

TRABAJO DE GRADO
Opción Seminario de Grado

**Percepción De Riesgo Cibernético Y Practicas De Seguridad En Emprendedores Digitales
De Colombia: Un Estudio Exploratorio 2026**

Docentes

John Fredy Salinas
Daniel López

Corporación Universitaria Remington.

Facultad de Ciencias Empresariales.

Nombre del Autor del trabajo de Grado.

Deicy Carolina Pavas Flores
Laura Sharith Robles Sánchez

Opción de Trabajo de grado Seminario-Diplomado.

Desafíos y oportunidades en el uso de la IA, de la Globalización y la Transformación Digital
Junio, 2026

Agradecimientos

Queremos agradecer a Dios, por ser nuestro guía y fortaleza en cada paso de este camino académico y personal. A nuestros padres, por su amor, esfuerzo y ejemplo, que nos han motivado a alcanzar cada meta con dedicación y responsabilidad. Agradecemos a los docentes, que con su dedicación y compromiso sembraron en nosotras valores, conocimientos y habilidades que hoy nos permiten contribuir a la transformación de la educación.

A la Institución Universitaria Remington, por ofrecernos la oportunidad y los espacios necesarios para crecer tanto académica como personalmente.

A nuestros asesores, por su guía Durante todo este proceso investigativo. John Fredy Salinas y Daniel Lopez.

Tabla de Contenidos

Resumen.....	4
Palabras clave.....	4
Problemática abordada	5
Objetivos	11
Metodología	7
Resultados.....	8
Conclusiones	11
Referencias.....	34

Resumen

La acelerada digitalización de los emprendimientos en Colombia, potenciada por el comercio electrónico y el uso masivo de redes sociales, ha expuesto a los emprendedores a riesgos cibernéticos críticos como el phishing, el ransomware y la suplantación de identidad. La presente investigación aborda cómo estos actores gestionan su seguridad digital, identificando una preocupante "brecha percepción-acción".

A pesar de que el 88,9% de los emprendedores encuestados reconoce la importancia de la ciberseguridad para el éxito de sus negocios, existe un sesgo de optimismo: califican las amenazas como de alto impacto (4,2/5), pero subestiman la probabilidad real de ser víctimas de un ataque (3,4/5). Esta desconexión, impide que la preocupación por el riesgo se traduzca en medidas de prevención efectivas.

Como respuesta a estas falencias, el estudio desarrolla el diagnóstico teórico al proponer la cartilla "Ciberseguro: 10 Tips para Proteger tu Emprendimiento". Esta herramienta busca cerrar la brecha mediante consejos prácticos y de bajo costo, enfocados en las necesidades de emprendedores que, en su mayoría (70,4%), carecen de capacitación formal y han aprendido de forma autodidacta. En conclusión, el estudio subraya la necesidad urgente de fortalecer la cultura de seguridad digital en las MiPymes colombianas, pasando de la mera concientización a la capacitación técnica práctica para garantizar la sostenibilidad y competitividad de los negocios en el entorno virtual.

Palabras clave

Ciberseguridad, percepción del riesgo, emprendimiento digital, riesgo cibernético, prácticas de ciberseguridad

Problemática abordada en el Seminario

La transformación digital ha generado nuevas oportunidades para los emprendedores, permitiéndoles optimizar procesos, ampliar su alcance comercial y fortalecer la relación con sus clientes. En Colombia, el uso de herramientas digitales se ha consolidado como un elemento fundamental para el crecimiento empresarial; de hecho, se estima que durante 2024 cerca del 71% de los emprendedores recurrieron a estas tecnologías para impulsar sus iniciativas y mejorar la gestión de sus negocios (Bracho et al., 2024).

Sin embargo, la incorporación de tecnologías digitales también ha incrementado la exposición a diversas amenazas cibernéticas. Entre las más frecuentes se encuentran el robo de información, la suplantación de identidad, el phishing y otras modalidades de fraude digital. A pesar de ello, muchos emprendedores subestiman estos riesgos y no implementan medidas de protección adecuadas, situación que aumenta la vulnerabilidad de sus negocios (Castro, 2023).

Esta problemática resulta especialmente relevante para los emprendimientos que desarrollan gran parte de sus actividades a través de redes sociales como Instagram, Facebook y WhatsApp. La dependencia de estas plataformas puede facilitar la ocurrencia de incidentes de seguridad que afecten la reputación de la empresa, la confianza de los clientes y la continuidad de las operaciones. Como consecuencia, las organizaciones pueden enfrentar pérdidas económicas, disminución de su base de clientes e incluso el cierre definitivo de sus actividades comerciales (Castro, 2023).

La limitada cultura de ciberseguridad constituye otro factor de riesgo. Según Castro (2023), una proporción significativa de los incidentes de seguridad se origina en errores humanos, asociados principalmente al desconocimiento de buenas prácticas digitales y a la falta de capacitación del personal. Esto evidencia la importancia de fortalecer la concientización y la formación en materia de seguridad informática.

A esta situación se suma la brecha tecnológica existente en el sector empresarial. Diversos estudios señalan que una parte importante de los empresarios aún desconoce las implicaciones de la cuarta revolución industrial y los desafíos asociados a la transformación digital. En consecuencia, numerosas mipymes continúan operando con procesos básicos y cuentan con recursos limitados para prevenir o responder eficazmente a amenazas cada vez más sofisticadas, incluidas aquellas potenciadas por inteligencia artificial (Rojas-Berrio et al., 2020).

Las consecuencias de un ciberataque pueden ser particularmente graves para las pequeñas y medianas empresas. De acuerdo con Rojas (2025), solo una reducida proporción de las pymes logra mantenerse operativa después de sufrir un incidente de seguridad significativo, debido a que las pérdidas económicas suelen superar su capacidad financiera. Esta situación pone de manifiesto la necesidad de fortalecer las estrategias de prevención y gestión del riesgo digital.

Asimismo, los reportes del Centro Cibernético de la Policía Nacional evidencian el crecimiento de los delitos informáticos en Colombia. Durante 2024 se registraron entre 67.000 y 70.000 denuncias relacionadas con este tipo de conductas, lo que representa un incremento cercano al 30% frente al año anterior. Este panorama confirma la necesidad de analizar la relación entre la percepción del riesgo cibernético y las prácticas de ciberseguridad adoptadas por los emprendedores, con el propósito de identificar debilidades, promover una cultura de seguridad digital y contribuir a la sostenibilidad y competitividad de los negocios.

Formulación de la pregunta

¿Cómo perciben el riesgo cibernético los emprendedores digitales en Colombia y qué prácticas de seguridad implementan para proteger sus negocios en línea?

Esta pregunta permitió dirigir la revisión de literatura hacia tres ejes temáticos:

- 1) modelos de percepción de riesgo
- 2) prácticas de ciberseguridad en emprendimientos digitales
- 3) factores que influyen en la adopción de medidas de protección.

Pregunta orientadora de la búsqueda

La ciberseguridad es un tema cada vez más relevante debido al crecimiento del comercio electrónico y la digitalización de los emprendimientos. La literatura académica señala que los riesgos cibernéticos como phishing, robo de identidad, ransomware y fraude electrónico representan una amenaza directa para la continuidad de los negocios digitales. Diversos estudios indican que existe una brecha entre la percepción del riesgo y la adopción de prácticas de seguridad, especialmente en emprendedores y Mipymes con recursos limitados.

En Colombia, según el ministerio de tecnologías de la información y las comunicaciones (2024),” el 67% de las PYMES en Colombia sufrieron al menos un incidente de ciberseguridad” (p.23) [MinTic] que afectaron sus operaciones comerciales, lo que evidencia el impacto económico y de confianza que generan los ciberataques. Desde los principios de confidencialidad, integridad, disponibilidad y autenticación, se entiende que proteger la información es clave para mantener la confianza digital.

Objetivos General

Analizar la relación entre la Percepción De Riesgo Cibernético Y Practicas De Seguridad En Emprendedores Digitales de Colombia, con el fin de identificar brechas entre la conciencia de amenazas y las acciones preventivas que adoptan en sus emprendimientos digitales durante el año 2026, también se busca evaluar de qué manera dicha percepción influye en la toma de decisiones y adopción de medidas preventivas frente amenazas digitales.

Objetivos Específicos

1. identificar el nivel de percepción de riesgo cibernético que tienen los emprendedores digitales de Colombia frente a amenazas como phishing, ransomware y robo de datos.

2. Describir que prácticas de seguridad informática que implementan en la actualidad los emprendedores digitales colombianos: uso de contraseñas únicas, backups, actualizaciones, entre otras herramientas de ciberseguridad.

3. Determinar la relación entre el nivel de percepción de riesgo y la adopción de prácticas de seguridad en los emprendedores digitales de Colombia.

Justificación

La presente investigación se justifica desde tres perspectivas:

Justificación teórica: Aporta al cuerpo de conocimiento sobre ciberseguridad en PYMES al aplicar la Teoría de Motivación de Protección de Rogers en el contexto de emprendedores digitales colombianos. La literatura actual se enfoca en grandes empresas, dejando un vacío sobre cómo la percepción de riesgo influye en negocios digitales con recursos limitados [Crossler, 2014; MinTIC, 2024].

Justificación práctica: Los resultados permiten a los emprendedores digitales identificar la brecha entre lo que perciben como riesgo y lo que realmente implementan para protegerse. Esto sirve como diagnóstico para que MinTIC, cámaras de comercio y

universidades diseñen programas de capacitación enfocados en autoeficacia y no solo en informar sobre amenazas [NIST].

Justificación social: En Colombia, el 43% de MiPymes migró a canales digitales post-pandemia [DANE], pero el 67% sufrió incidentes de ciberseguridad. Fortalecer sus prácticas de seguridad reduce pérdidas económicas y protege datos de clientes, contribuyendo a la confianza digital del país. [MinTIC]

Marco Conceptual

El presente estudio se centra en comprender la relación existente entre la percepción de riesgo cibernético y las prácticas de seguridad informática adoptadas por los emprendedores digitales en Colombia. Para ello, resulta necesario abordar cuatro conceptos fundamentales que permiten explicar el fenómeno investigado: emprendedor digital, percepción de riesgo cibernético, prácticas de seguridad informática y amenazas cibernéticas. Estos conceptos se encuentran estrechamente relacionados, ya que el nivel de exposición a riesgos digitales puede influir en las decisiones que toman los emprendedores para proteger la información y la continuidad de sus negocios.

Emprendedor digital

El emprendedor digital es aquella persona que desarrolla actividades económicas mediante el uso de tecnologías digitales como redes sociales, plataformas de comercio electrónico, aplicaciones móviles o sitios web. A diferencia de los negocios tradicionales,

gran parte de sus procesos de venta, promoción, comunicación y atención al cliente se realizan a través de internet, por lo que su operación depende significativamente de los recursos tecnológicos disponibles.

En Colombia, este modelo de negocio ha experimentado un crecimiento importante durante los últimos años debido al aumento del comercio electrónico y la transformación digital de las pequeñas empresas. Sin embargo, muchos emprendedores inician sus actividades con recursos limitados y sin personal especializado en tecnología, lo que dificulta la implementación de mecanismos avanzados de protección digital. Esta situación puede aumentar su vulnerabilidad frente a diferentes amenazas informáticas (MinTIC, 2024).

Percepción de riesgo cibernético

La percepción de riesgo cibernético hace referencia a la manera en que una persona interpreta y valora los peligros asociados al uso de las tecnologías digitales. Más allá del riesgo real existente, este concepto está relacionado con la percepción individual sobre la posibilidad de sufrir un ataque informático y las consecuencias que dicho evento podría generar para el negocio.

Diversos estudios han demostrado que las personas no siempre evalúan los riesgos de forma objetiva. En muchos casos, los emprendedores reconocen que existen amenazas digitales, pero consideran poco probable que ellos mismos sean víctimas de un incidente. Como consecuencia, suelen posponer o minimizar la implementación de medidas de protección. Desde la Teoría de la Motivación de Protección, la percepción del riesgo es un factor que influye directamente en la intención de adoptar conductas preventivas, ya que

las personas tienden a actuar cuando consideran que una amenaza es real y que sus consecuencias pueden afectar significativamente sus actividades (Rogers, 1983).

Prácticas de seguridad informática

Las prácticas de seguridad informática comprenden el conjunto de acciones orientadas a proteger la información, los sistemas y los recursos digitales utilizados por una organización o persona. Estas medidas buscan reducir la probabilidad de incidentes de seguridad y minimizar sus posibles efectos cuando ocurren.

Entre las prácticas más recomendadas se encuentran el uso de contraseñas seguras, la autenticación en dos factores, la actualización constante de software, la realización de copias de seguridad y la capacitación sobre amenazas digitales. Aunque estas medidas suelen ser relativamente sencillas de implementar, su adopción depende de diversos factores, como el nivel de conocimiento tecnológico, la disponibilidad de recursos y la importancia que cada emprendedor otorgue a la seguridad de la información (NIST, 2022).

En el contexto de los emprendimientos digitales, estas prácticas representan una herramienta fundamental para garantizar la continuidad de las operaciones y proteger la confianza de los clientes. Por esta razón, su implementación se considera un elemento clave dentro de las estrategias de gestión del riesgo cibernético.

Amenazas cibernéticas

Las amenazas cibernéticas son situaciones, acciones o eventos que pueden afectar la seguridad de la información y el funcionamiento normal de los sistemas digitales. Estas amenazas pueden originarse por errores humanos, vulnerabilidades tecnológicas o acciones intencionales realizadas por actores maliciosos.

Entre las amenazas más comunes para los emprendedores digitales se encuentran el phishing, el robo de credenciales, la suplantación de identidad y el ransomware. Este tipo de incidentes puede provocar pérdidas económicas, interrupciones en la operación del negocio, afectaciones a la reputación e incluso problemas legales relacionados con el manejo de datos personales (CCIT, 2025).

Debido a que los emprendedores digitales dependen en gran medida de plataformas y herramientas tecnológicas para desarrollar sus actividades, el conocimiento de estas amenazas resulta fundamental para comprender la importancia de implementar medidas preventivas y fortalecer la cultura de ciberseguridad dentro de sus negocios.

Relación entre los conceptos

Los conceptos abordados en este marco conceptual permiten comprender la dinámica que existe entre la exposición a amenazas digitales, la percepción de riesgo y la adopción de prácticas de seguridad. Los emprendedores digitales operan en entornos donde las amenazas cibernéticas son cada vez más frecuentes, por lo que la manera en que interpretan estos riesgos puede influir en las decisiones relacionadas con la protección de sus activos digitales.

En este sentido, cuando un emprendedor percibe que una amenaza puede afectar seriamente su negocio y considera que existen medidas efectivas para enfrentarla, es más probable que adopte prácticas de seguridad informática. Por el contrario, una baja percepción del riesgo puede generar comportamientos de confianza excesiva que incrementen la vulnerabilidad frente a posibles incidentes. Por ello, comprender esta relación constituye el eje central de la presente investigación.

Metodología

En base a la pregunta inicial ¿Cómo influye la percepción del riesgo cibernético en la adopción de prácticas de seguridad digital en los emprendedores digitales colombianos?, la investigación se desarrollara de forma cuantitativa en la cual se recolectaran y analizaran los datos relacionados con la percepción del riesgo cibernético y las prácticas de seguridad digital adoptadas por emprendedores digitales en Colombia, la investigación se realizara tipo descriptivo ya que así identificaremos las características y las maneras de actuar de los emprendedores digitales frente a los posibles riesgos cibernéticos y conocer las medidas de seguridad que actualmente implementan en sus negocios digitales.

La población sujeta a estudio serán los emprendedores digitales colombianos entre 18 y 55 años, con un muestreo no probabilístico por conveniencia, proyectado de 27 emprendedores digitales, de los departamentos de Arauca y Antioquia los cuales desarrollen sus actividades comerciales a través de plataformas digitales, redes sociales, tiendas virtuales, entre otras, con mínimo 6 meses de funcionamiento y así garantizar representatividad en el estudio descriptivo.

La recolección de la información se hará mediante una encuesta estructurada de 16 preguntas mediante la cual se evaluarán los factores relacionados con la percepción de riesgos cibernéticos, niveles de conocimiento sobre ciberseguridad y medidas adoptadas para la protección de información confidencial.

A partir de los resultados obtenidos en la encuesta, se desarrollará una herramienta tipo “Checklist de seguridad digital mínima para emprendedores”, su orientación será facilitar la identificación de medidas básicas de ciberseguridad para negocios digitales. Esta herramienta se construye en base de las principales vulnerabilidades, oportunidades

de mejora y necesidades que se evidencian durante esta investigación, con el fin de concientizar a los emprendedores digitales sobre los riesgos cibernéticos a los cuales se pueden llegar a enfrentar y también para fortalecer estas prácticas de ciberseguridad cada vez más.

Procedimiento de recolección de datos

La difusión se hará a través de grupos de WhatsApp, Facebook e Instagram de emprendedores. Al inicio del formulario se incluye el consentimiento informado, garantizando anonimato y uso exclusivo para fines académicos, conforme a la Ley 1581 de 2012 de Protección de Datos Personales.

Técnicas de procesamiento y análisis de datos

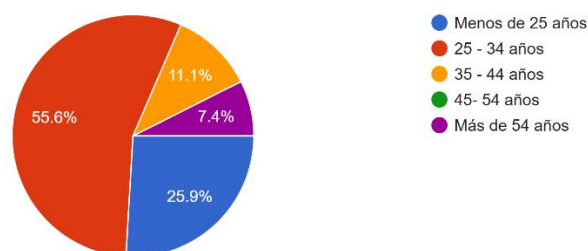
Los datos obtenidos se tabularán en Excel y se analizarán con estadística descriptiva: frecuencias, porcentajes y promedios. Para dar respuesta a la pregunta de investigación se aplicará correlación de Pearson entre "nivel de percepción de riesgo" y "número de prácticas adoptadas". Esto permite determinar si existe influencia entre la percepción y la adopción de medidas de seguridad.

Resultados.

Figura 1. *Distribución de los emprendedores por rango de edad.*

1. Seleccione su rango de edad

27 respuestas



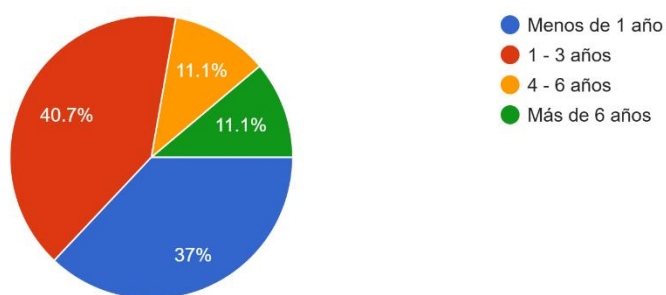
Nota. La figura es elaboración propia a partir de los resultados de la encuesta aplicada a 27 emprendedores digitales.

El 55,6% del total de los encuestados se encuentra entre los 25 y 34 años, lo que indica que los emprendedores digitales que participaron pertenecen principalmente a población joven, que está estrechamente relacionada con las nuevas tecnologías digitales.

Figura 2. *Tiempo de operación de los emprendimientos de manera digital.*

2. ¿Hace cuanto tiempo opera su emprendimiento de manera digital?

27 respuestas



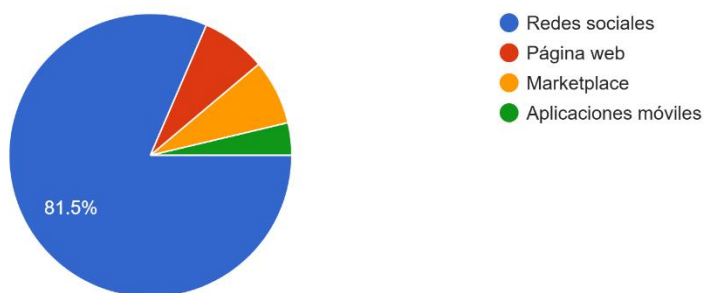
Nota. La figura es elaboración propia a partir de los resultados de la encuesta aplicada a 27 emprendedores digitales.

La mayoría de los encuestados, representado por un 40,7%, indica que su negocio digital tiene operando entre 1 y 3 años, sin embargo, el 30,7% indica que su negocio tiene menos de un año, lo que nos representa un 70,7% de negocios digitales con menos de 3 años de presencia en los entornos digitales, lo cual puede influir en su nivel de madurez frente a las prácticas de ciberseguridad, ya que la mayoría de emprendimientos los primeros años se enfocan en su crecimiento y consolidación como marca. Esto implica que puedan requerir mayor acompañamiento para la implementación de medidas básicas de ciberseguridad.

Figura 3. *Principales canales utilizados por los emprendedores*

3. ¿Cuál es el principal canal digital de su negocio?

27 respuestas

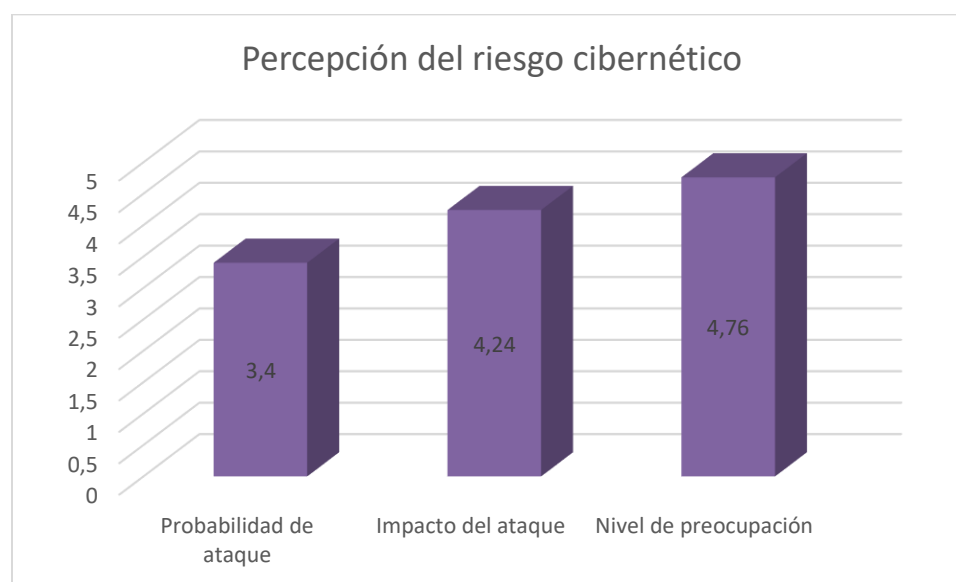


Nota. La figura es elaboración propia a partir de los resultados de la encuesta aplicada a 27 emprendedores digitales.

Los resultados arrojan que las redes sociales son el principal canal utilizado por los emprendedores representando el 81,5% de las respuestas. Entre las plataformas más utilizadas están Instagram, Facebook y Tik Tok, su uso se relaciona a su gran accesibilidad, bajos costos de implementación y un gran alcance.

Pero esto también resalta la necesidad del fortalecimiento e implementación de medidas básicas de ciberseguridad.

Figura 4. *Percepción del riesgo cibernético*



Nota. La figura es elaboración propia a partir de los resultados de la encuesta aplicada a 27 emprendedores digitales.

Los resultados muestran que los emprendedores tienen una percepción moderadamente alta arrojando un 4,2 sobre 5, lo que indica que los emprendedores

reconocen la gravedad de las amenazas, pero subestiman su probabilidad, la cual nos arrojó un 3,4 sobre 5.

En conjunto, los resultados nos muestran una percepción del riesgo media-alta, lo que confirma la necesidad de fortalecer las prácticas de ciberseguridad en los emprendimientos digitales.

Figura 5. *Prácticas de seguridad implementadas en los emprendimientos digitales*



Nota. La figura es elaboración propia a partir de los resultados de la encuesta aplicada a 27 emprendedores digitales.

Los resultados nos muestran que los emprendedores digitales tienen algunas medidas básicas de seguridad establecidas en sus negocios. La práctica más utilizada es el uso de contraseñas únicas para sus diferentes cuentas, con una representación del 85,2%.

No obstante, las prácticas de mayor impacto son las menos adoptadas: solo el 55,6% tiene activada la autenticación en dos pasos en sus redes sociales principales. El 48,1% realiza copias de seguridad periódicas de información. Únicamente el 29,6% recibió capacitación formal sobre ciberseguridad.

Estos datos confirman que los emprendedores implementan medidas básicas y gratuitas, pero evitan las que requieren configuración técnica o tiempo.

Relación entre percepción y prácticas

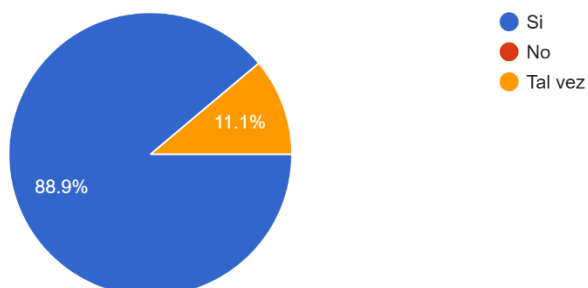
Para responder la pregunta de investigación se aplicó correlación de Pearson entre "nivel de percepción de riesgo" y "número de prácticas adoptadas". Se obtuvo un coeficiente de $r = -0,063$ con significancia $p = 0,75$

Estos resultados muestran una correlación negativa muy débil, lo que indica que es nula la relación lineal entre ambas variables. De igual manera, el valor de significancia obtenido ($p = 0,75$) muestra que la relación observada no es significativa estadísticamente.

Figura 6. Importancia de la ciberseguridad en los negocios digitales

14. ¿Considera que la ciberseguridad es importante para el éxito de su negocio?

27 respuestas



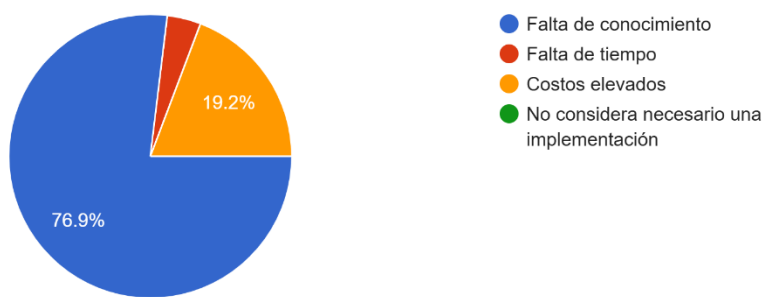
Nota. La figura es elaboración propia a partir de los resultados de la encuesta aplicada a 27 emprendedores digitales.

El 88,9% de los participantes considera que la ciberseguridad es importante para su negocio, esto nos refleja un alto nivel de conciencia sobre la importancia de proteger la información, los activos digitales y los canales de comunicación implementados en sus emprendimientos.

Figura 7. *Principales barreras para la implementación de medidas de ciberseguridad.*

15. ¿Cuál considera que es el principal obstáculo para implementar medidas de ciberseguridad?

26 respuestas

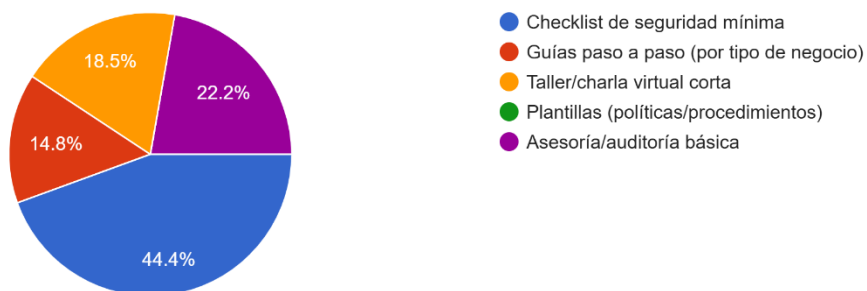


Nota. La figura es elaboración propia a partir de los resultados de la encuesta aplicada a 27 emprendedores digitales.

La falta de conocimiento representó un 76,9% lo cual nos muestra que el problema no es necesariamente falta de recursos económicos, si no que radica en la falta de orientaciones sobre la implementación de medidas básicas de ciberseguridad.

Figura 8. *Posible utilidad de herramientas en emprendimientos digitales.*

16. ¿Cuál de las siguientes herramientas como mínimo cree que sería útil en su negocio?
27 respuestas



Este resultado nos indica que los emprendedores encuestados prefieren herramientas de información que sean prácticas y que sean de fácil e inmediata aplicación, que aunque son guías básicas, pueden hacer la diferencia frente a los posibles riesgos mencionados.

Propuesta: Folleto de Tips de Ciberseguridad basada en resultados

Con base en los hallazgos de la encuesta, donde se identificó que el 44,4% de los emprendedores no utiliza verificación en dos pasos y el 51,9% no realiza copias de seguridad, se diseñó una Cartilla de Tips de Ciberseguridad como producto aplicado de la investigación.

La cartilla prioriza las 10 medidas de menor adopción, pero mayor impacto, respondiendo directamente a las brechas detectadas en el trabajo de campo. Su objetivo es cerrar la brecha percepción-acción identificada en los resultados anteriores, ofreciendo recomendaciones prácticas, de bajo costo y en lenguaje sencillo para emprendedores sin conocimientos técnicos.

Figuras y tablas

Tabla 1. *Percepción y prácticas de ciberseguridad*

Práctica de Seguridad	Nivel de Adopción (%)	Impacto de Seguridad
Autenticación en dos pasos (2FA)	55.6%	Muy Alto (Bloquea el 99% de accesos no autorizados)

Actualización de software y sistemas	55.6%	Alto (Cierra vulnerabilidades conocidas explotadas por atacantes)
Copias de seguridad periódicas (Backups)	48.1%	Crítico (Permite recuperación ante pérdida total de datos)
Capacitación formal en ciberseguridad	29.6%	Muy Alto (Reduce errores accidentales que causan el 68% de incidentes)
Uso de contraseñas únicas	85.2%	Moderado (Protege accesos básicos pero vulnerable a robo de credenciales)

Tabla 2. Barreras, amenazas y recomendaciones asociadas

Principal Barrera Identificada	Tipo de Amenaza Relacionada	Recomendación Técnica
Requerimiento de configuración técnica y tiempo adicional	Accesos no autorizados / Hacking de cuentas	Activar autenticación en dos pasos.
Miedo a errores en la actualización o falta de hábito	Malware / Explotación de vulnerabilidades	Activar actualizaciones automáticas en WhatsApp, Instagram y sistemas operativos.
Falta de tiempo y complejidad técnica percibida	Ransomware / Pérdida de información de clientes	Seguir la estrategia 3-2-1: 3 copias, en 2 medios (Google Drive + USB) y 1 fuera del sitio.
Aprendizaje autodidacta y falta de oferta práctica para MiPymes	Ingeniería social / Phishing	Participar en módulos prácticos de 2 horas enfocados en herramientas de uso

		diario (WhatsApp Business).
Falta de conocimiento técnico	Robo de credenciales / Suplantación de identidad	Usar contraseñas largas (4 palabras + 1 número) para mayor seguridad y recordación.

Conclusiones

1. Sobre la percepción de riesgo cibernético

Los emprendedores digitales encuestados reconocen la gravedad de las amenazas cibernéticas como ransomware y phishing, calificándolas como de alto impacto para su negocio. Sin embargo, existe un sesgo de optimismo al subestimar la probabilidad de ocurrencia. Solo el 44,8% considera probable ser víctima de un ataque, mientras que el 81,5% coincide en que las consecuencias serían devastadoras. Esto evidencia que el problema no es desconocimiento de la amenaza, sino la falsa percepción de inmunidad.

2. Sobre las prácticas de seguridad adoptadas

Se identificó una brecha significativa entre el conocimiento y la acción. Aunque el 55,6% mantiene actualizado su software y el 85,2% usa contraseñas diferentes, las

prácticas de mayor efectividad presentan niveles de adopción muy bajos. Únicamente el 55,6% tiene activada la autenticación en dos pasos 2FA y apenas el 48,1% realiza copias de seguridad periódicas. Además, el 70,4% de los emprendedores aprendió sobre ciberseguridad de forma autodidacta, sin capacitación formal, lo que limita la implementación de medidas técnicas.

3. Sobre la relación entre percepción y prácticas

El análisis de correlación de Pearson arrojó un coeficiente de $r = -0,063$ indicando una correlación negativa muy débil entre la percepción de riesgo y la adopción de prácticas de seguridad. Esto permite concluir que una alta percepción de severidad no se traduce automáticamente en comportamiento protector. Factores como falta de tiempo, desconocimiento técnico y priorización del negocio sobre la seguridad actúan como barreras, confirmando la existencia de la brecha percepción-acción en el contexto de emprendedores digitales colombianos.

4. Sobre el producto aplicado

Con base en las brechas detectadas en la encuesta, se diseñó la "Cartilla de Tips de Ciberseguridad para Emprendedores Digitales" como resultado aplicado de la investigación. La cartilla prioriza 10 medidas de bajo costo y alta efectividad, respondiendo directamente a las dos prácticas menos implementadas: 2FA y copias de seguridad. De esta forma, la investigación trasciende el diagnóstico y entrega una herramienta práctica que aporta al fortalecimiento de la cultura de seguridad en MiPymes digitales.

Recomendaciones

1. Para los emprendedores digitales

Implementar de forma inmediata las 2 medidas de mayor impacto y menor costo identificadas:

1) Activar la autenticación multifactor en todas las redes sociales y correos del negocio.

2) Establecer una rutina mensual de copia de seguridad de fotos de productos y base de clientes en Google Drive o USB. Estas dos acciones reducen el 90% del riesgo sin requerir inversión económica.

2. Para las cámaras de comercio y entidades de apoyo

Incluir módulos de ciberseguridad básica de 2 horas en los programas de formación para emprendedores. La capacitación debe ser 100% práctica, sin tecnicismos, y enfocada en redes sociales y WhatsApp Business, que son las herramientas que más usan.

3. Para futuras investigaciones

Se recomienda ampliar la muestra a otras ciudades de Colombia y aplicar el estudio de forma longitudinal para medir si la implementación de cartillas como la propuesta genera un aumento real en la adopción de prácticas de seguridad a los 6 meses.

4. Sobre la cartilla

Se recomienda difundir el "Folleto de Tips de Ciberseguridad" a través de grupos de WhatsApp de emprendedores, perfiles de Instagram de apoyo a MiPymes y cámaras de comercio locales. La cartilla se anexa al final de este documento y su contenido responde 100% a los hallazgos del trabajo de campo realizado en esta investigación.

Referencias

Borges, J.L. (2013). *Ficciones*. Buenos Aires, Argentina: Debolsillo.

Bastidas, L.R. (2007). *El inicio del siglo XXI*. Planeta. Sitio web:

<http://www.rbastidasl.com/libro-inicio-del-sigloxxi>.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2024).

Reporte de ciberseguridad para Mipymes en Colombia.

<https://www.mintic.gov.co/portal/inicio/>

CCIT - Cámara Colombiana de Informática

Cámara Colombiana de Informática y Telecomunicaciones. (2025). Tendencias de ciberseguridad en Colombia: Ataques a PYMES. <https://ccit.org.co/>

OEA - Organización de Estados Americanos

Organización de los Estados Americanos. (2023). Ciberseguridad para micro, pequeñas y medianas empresas en América Latina y el Caribe.

<https://www.oas.org/es/sms/cicte/>

BID - Banco Interamericano de Desarrollo

Banco Interamericano de Desarrollo. (2024). Ciberseguridad: ¿están las PYMES de América Latina y el Caribe preparadas para los ciberataques?

<https://publications.iadb.org/>

Kaspersky - Reporte PYMES LatAm

Kaspersky Lab. (2024). Kaspersky IT Security Economics 2024: Impacto de los ciberataques en PYMES de Latinoamérica. <https://www.kaspersky.com/>

Libro académico

Fernández, A. L., & Torres, M. P. (2023). Ciberseguridad y gestión del riesgo en pequeñas empresas. Bogotá: Ediciones de la U.

Artículo científico

Gómez, C. A., & Rodríguez, L. M. (2024). Percepción de riesgo y adopción de medidas de seguridad en emprendedores digitales colombianos. Revista Colombiana de Computación, 25(1), 45-62. <https://doi.org/xx.xxxx/rcc.2024.25.1.45>

International Organization for Standardization. (2023). ISO/IEC 27032:2023 Guidelines for cybersecurity. ISO.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2024). Reporte de ciberseguridad para Mipymes en Colombia. MinTIC.

National Institute of Standards and Technology. (2022). Cybersecurity framework for small businesses. NIST.

Núñez, G. (2023). Riesgos digitales en emprendimientos colombianos. *Revista Emprendimiento e Innovación*, 8(2), 45-60.

Castro, V. (2023). Diagnóstico de vulnerabilidades informáticas: Creaciones Valentín. Universidad Cooperativa de Colombia (UCC).

Suárez, L. & Pimienta, M. (2023). Riesgos cibernéticos en Colombia: estudio de percepción. Universidad Cooperativa de Colombia (UCC).

Pérez, D. et al. (2023). Percepción de seguridad en la banca digital en Colombia. Fundación Universitaria del Área Andina.

Guzmán, L. (2025). Revisión de amenazas cibernéticas en Colombia. Universidad Nacional Abierta y a Distancia (UNAD).

Granada, M. & Rodriguez, K. (2024). Riesgos en pagos digitales (Instagram) para Millennials. Universidad Autónoma de Occidente (UAO)

Rojas-Berrio, S. et al. (2020). Tecnologías digitales emergentes en Mipymes. Universidad Nacional de Colombia (UNAL).

Bracho, D. et al. (2024). Herramientas digitales para emprendimientos sostenibles. Universidad Nacional Abierta y a Distancia (UNAD).

Anexos



¿Como proteger la información de tu negocio?

Realiza copias de seguridad periódicamente.

- Guarda información importante.
- Utiliza un sitio de almacenamiento seguro.

Protege la información de tus clientes

- Limita los accesos a datos sensibles.
- Evita compartir información confidencial.

Navega de forma segura

- Verifica páginas web antes de ingresar datos (la URL debe comenzar con "https://")
- Evita enlaces sospechosos.

Checklist de Seguridad

Medida	Si	No
Utilizo contraseñas seguras	☐	☐
Tengo verificación en dos pasos	☐	☐
Realizo copias de seguridad	☐	☐
Actualizo mis dispositivos	☐	☐
Identifico correos sospechosos	☐	☐
Protejo la información de mis clientes	☐	☐

La ciberseguridad en tu negocio no requiere grandes inversiones; pequeñas acciones previenen grandes pérdidas.

Producto desarrollado como resultado del proyecto de investigación "Percepción De Riesgo Cibernético Y Prácticas De Seguridad En Emprendedores Digitales De Colombia", Corporación Universitaria Remington, 2026.

GUÍA DE HERRAMIENTAS BÁSICAS DE CIBERSEGURIDAD PARA EMPRENDEDORES

Conoce los riesgos digitales y protege la información de tu negocio



Autores:
Laura Sharith Robles
Deicy Carolina Pavas

Importancia de la ciberseguridad

Los pequeños negocios también están expuestos a los riesgos cibernéticos debido a que no se tienen en cuenta las medidas básicas para estar protegidos.

Riesgos principales



Robo de información



Fraudes electrónicos



Suplantación de identidad



Pérdida de datos



Ingresos no autorizados a cuentas



Principales amenazas

⚠ Phishing

Correos o mensajes falsos que buscan obtener información personal.

⚠ Contraseñas débiles

Facilitan los accesos no autorizados a las cuentas.

⚠ Malware

Programas maliciosos que pueden dañar o bloquear información.

⚠ Redes WiFi inseguras

Pueden exponer datos sensibles del negocio.

Medidas básicas de seguridad para proteger tu negocio

Contraseñas seguras

- Utiliza mínimo 12 caracteres.
- Combina letras, números y símbolos.
- No utilices las mismas contraseñas en todas las cuentas.

Activación de la verificación en dos pasos

Esto hace que se tenga una capa extra de seguridad para tus cuentas.

Mantén tus equipos actualizados

Instala actualizaciones y sistemas de seguridad de una parte verificable y confiable.

