el fin de dar respuesta a los objetivos e hipótesis de investigación.

El análisis se realizará utilizando el programa estadístico SPSS (Statistical Package for the Social Sciences), versión 25. El proceso se gestionará en dos etapas principales. Primero, se ejecutará un análisis descriptivo univariado para cada una de las variables y sus dimensiones. Esta etapa incluirá el cálculo de estadísticos como frecuencias, porcentajes, medias y desviaciones estándar, los cuales se presentarán mediante tablas y gráficos de barras. Este análisis descriptivo tiene como objetivo "retratar" el comportamiento de la muestra en relación con cada ítem y dimensión, permitiendo caracterizar los niveles de percepción de riesgo y las prácticas de seguridad móvil predominantes entre los estudiantes encuestados. La interpretación de estos por-

centajes y tendencias proporcionará la base empírica para describir el estado de las variables, cumpliendo así con el primer nivel de la investigación.

En una segunda etapa, y para abordar el objetivo correlacional del estudio, se aplicará un análisis inferencial bivariado. Dado que las escalas Likert generan datos ordinales y se busca evaluar la relación entre dos variables, la prueba estadística seleccionada es el coeficiente de correlación Rho de Spearman. Esta prueba es no paramétrica y adecuada para datos ordinales, permitiendo determinar la fuerza y dirección de la asociación entre las puntuaciones totales (o por dimensiones) de la variable "riesgos informáticos" y la variable "seguridad en dispositivos móviles". La interpretación del Rho de Spearman, junto con su nivel de significancia estadística (valor p), será fundamental para probar o rechazar la hipótesis general y las hipótesis específicas de la investigación. Un coeficiente positivo y significativo sugeriría que a mayores percepciones de riesgo, se asocian mejores prácticas de seguridad, o viceversa; mientras que un coeficiente no significativo indicaría la ausencia de una relación lineal entre estos constructos en la muestra estudiada. De esta manera, el análisis integra la descripción del panorama con la exploración de las conexiones subyacentes entre los fenómenos investigados.

# CAPÍTULO 3
# DE LA PERCEPCIÓN A LA PRÁCTICA. DESENTRAÑANDO LA RELACIÓN ENTRE CONCIENCIA DEL RIESGO Y COMPORTAMIENTO SEGURO



## Interpretando el panorama. Un retrato descriptivo de los riesgos y la seguridad digital

La presentación de resultados constituye el momento en el que los datos, sometidos a un riguroso procesamiento analítico, se despliegan para ofrecer una respuesta empírica a las interrogantes de la investigación. Esta sección se dedica a exponer los hallazgos derivados del análisis estadístico, comenzando por una exploración descriptiva exhaustiva que permite comprender la distribución y las tendencias predominantes dentro de la muestra estudiada. Los resultados descriptivos funcionan como una cartografía inicial, delineando el perfil de la población en relación con las variables centrales del estudio: los riesgos informáticos y la seguridad en dispositivos móviles. A través de tablas y figuras, se ofrece una visión cuantificada y estructurada de cómo los estudiantes de la carrera de Desarrollo de Software perciben las amenazas del entorno digital y cómo reportan gestionar la protección de sus dispositivos portátiles. Este ejercicio no solo cumple con el objetivo de caracterizar el estado actual de estos fenómenos, sino que también establece la base factual necesaria para las posteriores interpretaciones correlacionales, permitiendo contextualizar las relaciones dentro de un marco de referencia claro sobre los niveles de riesgo y seguridad predominantes.

### El panorama general. Niveles de riesgo informático y seguridad móvil

El análisis descriptivo de la Variable 1: Riesgos Informáticos en su conjunto revela una percepción moderada-alta entre los estudiantes encuestados. Como se detalla en la Tabla 8, la distribución de los niveles de percepción global de riesgo muestra que el 46% de los participantes se ubica en un nivel medio, indicando una conciencia generalizada pero no alarmante sobre las diversas amenazas digitales. Un 30% reporta un nivel alto de percepción, lo que sugiere que una porción significativa del alumnado se siente particularmente vulnerable o está muy al tanto de los peligros existentes.

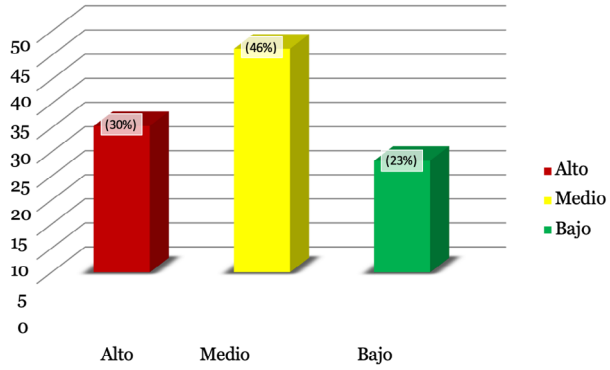
Tabla 8. Descripción de los Riesgos Informático

| Variable 1: Riesgos Informático | | | | |
|---|---|---|---|---|
| | | Frecuencia | Porcentaje | Porcentaje válido |
| Válido | Alto | 17 | (30.4%) | (30.4%) |
| | Medio | 26 | (46.4%) | (46.4%) |
| | Bajo | 13 | (23.2%) | (23.2%) |
| Total | | 56 | (100.0%) | (100.0%) |

Fuente: Tiznado Ubillus (2019), ejecutado por el SPSS Versión 25

En contraste, un 23% manifiesta un nivel bajo, grupo que posiblemente subestima los riesgos o considera que las medidas de seguridad básicas son suficientes. Esta distribución, que puede visualizarse de manera más intuitiva en la Figura 7, presenta un perfil donde la percepción de riesgo no es homogeneamente baja, sino que existe un gradiente de conciencia que justifica la investigación. El hallazgo de que casi un tercio de la muestra se sitúa en un nivel alto es especialmente relevante, pues indica que los temas de ciberseguridad resuenan con fuerza en una parte considerable de los futuros desarrolladores, posiblemente debido a su exposición técnica o a experiencias previas con incidentes de seguridad.

Figura 7. Descripción en porcentaje de los Riesgos Informáticos



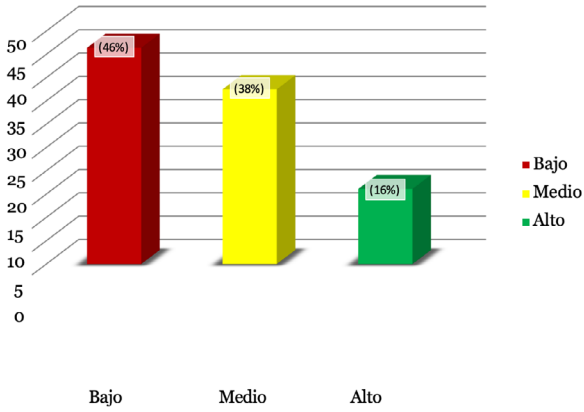

Fuente: Tiznado Ubillus (2019).

En cuanto a la **Variable 2:** Seguridad en Dispositivos Móviles, los resultados generales, presentados en la Tabla 9, arrojan un panorama ligeramente más positivo pero con áreas de preocupación. El 46% de los estudiantes reporta un nivel alto de prácticas de seguridad, lo que es alentador y sugiere que casi la mitad del grupo implementa medidas de protección consistentes en sus dispositivos. Un 38% se ubica en un nivel medio, indicando la aplicación de algunas prácticas básicas pero con posibles omisiones en aspectos más avanzados. Sin embargo, un 16% aún se encuentra en un nivel bajo, lo que representa una brecha de seguridad significativa dentro de una población que, por su formación, se esperaría más consciente. La Figura 8 ilustra esta distribución, destacando visualmente que mientras la mayoría se agrupa en los niveles medio y alto, existe una minoría no despreciable cuyas prácticas podrían hacerlos particularmente vulnerables. Este dato es crucial, ya que evidencia que el conocimiento técnico sobre desarrollo de software no se traduce automáticamente en comportamientos seguros en el uso personal de la tecnología, una disociación que ha sido observada en otros estudios con poblaciones de TI (Hadlington, 2017).

Tabla 9. Descripción de la Seguridad en los dispositivos Móvil

| **Variable 2: Seguridad en Dispositivo Móvil** | | | | | |
|---|---|---|---|---|---|
| | | **Frecuencia** | **Porcentaje** | **Porcentaje válido** | **Porcentaje acumulado** |
| Valido | Bajo | 26 | (46.4%) | (46.4%) | (46.4%) |
| | Medio | 21 | (37.5%) | (37.5%) | (83.9%) |
| | Alto | 9 | (16.1%) | (16.1%) | (100.0%) |
| Total | | 56 | (100.0%) | (100.0%) | |

Fuente: Tiznado Ubillus (2019), ejecutado por el SPSS Versión 25




Fuente: Tiznado Ubillus (2019).

## Desglosando la amenaza. Percepción de riesgo por dimensiones específicas

Para comprender con mayor profundidad qué tipos específicos de riesgos generan mayor preocupación, es necesario analizar los resultados por cada una de las dimensiones operacionalizadas de la variable de riesgos informáticos. Este desglose revela matices importantes que el puntaje general puede ocultar.

**La Dimensión 1:** Riesgos Provenientes del Equipo (Hardware), cuyos datos se muestran en la Tabla 10, presenta una distribución casi tripartita. Un 36% de los estudiantes percibe un nivel alto de riesgo asociado a fallas físicas, robo, daño u obsolescencia de sus dispositivos. Un 32% lo sitúa en nivel medio y otro 32% en nivel bajo. Como se aprecia en la Figura 9, esta es la dimensión donde la percepción de riesgo alto alcanza su mayor porcentaje entre las cuatro analizadas. Esto podría deberse a la tangibilidad de la amenaza: la pérdida física o el mal funcionamiento del dispositivo son eventos concretos y costosos, fácilmente imaginables para los usuarios, a diferencia de amenazas de software más abstractas. Este resultado resalta la importancia de incluir

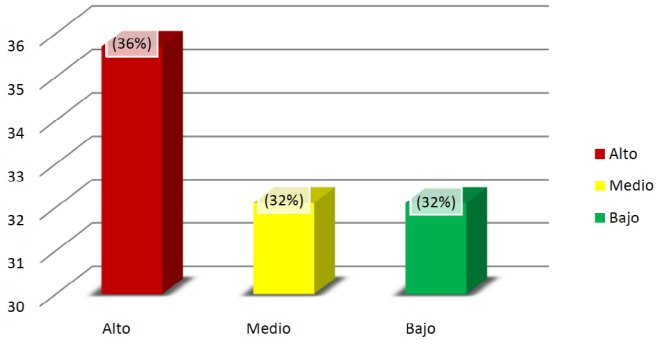
políticas de respaldo y cifrado en la formación en ciberseguridad, ya que la protección de los datos ante un incidente físico es una preocupación latente.

Tabla 10. Descripción de los Riesgos proveniente del equipo

| **Dimensión 1: Riesgos proveniente del equipo** | | | | | |
|---|---|---|---|---|---|
| | | **Frecuencia** | **Porcentaje** | **Porcentaje válido** | **Porcentaje acumulado** |
| Valido | Alto | 20 | (35.7%) | (35.7%) | (35.7%) |
| | Medio | 18 | (32.1%) | (32.1%) | (67.9%) |
| | Bajo | 18 | (32.1%) | (32.1%) | (100.0%) |
| Total | | 56 | (100%) | (100%) | |

Fuente: Tiznado Ubillus (2019), ejecutado por el SPSS Versión 25

Figura 9. Descripción en porcentaje de los Riesgos proveniente de los equipos.




Fuente: Tiznado Ubillus (2019).

La Dimensión 2: Riesgos Provenientes de los Programas (Software), detallada en la Tabla 11, exhibe un patrón distinto. Aquí, la percepción predominante se concentra abrumadoramente en el nivel medio, con un 59% de las respuestas. Solo un 14% considera el riesgo como alto, y un 27% como bajo. La Figura 10 grafica claramente esta concentración en la categoría central. Este

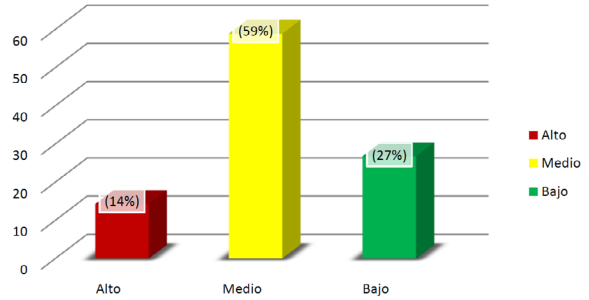
hallazgo es particularmente interesante, pues contrasta con la prevalencia real de amenazas de software como el malware, el phishing y la explotación de vulnerabilidades, que son de las más comunes en el panorama digital actual. La relativamente baja percepción de alto riesgo (14%) podría indicar una falsa sensación de seguridad proporcionada por herramientas como antivirus, o una subestimación de la sofisticación de los ataques modernos. Sugiere que, aunque los estudiantes reconocen la existencia de estos riesgos (de ahí el alto porcentaje en nivel medio), no los perciben como una amenaza inminente o de alto impacto personal, un sesgo cognitivo que podría dejarlos expuestos.

Tabla 11. Descripción de los Riesgos proveniente de los programas.

| **Dimensión 2: Riesgos proveniente de los programas** | | | | | |
|---|---|---|---|---|---|
| | | **Frecuencia** | **Porcentaje** | **Porcentaje válido** | **Porcentaje acumulado** |
| Valido | Alto | 8 | (14.3%) | (14.3%) | (14.3%) |
| | Medio | 33 | (58.9%) | (58.9%) | (73.2%) |
| | Bajo | 15 | (26.8%) | (26.8%) | (100.0%) |
| Total | | 56 | (100%) | (100%) | |

Fuente: Tiznado Ubillus (2019), ejecutado por el SPSS Versión 25

Figura 10. Descripción en porcentaje de los Riesgos proveniente de los programas




Fuente: Tiznado Ubillus (2019).

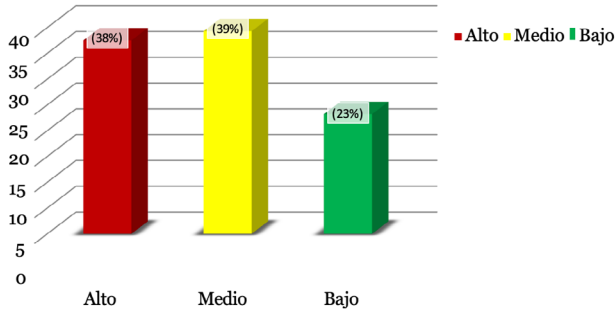
**En la Dimensión 3:** Riesgos Relacionados con los Trabajos, los resultados de la Tabla 12 muestran una distribución muy equilibrada entre las categorías alta y media. Un 38% de los encuestados percibe un alto riesgo de pérdida, corrupción o acceso no autorizado a sus datos académicos y profesionales (código, documentos), mientras que un 39% lo sitúa en un nivel medio. Solo un 23% lo considera bajo. La Figura 11 refleja esta dualidad. El hecho de que más de un tercio de los estudiantes vea como alta la amenaza a su producción intelectual y laboral es un dato muy significativo. Indica que valoran su trabajo y son conscientes de su vulnerabilidad en el entorno digital. Esta preocupación podría ser un motivador clave para la adopción de prácticas de seguridad más robustas, como el uso de repositorios con control de versiones, el cifrado de archivos sensibles y la autenticación de dos factores en servicios en la nube, conectando directamente la percepción de riesgo con posibles comportamientos de protección.

Tabla 12. Descripción de los Riesgos relacionado con los trabajos.

| **Dimensión 3: Riesgos relacionado con los trabajos.** | | | | | |
|---|---|---|---|---|---|
| | | **Frecuencia** | **Porcentaje** | **Porcentaje válido** | **Porcentaje acumulado** |
| Valido | Alto | 21 | (37.5%) | (37.5%) | (37.5%) |
| | Medio | 22 | (39.3%) | (39.3%) | (76.8%) |
| | Bajo | 13 | (23.2%) | (23.2%) | (100.0%) |
| Total | | 56 | (100%) | (100%) | |

Fuente: Tiznado Ubillus (2019), ejecutado por el SPSS Versión 25

Figura 11. Descripción en porcentaje de los Riesgos relacionado con los trabajos




Fuente: Tiznado Ubillus (2019).

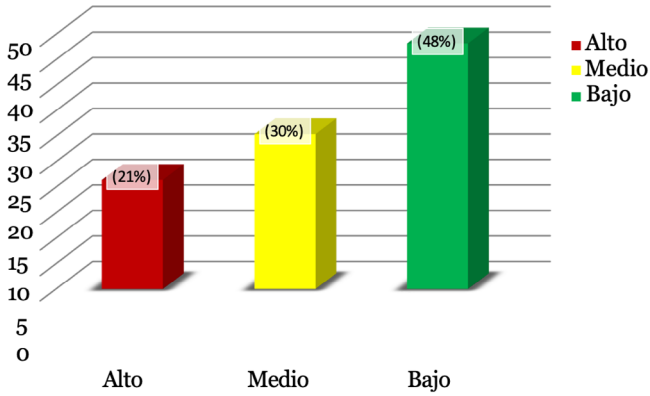
Finalmente, la **Dimensión 4:** Riesgos Respecto de las Personas (Factores Humanos) presenta el perfil más positivo, según los datos de la Tabla 13. Casi la mitad de los participantes (48%) reporta un nivel bajo de percepción de riesgo asociado a la ingeniería social, las malas prácticas con contraseñas o la negligencia. Un 30% lo sitúa en nivel medio y solo un 21% en nivel alto. La Figura 12 ilustra esta tendencia, donde la barra correspondiente al nivel bajo es la más prominente. Este resultado es, paradójicamente, uno de los más alarmantes desde una perspectiva de seguridad, ya que el factor humano es consistentemente identificado como el eslabón más débil en la cadena de ciberseguridad (ENISA, 2022). La baja percepción de riesgo en esta dimensión sugiere que los estudiantes pueden estar sobreestimando su capacidad para detectar intentos de phishing o subestimando la importancia de hábitos como el uso de contraseñas únicas y complejas. Esta brecha entre la percepción y la realidad del riesgo humano representa un área crítica para la intervención educativa, pues las amenazas que explotan la psicología y el comportamiento son de las más difíciles de mitigar con solo soluciones técnicas.

Tabla 13. Descripción de los Riesgos respecto a las personas.

| Dimensión 1: Riesgos respecto a las personas | | | | | |
|---|---|---|---|---|---|
| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
| Valido | Alto | 12 | (21.4%) | (21.4%) | (21.4%) |
| | Medio | 17 | (30.4%) | (30.4%) | (51.8%) |
| | Bajo | 27 | (48.2%) | (48.2%) | (100.0%) |
| Total | | 56 | (100%) | (100%) | |

Fuente: Tiznado Ubillus (2019), ejecutado por el SPSS Versión 25

Figura 12. Descripción en porcentaje de los Riesgos respecto a las personas




Fuente: Tiznado Ubillus (2019).

En síntesis, este análisis descriptivo multidimensional revela un panorama complejo y matizado. Los futuros desarrolladores de software muestran una conciencia variable según el tipo de riesgo: son más sensibles a las amenazas tangibles al hardware y a la pérdida de su trabajo, pero parecen subestimar, en promedio, los riesgos asociados al software malicioso y, de manera más crítica, los riesgos inherentes al factor humano. Esta cartografía de la percepción proporciona un diagnóstico invaluable para orientar los conte-

nidos de formación en ciberseguridad, destacando la necesidad urgente de fortalecer la conciencia sobre ingeniería social y hábitos de seguridad proactivos, incluso en una población con conocimientos técnicos en crecimiento.

## Del planteamiento a la verificación. La prueba empírica de las conexiones postuladas

La transición desde la descripción del panorama hacia la validación de las proposiciones teóricas constituye la fase crucial donde la investigación somete sus hipótesis al escrutinio de la evidencia estadística. Este proceso de prueba de hipótesis representa el núcleo inferencial del estudio, destinado a determinar si las relaciones postuladas entre los constructos centrales; los riesgos informáticos y la seguridad en dispositivos móviles, encuentran respaldo en los datos recolectados de la población objetivo. Se establece, por tanto, un marco de decisión basado en la lógica del contraste de hipótesis, donde cada afirmación (hipótesis alternativa, H1) se enfrenta a su negación estadística (hipótesis nula, H0). Para este fin, se adopta un nivel de significancia ($\alpha$) de 0.05, un estándar ampliamente aceptado en ciencias sociales que establece un umbral del 5% de probabilidad de rechazar la hipótesis nula cuando esta es verdadera (error Tipo I). Las reglas de decisión son claras: si el valor de probabilidad (p) obtenido en la prueba estadística es menor que $\alpha$ ($p < .05$), se rechaza la hipótesis nula, dando apoyo a la hipótesis alternativa. Si p es mayor que $\alpha$ ($p > .05$), no existe evidencia estadística suficiente para rechazar la hipótesis nula. La aplicación coherente de este protocolo a la hipótesis general y a las cuatro hipótesis específicas, utilizando el coeficiente de correlación Rho de Spearman, permitirá discernir con precisión qué dimensiones de la percepción de riesgo se asocian significativamente con las prácticas de seguridad móvil reportadas por los futuros desarrolladores de software.

## El vínculo general confirmado. Una correlación sólida entre conciencia y acción

La prueba de la hipótesis general buscaba evaluar la relación global entre la percepción agregada de riesgos informáticos y el nivel general de seguridad implementado en los dispositivos móviles. La hipótesis alternativa (H1) postulaba que dicha relación existía, mientras la hipótesis nula (H0) negaba cualquier asociación sistemática. Los resultados del análisis, sintetizados en la Tabla 14, ofrecen una respuesta contundente. El coeficiente Rho de Spearman obtenido es de $\rho = 0.782$, un valor que, según las convenciones de interpretación (Schober, Boer, & Schwarte, 2018), se clasifica como una correlación positiva y fuerte. Este hallazgo indica que existe una tendencia clara y marcada: a medida que los estudiantes reportan una mayor conciencia y preocupación por los diversos riesgos informáticos, también tienden a manifestar la adopción de prácticas de seguridad móvil más robustas y consistentes. La fuerza de esta asociación sugiere que la percepción del riesgo no es un factor aislado, sino que está íntimamente vinculada al comportamiento de protección en el ecosistema digital personal.

Tabla 14. Resultado–prueba de correlación Rho Spearman sobre la hipótesis general

| | | | **Riesgo Informático** | **Seguridad D. móvil** |
|---|---|---|---|---|
| Rho de Spearman | Riesgo informático | Coeficiente de correlación | 1,000 | ,782** |
| | | Sig. (bilateral) | | ,000 |
| | | N | 56 | 56 |
| | Seguridad D. móvil | Coeficiente de correlación | ,782** | 1,000 |
| | | Sig. (bilateral) | 000 | |
| | | N | 56 | 56 |

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Tiznado Ubillus (2019).

La solidez estadística de este hallazgo se confirma al examinar el valor de significancia (p), el cual es reportado como 0.000 ($p < .001$). Dado que este valor es considerablemente menor que el nivel de significancia establecido ($\alpha = 0.05$), se cumple el criterio para rechazar la hipótesis nula (H0). En consecuencia, se acepta la hipótesis alternativa (H1). La conclusión estadística se formula de la siguiente manera: Existe una correlación positiva, fuerte y estadísticamente significativa entre los riesgos informáticos y la seguridad en los dispositivos móviles en los estudiantes de la carrera de desarrollo de software de una institución en formación profesional técnica superior. Este resultado fundacional valida el marco teórico central del estudio y proporciona un punto de partida esencial para el análisis dimensional más detallado, confirmando que la conexión entre la cognición del riesgo y la conducta de seguridad es un fenómeno mensurable y relevante en esta población.

## Matices dimensionales. Desentrañando las fuentes específicas de la relación

Si bien el vínculo general es sólido, la verdadera riqueza analítica emerge al examinar cómo se comporta esta relación cuando se desagrega la variable de riesgos informáticos en sus dimensiones constitutivas. Este análisis granular permite identificar qué tipos específicos de riesgos actúan como motivadores más efectivos para la adopción de prácticas seguras, revelando un panorama más complejo y matizado.

La Hipótesis Específica 1 exploraba la relación entre la seguridad móvil y la dimensión de riesgos provenientes del equipo (hardware), es decir, aquellos asociados a fallas físicas, robo o daño del dispositivo. Los resultados presentados en la Tabla 15 muestran un coeficiente Rho de Spearman de $\rho = 0.178$. Esta magnitud indica una correlación positiva pero débil, casi despreciable según los criterios convencionales. Más decisivo aún es el valor de significancia asociado, $p = .191$. Dado que $0.191 > 0.05$, el resultado no es estadísticamente significativo. Por lo tanto, no se cumple el criterio para rechazar la hipótesis nula. Se concluye que no existe una relación significativa entre la percepción

de riesgos asociados al hardware y el nivel de seguridad reportado en los dispositivos móviles. Este hallazgo es intrigante y sugiere que, aunque los estudiantes pueden preocuparse por que su teléfono se rompa o sea robado (como se vio en los resultados descriptivos), esta preocupación no se traduce de manera directa o consistente en la implementación de medidas de seguridad digital proactivas, como el cifrado o las copias de seguridad en la nube. La protección del dispositivo físico y la protección de los datos que contiene parecen ser, en la mente de los participantes, dominios cognitivos y conductuales distintos.

Tabla 15. Resultado–prueba de correlación Rho Spearman sobre la hipótesis especifica 1

| | | | **Seguridad D. móvil** | **Riesgo p. de equipo** |
|---|---|---|---|---|
| Rho de Spearman | Seguridad D. móvil | Coeficiente de correlación | 1,000 | ,178 |
| | | Sig. (bilateral) | . | ,191 |
| | | N | 56 | 56 |
| | Riesgo p. de equipo | Coeficiente de correlación | ,178 | 1,000 |
| | | Sig. (bilateral) | ,191 | . |
| | | N | 56 | 56 |
| | **. La correlación es significativa en el nivel 0,01 (bilateral). | | | |

Fuente: Tiznado Ubillus (2019).

En marcado contraste, la Hipótesis Específica 2, que evaluaba la relación con los riesgos provenientes de los programas (software) tales como malware, vulnerabilidades, software malicioso, arroja un resultado robusto. La Tabla 16 reporta un coeficiente Rho de $\rho = 0.679$, interpretado como una correlación positiva y moderadamente fuerte. El valor de significancia es nuevamente $p < .001$ (.000). Al ser $p < \alpha$, se rechaza la hipótesis nula y se acepta la hipótesis alternativa. Esto significa que la percepción de amenazas ligadas al software

sí se asocia de manera significativa con mejores prácticas de seguridad móvil. Este resultado tiene una lógica poderosa: las amenazas de software (virus, phishing, aplicaciones espía) son combatidas precisamente con las herramientas y comportamientos que constituyen la seguridad móvil (antivirus, actualizaciones, descargas desde fuentes oficiales, cautela con enlaces). Los estudiantes que son más conscientes de estos riesgos digitales abstractos son precisamente aquellos que reportan tomar medidas concretas para defenderse de ellos, demostrando una alineación clara entre la percepción de la amenaza y la acción correctiva correspondiente.

Tabla 16. Resultado–prueba de correlación Rho Spearman sobre la hipótesis especifica 2

| | | | **Seguridad D. móvil** | **Riesgo p. de los programas** |
|---|---|---|---|---|
| Rho de Spearman | Seguridad D. móvil | Coeficiente de correlación | 1,000 | ,679** |
| | | Sig. (bilateral) | . | ,000 |
| | | N | 56 | 56 |
| | Riesgo p. de los programas | Coeficiente de correlación | ,679** | 1,000 |
| | | Sig. (bilateral) | ,000 | . |
| | | N | 56 | 56 |

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Tiznado Ubillus (2019).

La Hipótesis Específica 3 se centraba en los riesgos relacionados con los trabajos, es decir, la pérdida o compromiso de datos académicos y profesionales. Los resultados de la Tabla 17 muestran un coeficiente Rho de ρ = 0.577, lo que representa una correlación positiva y moderada. El valor p es de .000, nuevamente muy por debajo del umbral de .05, lo que lleva al rechazo de la hipótesis nula. Por lo tanto, existe una relación significativa: una mayor preocu-

pación por la seguridad de los productos de su trabajo (código, documentos, proyectos) se correlaciona con un mayor reporte de prácticas de seguridad en sus dispositivos móviles. Este hallazgo subraya el papel motivador del valor percibido de los activos digitales. Cuando los estudiantes perciben que su esfuerzo intelectual y profesional está en riesgo, es más probable que activen mecanismos de protección, posiblemente extendiendo las buenas prácticas aprendidas o intuitivas en el ámbito académico-profesional al uso personal de su dispositivo. Es una conexión que vincula la seguridad con la productividad y la preservación del capital intelectual.

Tabla 17. Resultado-prueba de correlación Rho Spearman sobre la hipótesis especifica 3

| | | | **Seguridad D. móvil** | **Riesgo r. con los trabajos** |
|---|---|---|---|---|
| Rho de Spearman | Seguridad D. móvil | Coeficiente de correlación | 1,000 | ,577** |
| | | Sig. (bilateral) | . | ,000 |
| | | N | 56 | 56 |
| | Riesgo relacionado con los trabajos | Coeficiente de correlación | ,577** | 1,000 |
| | | Sig. (bilateral) | ,000 | . |
| | | N | 56 | 56 |

**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Tiznado Ubillus (2019).

Finalmente, la Hipótesis Específica 4 examinaba la relación con los riesgos respecto de las personas, el factor humano (ingeniería social, malos hábitos de contraseñas, negligencia). Los datos de la Tabla 18 revelan un coeficiente Rho de $\rho = 0.637$, una correlación positiva y moderadamente fuerte, con un valor p de .000. Cumpliéndose $p < \alpha$, se rechaza la hipótesis nula y se acepta la hipótesis alternativa. Este es un resultado de capital importancia, pues indica que los estudiantes que tienen una mayor conciencia de los riesgos asocia-

dos al comportamiento humano, el eslabón tradicionalmente más débil en la cadena de seguridad, son también aquellos que afirman tener mejores prácticas de seguridad móvil. Sugiere que la comprensión de que la propia acción (o inacción) es una fuente de vulnerabilidad puede ser un motivador clave para adoptar conductas más prudentes, como el uso de autenticación de dos factores, la desconfianza ante correos sospechosos o la gestión cuidadosa de credenciales. Aceptar la propia falibilidad parece ser, en este grupo, un paso hacia una postura más segura.

Tabla 18. Resultado-prueba de correlación Rho Spearman sobre la hipótesis especifica 4

| | | | **Seguridad D. móvil** | **Riesgo R. a las personas** |
|---|---|---|---|---|
| Rho de Spearman | Seguridad D. móvil | Coeficiente de correlación | 1,000 | ,637** |
| | | Sig. (bilateral) | . | ,000 |
| | | N | 56 | 56 |
| | Riesgo respecto a las personas | Coeficiente de correlación | ,637** | 1,000 |
| | | Sig. (bilateral) | ,000 | . |
| | | N | 56 | 56 |

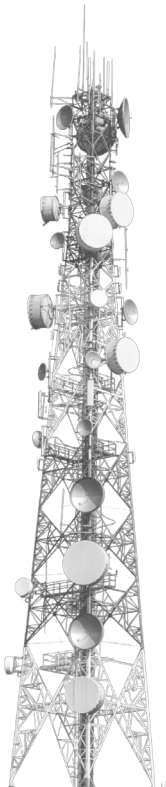
**. La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Tiznado Ubillus (2019).

En síntesis, la prueba de hipótesis revela un patrón claro y diferenciado. Mientras la relación general es fuerte, su intensidad y significancia varían según la naturaleza del riesgo percibido. Los riesgos abstractos y digitales (software, factor humano) y aquellos ligados a activos valiosos (trabajos) muestran asociaciones significativas y de moderadas a fuertes con la seguridad móvil. En cambio, el riesgo tangible asociado al hardware no muestra un vínculo es-

tadísticamente discernible. Este desglose no solo valida la hipótesis central del estudio, sino que enriquece profundamente la comprensión del fenómeno, señalando que no todos los riesgos motivan por igual la acción preventiva, y destacando las áreas de percepción (software y factor humano) que parecen ser los motores más efectivos para fomentar una cultura de seguridad proactiva entre los futuros profesionales de la tecnología.

# CAPÍTULO 4
# INTERPRETACIÓN Y DIÁLOGO CON LA EVIDENCIA. DISCUSIÓN DE LOS HALLAZGOS



La discusión constituye el espacio analítico donde los hallazgos empíricos del estudio son interpretados a la luz del marco teórico establecido, se contrastan con investigaciones previas y se extraen sus implicaciones más profundas. El objetivo central de este proyecto de investigación fue determinar la existencia y naturaleza de la relación entre los riesgos informáticos y la seguridad en los dispositivos móviles en una población específica de estudiantes de desarrollo de software. Los datos recolectados han proporcionado una respuesta clara y sustentada estadísticamente. Como se demostró en los análisis correlacionales, el coeficiente Rho de Spearman de 0.782 revela una correlación positiva y fuerte entre ambas variables, con un grado de significación estadística ($p < .001$) que permite rechazar firmemente la hipótesis nula. Este resultado no solo valida la premisa central de la investigación, sino que abre la puerta a un diálogo interpretativo sobre lo que esta asociación significa en el contexto de la formación de futuros profesionales del sector tecnológico. La evidencia sugiere de manera contundente que, para estos estudiantes, un mayor nivel de conciencia y percepción de las amenazas digitales se corresponde con un reporte más robusto de prácticas de protección en sus dispositivos personales. Este vínculo entre la cognición del riesgo y la conducta de seguridad establece un pilar fundamental para el diseño de intervenciones educativas efectivas, pues indica que incrementar el conocimiento sobre los peligros del entorno digital puede ser una vía prometedora para motivar una adopción más generalizada de hábitos seguros.

## Perfil de riesgo y seguridad. Un espejo de la literatura previa

Al profundizar en el perfil descriptivo de cada variable, los resultados del presente estudio entablan un diálogo significativo con investigaciones antecedentes, encontrando tanto convergencias como matices distintivos. En cuanto a la variable de riesgos informáticos, la distribución de los niveles de percepción (30% alto, 46% medio, 23% bajo) pinta un panorama donde la conciencia del riesgo es predominante pero no uniformemente crítica. Esta distribución encuentra ecos en trabajos previos que han evaluado percepcio-

nes similares. Por ejemplo, Otoya (2017), en su tesis sobre gestión de riesgos, encontró que un 63.33% de su población calificaba el nivel de gestión como "malo", lo que refleja una percepción negativa ampliamente extendida sobre la capacidad de manejar las amenazas, un sentimiento que puede ser paralelo a la concentración en niveles medio y alto observada aquí. De manera complementaria, Llontop (2018) identificó una deficiencia específica del 9.3% en la gestión de riesgos. Estas coincidencias subrayan que la percepción de vulnerabilidad y la identificación de deficiencias en el manejo de amenazas son temas recurrentes en la literatura. Estos hallazgos empíricos refuerzan y dan cuerpo operativo a la definición conceptual de Téllez (2008), quien define el riesgo informático como "la posibilidad de que ocurra un daño" (p. 158) y lo asocia a "la inseguridad existente" que permite la materialización de una amenaza. Los datos de este estudio, al mostrar que una mayoría percibe el riesgo en niveles medio y alto, confirman que esta "inseguridad existente" es una realidad palpable en la experiencia subjetiva de los estudiantes, constituyendo el sustrato cognitivo a partir del cual se pueden—o no—generar comportamientos de protección.

De manera análoga, los resultados de la variable de seguridad en dispositivos móviles (46% nivel alto, 38% medio, 16% bajo) establecen un interesante paralelismo con estudios anteriores. Nuevamente, el trabajo de Otoya (2017) sobre seguridad de la información reporta una distribución preocupante: 50% de los niveles percibidos como "deficientes", 34.17% como "regulares" y solo 15.83% como "eficientes". La similitud en la proporción del segmento con desempeño más bajo (16% vs. 15.83%) es notable y sugiere que, independientemente del contexto específico, existe una fracción significativa y consistente de la población que mantiene prácticas de seguridad insuficientes. Esta convergencia fortalece la validez externa de los hallazgos actuales. La investigación de Erreyes (2017), citada en los antecedentes, aporta una perspectiva aplicada al enfocarse en seleccionar y aplicar recursos de seguridad para la protección de datos en dispositivos móviles del público general. Su enfoque en la acción protectora resuena con la definición operativa de seguridad utilizada aquí, la cual se alinea con Domingo (2011), para quien la seguridad implica "una lista de elementos necesario para la identificación de los niveles de protección

que se está utilizando" (p. 7). Los resultados descriptivos del presente estudio, al cuantificar esos "niveles de protección" autorreportados, operacionalizan y miden precisamente el constructo al que alude Domingo, revelando que, si bien casi la mitad de los estudiantes alcanza un nivel alto, una porción no menor se ubica en un espectro de protección medio-bajo, lo que confirma la necesidad de seguir promoviendo la adopción de estos "elementos necesarios".

## Vulnerabilidad y mitigación. La relación dialéctica entre riesgo y protección

La discusión más profunda emerge al integrar los hallazgos de ambas variables y su relación. La significativa correlación positiva encontrada ($\rho = 0.782$) dibuja una realidad en la que la seguridad y la vulnerabilidad coexisten en una relación dialéctica. La existencia de una percepción de riesgo no es, en esta muestra, un motivo para la parálisis o la resignación, sino que parece actuar como un catalizador para la acción mitigadora. Este entendimiento es crucial: la seguridad no es la mera ausencia de riesgo, sino la respuesta activa y consciente a su presencia. Esta interpretación se ve robustecida al considerar investigaciones que han profundizado en las vulnerabilidades técnicas específicas. Por ejemplo, López (2016) se enfocó en identificar y explotar vulnerabilidades en dispositivos Android para luego proponer mitigaciones. Su trabajo ilustra el ciclo completo que conecta la identificación del riesgo (vulnerabilidades en el sistema operativo) con la búsqueda de soluciones de seguridad (parches, configuraciones). El presente estudio, al nivel perceptual y conductual, captura la contraparte humana de ese ciclo: la conciencia de que existen vectores de ataque (como los explorados por López) se correlaciona con la implementación de medidas que, en teoría, buscan cerrar esas brechas. Así, se argumenta que la seguridad es existente precisamente porque se reconoce la vulnerabilidad; si no hubiera riesgo percibido, probablemente no habría motivación para implementar protecciones. Esta dinámica refuerza la idea de que una cultura de seguridad robusta no se basa en la ilusión de invulnerabilidad, sino en el reconocimiento realista de las amenazas y en el compromiso sostenido con las prácticas de defensa.

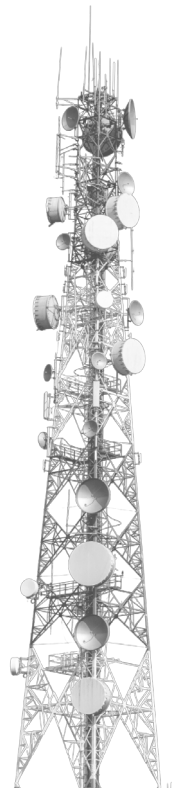
## Hacia una cultura de seguridad proactiva. Implicaciones y recomendaciones derivadas

La convergencia de los hallazgos propios con la literatura antecedente no solo valida la investigación, sino que también apunta de manera consistente hacia un camino de acción. Las recomendaciones implícitas y explícitas que emergen de este conjunto de trabajos subrayan la necesidad de intervenciones educativas y de capacitación estructuradas. El presente estudio identifica que, a pesar de la correlación general positiva, persisten porcentajes significativos de estudiantes con percepciones de riesgo bajas y prácticas de seguridad mejorables. Esta brecha coincide plenamente con la recomendación central de trabajos como el de Huamán (2017), quien propuso un proyecto de comunicación para construir una cultura de seguridad de la información entre el personal administrativo de una universidad. La traslación de esta recomendación al contexto de los estudiantes de desarrollo de software es directa y urgente. No se trata solo de enseñar a programar de manera segura, sino de fomentar una cultura de seguridad integral que permee su interacción cotidiana con la tecnología. Las capacitaciones deben, por tanto, ser bidireccionales: por un lado, deben elevar y precisar la percepción de los riesgos, particularmente en dimensiones como el factor humano y el software malicioso, donde las asociaciones fueron más fuertes; por otro lado, deben proveer el conocimiento práctico y accesible para implementar las medidas de seguridad correspondientes, cerrando el circuito entre "saber el peligro" y "saber cómo protegerse".

En conclusión, la discusión de los resultados revela un panorama coherente y alentador, pero no exento de desafíos. La fuerte relación entre la percepción de riesgos informáticos y la seguridad en dispositivos móviles valida el enfoque del estudio y sugiere que las intervenciones basadas en la concienciación pueden ser efectivas. Los perfiles descriptivos, en diálogo con investigaciones previas, confirman la presencia de vulnerabilidades perceptuales y conductuales recurrentes en poblaciones con y sin formación técnica especializada. Finalmente, la síntesis de estos elementos con la literatura es-

pecializada converge en una recomendación clara: la imperiosa necesidad de institucionalizar programas de formación y sensibilización en ciberseguridad que trasciendan lo técnico y fomenten una postura proactiva y responsable frente a los riesgos digitales, sentando las bases para una generación de desarrolladores que no solo construya software, sino que también lidere con el ejemplo en la práctica de una cultura de seguridad robusta.

# CAPÍTULO 5
# SÍNTESIS INTERPRETATIVA Y HORIZONTES DE ACCIÓN. CONCLUSIONES Y RECOMENDACIONES



La culminación del proceso investigativo se materializa en la síntesis de los hallazgos y en la derivación de implicaciones prácticas que trascienden el ámbito académico. Este capítulo tiene un doble propósito: primero, consolidar de manera estructurada y reflexiva las principales conclusiones extraídas del análisis de datos, articulando lo que los resultados revelan sobre la relación entre los riesgos informáticos y la seguridad en dispositivos móviles en el contexto estudiado; y segundo, traducir esas conclusiones en un conjunto de recomendaciones concretas y fundamentadas, dirigidas a mitigar los riesgos identificados y fortalecer las prácticas de seguridad entre la población objetivo y en entornos similares. Las conclusiones no son un mero resumen numérico, sino una interpretación integrada que vincula los resultados estadísticos con su significado sustantivo para la formación y la práctica profesional. De igual modo, las recomendaciones surgen directamente de las brechas y patrones identificados, proponiendo un camino a seguir para transformar el conocimiento generado en acción preventiva y en mejora educativa.

## Conclusiones. Un mapa de relaciones y vulnerabilidades

El análisis exhaustivo de los datos permite afirmar, con un alto grado de confianza estadística, que el objetivo principal de la investigación ha sido alcanzado. La evidencia empírica conduce a una conclusión general categórica: existe una relación positiva, fuerte y estadísticamente significativa entre la percepción de riesgos informáticos y el nivel de seguridad implementado en los dispositivos móviles por los estudiantes de la carrera de desarrollo de software. Esta conclusión se sustenta en el coeficiente de correlación Rho de Spearman de 0.782 y un valor de probabilidad de 0.000, lo que permite rechazar definitivamente la hipótesis nula. Este hallazgo central es de gran relevancia, pues valida la premisa teórica de que la concienciación sobre las amenazas del entorno digital constituye un factor asociado a la adopción de conductas protectoras. No obstante, esta relación general enmascara matices cruciales que se revelan al examinar las dimensiones específicas del riesgo, ofreciendo

un mapa detallado de qué tipos de amenazas funcionan como mejores predictores del comportamiento seguro.

La primera conclusión dimensional es igualmente esclarecedora: no se encontró una relación estadísticamente significativa entre la dimensión de riesgos provenientes del equipo (hardware) y las prácticas de seguridad móvil ($\rho = 0.178$, $p = .191$). Este resultado es particularmente llamativo si se considera que, de manera descriptiva, esta fue la dimensión con el porcentaje más alto de percepción de riesgo a nivel alto (36%). La disociación sugiere una brecha cognitivo-conductual: la preocupación por daños físicos, robo o fallas del dispositivo no se traduce de manera sistemática en la implementación de medidas de seguridad digital como el cifrado de datos, las copias de seguridad automatizadas en la nube o el uso de gestores de contraseñas. Los estudiantes parecen percibir la protección del objeto físico y la protección de la información que contiene como dominios separados, lo que los deja vulnerables a que un incidente físico (robo) se convierta también en una fuga masiva de datos personales o académicos por falta de cifrado.

En franco contraste, la segunda conclusión dimensional confirma que existe una correlación positiva y moderadamente fuerte entre la percepción de riesgos provenientes de los programas (software) y la seguridad en dispositivos móviles ($\rho = 0.679$, $p < .001$). Este hallazgo indica un alineamiento mucho más claro entre la amenaza percibida y la acción de defensa. Los estudiantes que son más conscientes de los peligros asociados al malware, el phishing, las aplicaciones maliciosas o las vulnerabilidades del software, son también aquellos que reportan con mayor frecuencia prácticas como mantener actualizado el sistema operativo, descargar aplicaciones solo de tiendas oficiales y utilizar software de seguridad. Esta dimensión, donde la percepción de riesgo se concentró mayoritariamente en un nivel medio (59%), parece actuar como un motor efectivo para la adopción de medidas de seguridad técnicas y específicas.

La tercera conclusión se refiere a los riesgos relacionados con los trabajos, donde también se halló una correlación positiva y moderada con la seguridad móvil ($\rho = 0.577$, $p < .001$). Este resultado subraya el valor motivador

que tiene la protección del capital intelectual y profesional. Cuando los estudiantes perciben que sus proyectos académicos, códigos fuente, documentos de investigación o datos laborales están en riesgo (38% nivel alto, 39% nivel medio), es más probable que adopten prácticas dirigidas a salvaguardar esa información en sus dispositivos. Esto podría reflejarse en el uso de aplicaciones de cifrado para archivos sensibles, la sincronización segura con servicios en la nube con autenticación de dos factores, o una mayor cautela al conectar el dispositivo a redes no confiables cuando se trabaja en material valioso. La seguridad se vincula aquí directamente con la productividad y la preservación del esfuerzo creativo.

Finalmente, la cuarta conclusión confirma una correlación positiva y moderadamente fuerte entre la percepción de riesgos respecto de las personas (factor humano) y la seguridad en dispositivos móviles ($\rho = 0.637$, $p < .001$). Este es un hallazgo de gran importancia práctica, considerando que esta fue la dimensión con el porcentaje más bajo de percepción de riesgo a nivel alto (solo 21%) y el más alto a nivel bajo (48%). A pesar de esta tendencia a subestimar el riesgo humano, aquellos estudiantes que sí reconocen los peligros de la ingeniería social, las malas prácticas con contraseñas o la negligencia, son precisamente los que muestran mejores hábitos de seguridad. Esto sugiere que superar la ilusión de invulnerabilidad personal es un paso crítico. Quienes comprenden que ellos mismos pueden ser el eslabón débil son más proclives a activar el bloqueo de pantalla, a ser escépticos ante mensajes de phishing, a usar contraseñas únicas y complejas, y a revisar los permisos de las aplicaciones. En definitiva, aceptar la propia falibilidad es el primer paso hacia una postura de autoprotección más robusta.

## Recomendaciones. De la evidencia a la práctica proactiva

Las conclusiones delineadas no solo describen un estado de cosas, sino que iluminan caminos concretos para la acción. Las siguientes recomendaciones, dirigidas a instituciones educativas, formadores y a los propios estudiantes, se derivan directamente de los patrones de vulnerabilidad y relación

identificados, con el objetivo de traducir los hallazgos en mejoras tangibles en la cultura de ciberseguridad.

*1. Implementación de programas integrados de concientización y capacitación técnica*

La fuerte correlación general señala que la concienciación es un motor efectivo, pero los resultados descriptivos muestran que los niveles de riesgo y seguridad pueden mejorarse. Se recomienda encarecidamente que la institución en formación profesional técnica superior, y otras formadoras en carreras tecnológicas, institucionalicen charlas, talleres y módulos curriculares obligatorios sobre ciberseguridad personal y profesional. Estos programas deben ser integrales, combatiendo específicamente las brechas identificadas. Deben, por un lado, elevar la percepción de riesgo en áreas subestimadas, como el factor humano, mediante ejemplos reales y simulaciones de ingeniería social. Por otro lado, deben proveer el conocimiento técnico práctico para implementar contramedidas, como configurar el cifrado del dispositivo, usar gestores de contraseñas o identificar aplicaciones legítimas.

*2. Fomentar una seguridad integral que incluya la protección física de los datos*

Dada la conclusión de que la preocupación por el hardware no se correlaciona con la seguridad digital, es crucial educar en la inextricable vinculación entre el dispositivo físico y los datos que almacena. Las recomendaciones deben enfatizar que un teléfono robado es una puerta de entrada a la vida digital de una persona si no está protegido. Se debe instruir activamente en: a) Activar el cifrado total del almacenamiento (una función disponible en la mayoría de los sistemas operativos modernos), que vuelve ilegibles los datos sin la contraseña o PIN; b) Configurar copias de seguridad automáticas y cifradas en servicios en la nube de confianza, para permitir la recuperación de la información tras un incidente; y c) Utilizar herramientas de borrado remoto,

vinculadas a la cuenta del dispositivo, que permitan eliminar la información de manera remota en caso de pérdida o robo. Esto transforma la preocupación por el objeto en una acción concreta de protección de la información.

*3. Promover la higiene digital en la gestión de software y conectividad*

Las conclusiones sobre los riesgos de software y la conectividad inalámbrica exigen recomendaciones de "higiene digital" básica pero crítica. Se debe aconsejar de manera explícita: a) Desactivar las conexiones inalámbricas no utilizadas (Bluetooth, Wi-Fi, NFC) cuando no se estén empleando, especialmente en lugares públicos, para reducir los vectores de ataque y la recolección pasiva de datos; b) Evitar absolutamente la instalación de aplicaciones (APKs) desde fuentes no oficiales (descargas directas de internet, enlaces en mensajes), ya que son el principal vector de infección de malware; c) Verificar escrupulosamente los permisos que solicitan las aplicaciones al instalarlas o actualizarlas, rechazando aquellos que sean excesivos o no relacionados con la función de la app (p.ej., una linterna que pide acceso a contactos y ubicación); y d) Habilitar las actualizaciones automáticas del sistema operativo y las aplicaciones, pues estas contienen parches de seguridad críticos para vulnerabilidades recién descubiertas. Estas prácticas, aunque simples, constituyen una barrera defensiva fundamental.

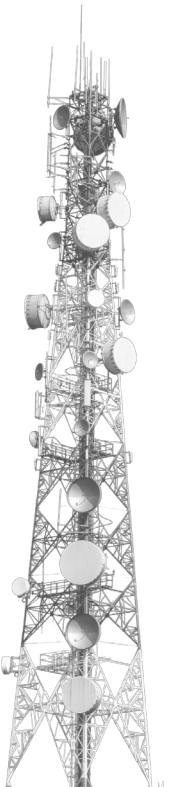
*4. Cultivar una mentalidad de desconfianza saludable y protección del capital profesional*

Finalmente, las conclusiones relacionadas con el factor humano y los trabajos apuntan a la necesidad de desarrollar una actitud proactiva. Se recomienda: a) Adoptar un escepticismo sistemático ante mensajes inesperados, ofertas demasiado buenas para ser verdad o solicitudes de información personal, verificando siempre la fuente por un canal independiente; b) Aplicar los principios de seguridad aprendidos en el ámbito académico-profesional

(como el control de versiones en Git o el manejo de secretos) al ámbito personal, tratando la información confidencial propia con el mismo cuidado; y c) Utilizar la autenticación de dos factores (2FA) en todos los servicios que la ofrezcan, especialmente en correo electrónico, banca en línea y redes sociales, para añadir una capa de seguridad que trascienda la contraseña. Estas acciones convierten la conciencia del riesgo en un protocolo de conducta habitual y resiliente.

En síntesis, esta investigación concluye que el vínculo entre el conocimiento del riesgo y la acción de seguridad es una realidad empírica en la población estudiada, con variaciones significativas según el tipo de amenaza percibida. A partir de este entendimiento, las recomendaciones propuestas buscan cerrar las brechas identificadas, fortaleciendo tanto la percepción como la práctica, para contribuir a la formación de una generación de desarrolladores de software que no solo sean competentes en la creación de tecnología, sino también ejemplares en su uso seguro y responsable.

# REFERENCIAS



Aguilera P. (2010). *Seguridad informática*. Editex, S.A.

Arias, F. (2012). *El proyecto de investigación: Introducción a la metodología científica*. Editorial Episteme.

Behar, D. (2008). *Metodología de la investigación*. Editorial Shaloom.

Bernal, C. A. (2010). *Metodología de la investigación*. Pearson Education.

Bustelo, C. (s.f.). *Identificación de riesgos en la producción, gestión y mantenimiento de documentos electrónicos.* PiedPiper. https://n9.cl/1gnyqb

Carcausto, W. y Guillen, O. (2013). *Guía de SPSS 21*. Universidad Cesar Vallejo.

Dei, D. (2008). *La tesis: Cómo orientarse en su elaboración*. Prometeo Editorial.

Domingo, M. (2011). *Seguridad en dispositivos móviles.* Create Commons. https://n9.cl/idly5k

El Comercio. (2018, 19 de agosto). *En qué consistió el ciberataque a los bancos peruanos y cómo se repelió.* https://n9.cl/qhi8h1

Erreyes, D. (2017). *Metodología para la selección de herramientas eficientes y protocolos adecuados para mejorar la seguridad de los dispositivos móviles* [Tesis de maestría, Universidad de Cuenca].

Escrivá, G., Romero, R., Ramada, D. y Onrubia, R. (2013). *Seguridad informática*. Macmillan Iberia, S.A.

Giusto, D. (2018, 6 de agosto). *Balance semestral de seguridad móvil*. WeLiveSecurity. https://n9.cl/n3iw6

González, A. (2018). *Seguridad en smartphone: Análisis de riesgos, de vulnerabilidades y auditoría de dispositivos* [Tesis de maestría, Universidad de Catalunya].

Hernández, R., Fernández, C., y Baptista, P. (2006). *Metodología de la investigación*. McGraw-Hill.

Huamán, F. (2017). *Plan de comunicaciones en seguridad de la información para el personal administrativo de la Pontificia Universidad Católica del Perú* [Tesis de maestría, Pontificia Universidad Católica del Perú].

Kemp, S. (2018). *Digital in 2018*. Hootsuite. https://n9.cl/jgbn1

La República. (2018, 18 de agosto). *Asbanc confirma que ataque financiero mundial afectó al Perú*. https://n9.cl/hw3w9

La República. (2018, 20 de agosto). *Ataque cibernético: Conoce cómo sabrás si eres víctima de un hacker*. https://n9.cl/chvu7

Llontop, G. (2018). *Gestión de riesgos de tecnologías de información de las empresas de Nephila Networks* [Tesis de maestría, Universidad César Vallejo].

López, A. (2016). *Aseguramiento de dispositivos móviles Android para el cumplimiento de la norma (PCI–DSS)* [Tesis de maestría, Universidad Internacional de la Rioja].

Mosquera, E. (2016, 26 de enero). *Protege tu móvil, es el año del malware.* El Mundo. https://n9.cl/ny6pl

Muñoz, C. (2011). *Cómo elaborar y asesorar una investigación de tesis*. Pearson Educación.

Otoya, M. (2017). *Gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017* [Tesis de maestría, Universidad César Vallejo].

Rojas, C. (2016). *Evaluación de la seguridad de aplicaciones móviles bancarias* [Tesis de maestría, Universidad de Chile].

Sabino, C. (2006). *Cómo hacer una tesis*. Editorial Panapo de Venezuela.

SENATI. (2018). *Cisco advierte sobre nocivos virus y malware en empresas*. https://n9.cl/lyvx1

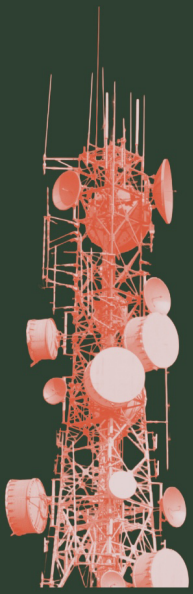
Serra, C. (2013). *Herramienta para evaluar la gestión de riesgos*. DataSec.

Téllez, J. (2008). *Derecho informático*. Instituto de Investigación Jurídica, Universidad Nacional Autónoma de México.

Tiznado Ubillus, J. A. (2019). *Riesgo y Seguridad en los Dispositivos Móviles en Estudiantes de la Carrera de Desarrollo de Software en el SENATI, 2019* [Tesis de maestría, Universidad César Vallejo].

Valderrama, S. (2013). *Pasos para elaborar proyectos de investigación científica*. Editorial San Marcos.

ATIK
editorial



ISBN: 978-9907-807-02-8