Desarrollo de un modelo de ciberseguridad basado en SCRUM para MiPymes del Huila, asegurando su viabilidad y escalabilidad.

Hernando Arbey Robles Puentes

Asesor

Vanessa Paola Pertuz Peralta

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnologías e Ingenierías ECBTI

Maestría en Gestión de Proyectos

2025

Resumen

Las micro, pequeñas y medianas empresas (MiPymes) del departamento del Huila enfrentan crecientes desafíos en materia de ciberseguridad, derivados de la digitalización de sus procesos y la limitada capacidad para implementar soluciones técnicas robustas. Este trabajo de grado presenta el desarrollo de un modelo de ciberseguridad basado en el marco de trabajo con la metodología ágil SCRUM, enfocado en fortalecer la protección de los activos digitales de estas empresas. A través de un enfoque iterativo e incremental, el modelo permite gestionar riesgos cibernéticos de forma flexible, adaptándose a las necesidades específicas de cada empresa y promoviendo una cultura organizacional centrada en la seguridad. El estudio evalúa la viabilidad y escalabilidad del modelo en el contexto regional, considerando factores técnicos, económicos y humanos. El modelo resultante presenta una guía estructurada que facilita a las MiPymes del Huila implementar prácticas de ciberseguridad efectivas, sostenibles y alineadas con su capacidad operativa.

***Palabras clave**:* Ciberseguridad, MiPymes, SCRUM, gestión ágil, modelo escalable, viabilidad tecnológica

Abstract

Micro, small, and medium-sized enterprises (MiPymes) in the Huila department face growing challenges in cybersecurity, arising from the digitalization of their processes and their limited capacity to implement robust technical solutions. This degree work presents the development of a cybersecurity model based on the framework with the agile SCRUM methodology, focused on strengthening the protection of the digital assets of these companies. Through an iterative and incremental approach, the model allows for flexible management of cyber risks, adapting to the specific needs of each company and promoting an organizational culture centered on security. The study assesses the feasibility and scalability of the model in the regional context, considering technical, economic, and human factors. The resulting model provides a structured guide that helps MiPymes in Huila implement effective, sustainable cybersecurity practices in line with their operational capacity.

Keywords*:* Cybersecurity, MSMEs, SCRUM, agile management, scalable model, technological feasibility.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Introducción

En la era digital, las micro, pequeñas y medianas empresas (MiPymes) enfrentan un entorno empresarial altamente competitivo y vulnerable a diversas amenazas cibernéticas. De acuerdo con el estudio de la Estimación del Potencial de Comerciantes 2024, de la Camara de comercio del Huila (Camara de Comercio del Huila, 2024) indica que:

"El tejido empresarial del Huila en el año 2023 estuvo compuesto por 39.070 unidades productivas, presentando un decrecimiento del 0,51% respecto al año anterior, caracterizado de la siguiente manera: el 83,27% son personas naturales y el 16,73% restante son personas jurídicas. El sector económico más representativo es Comercio al por mayor y al por menor (49,32%), seguido de Alojamiento y servicios de comida (14,16%) e Industrias manufactureras (8,46%). De igual manera, las microempresas representan el 97,22% del tejido empresarial del Huila, seguido de las pequeñas empresas con 2,14%, mientras que las medianas y grandes representan el 0,48% y 0,16% respectivamente. La concentración por ubicación de las empresas se establece en su mayoría en la zona Norte (57%), seguido de la zona Sur (23,16%), Centro (12,66%) y Occidente (7,18%)."

A pesar de representar una parte significativa del tejido productivo del departamento del Huila (97,22%) y de Colombia en general (95,3% (Ministerio de Industria, Comercio y Turismo, 2023) muchas de estas organizaciones carecen de estrategias efectivas de ciberseguridad que les permitan proteger sus activos digitales, información sensible y continuidad operativa. Esta situación se agrava por la limitada disponibilidad de recursos financieros y humanos, así como por la falta de conocimiento especializado en tecnologías de la información.

La creciente dependencia tecnológica en los procesos empresariales de las MiPymes exige la adopción de modelos de seguridad que no solo sean eficaces, sino también adaptables, sostenibles y adecuados a su realidad organizacional. En este contexto, los marcos ágiles, y en particular SCRUM, ofrecen una oportunidad estratégica para implementar soluciones de ciberseguridad de manera iterativa, incremental y colaborativa. Aplicar SCRUM a la gestión de la ciberseguridad permite un enfoque flexible y escalable que puede alinearse con las necesidades y capacidades de cada empresa, favoreciendo la mejora continua y la rápida adaptación al cambio.

Este proyecto tiene como propósito desarrollar un modelo de ciberseguridad basado en SCRUM, especialmente diseñado para MiPymes del Huila, que garantice su viabilidad operativa y su potencial de escalabilidad. A través de este enfoque se busca fortalecer la postura de seguridad de estas organizaciones, promoviendo una cultura organizacional orientada a la gestión ágil de riesgos tecnológicos. Este documento expone el desarrollo teórico, metodológico y práctico del modelo propuesto, así como su aplicación piloto y resultados obtenidos.

Descripción del Problema

Según el Estudio trimestral de ciberseguridad publicado por la Cámara Colombiana de Informática y Telecomunicaciones (2022), durante el año 2021 se registraron más de 41 billones de intentos de ataques cibernéticos en el mundo y siete billones en Colombia. Además, en el periodo de noviembre a mediados de diciembre de 2022, el equipo ColCERT del Ministerio TIC recibió 36 reportes de incidentes de ciberseguridad, de los cuales 18 afectaron a entidades públicas de orden nacional y 5 a entidades territoriales, lo que evidencia un impacto directo sobre el sector público (Ministerio TIC, 2022).

Según FortiGuard Labs de Fortinet, en 2023 Colombia recibió 12.000 millones de intentos de ciberataques, una cifra menor que los 20.000 millones en 2022, aunque los incidentes se volvieron más sofisticados y dirigidos (Cámara Colombiana de Informática y Telecomunicaciones, 2024). Solo en el primer semestre, el país sufrió más de 5.000 millones de intentos, ubicándose en el cuarto puesto regional (Vanguardia, 2023).

Asimismo, la Superintendencia Financiera reportó que el sistema bancario enfrentó 28.000 millones de ataques en 2023, con una tasa de éxito prácticamente nula y un presupuesto de $440.000 millones COP en ciberseguridad (Superintendencia Financiera de Colombia, 2024).

Durante 2024, la amenaza cibernética global escaló a niveles sin precedentes. Check Point Research (2024) reporta que, en el tercer trimestre, las organizaciones fueron blanco de un promedio de 1876 ataques semanales, un aumento del 75 % interanual, con América Latina recibiendo 2844 ataques semanales en promedio (+72 %). Además, el Ransomware alcanzó un nuevo máximo con 5414 víctimas publicadas (+11 % respecto a 2023), destacándose el cuarto trimestre como el más activo con 1827 incidentes, un aumento del 29 % (Cyberint, 2024).

A lo largo del año, se contabilizaron 6,9 mil millones de ataques de malware, se infectaron 21 millones de sitios web y 1,4 mil millones de cuentas de redes sociales fueron atacadas, todos con crecimientos de más del 10 % frente a 2023 (DataLock, 2024). Las cifras continuaron su escalada en 2024: COLCERT registró 22.086 vulnerabilidades, y los intentos de ciberataque superaron los 36.000 millones, consolidando a Colombia como el cuarto país más atacado de la región (Asociación Colombiana de Ingenieros de Sistemas, 2024).

De acuerdo con el último informe presentado por la fiscalía general de la Nación: "… en Colombia en el año 2021 el número de ataques cibernéticos aumentó en un 30%, comparado con el año anterior. Si bien, las compañías y entidades oficiales han venido trabajando fuertemente en estrategias tendientes a robustecer las medidas de ciberseguridad, estas no han sido suficientes, ya que casos como el secuestro de información o la afectación de datos a entidades mediante Ransomware o ataques de día cero sin filtración de datos, aún continúan presentándose y han ocasionado grandes pérdidas económicas para las organizaciones ya que éstas han tenido que efectuar cuantiosos pagos frente a este tipo extorsiones a los cibercriminales…". Frente a esta situación, si aquellas grandes organizaciones que cuentan con recursos para fortalecer la seguridad informática se pueden preguntar: ¿Y qué ocurre con las medianas y pequeñas empresas (MiPymes) del país frente a la seguridad de su información?

Estas empresas se han ido consolidando como el motor central de la producción del país. Y, como consecuencia de ese posicionamiento, deben también ingresar a las nuevas plataformas de ventas para mejorar su productividad. Desde la construcción de sitios Web, con servicios de pagos en línea y catálogos de ventas hace que la mirada de los ciberdelincuentes se dirija hacia este tipo de organización. Asimismo, los costos asociados en la protección de datos, hace que dichas empresas, desistan de tener su propio sistema de seguridad. Plantear un modelo para la

implementación, implica no solo los recursos tecnológicos sino humanos que le garanticen a cualquier microempresario el aseguramiento de su información y la de sus clientes.

El problema de la seguridad no se resuelve únicamente con la adquisición de software de protección, sino a través de la concientización. Según Avilés (2013), esto implica el compromiso de cada empleado en el manejo de los datos y la implementación de políticas organizacionales estrictas. No obstante, Avilés y Larrañaga (2015) sostienen que hoy la formación debe iniciarse desde el hogar. Las consecuencias de una brecha de seguridad trascienden la pérdida de datos financieros o de clientes; pueden derivar en crisis económicas graves que provoquen la disminución de empleos o incluso el cierre de la empresa, un concepto de eventos de gran impacto analizado por Taleb (2008).

En la actualidad, la transformación digital y la creciente dependencia de la tecnología han impulsado a las micro, pequeñas y medianas empresas (MiPymes) a adoptar sistemas informáticos para mejorar su competitividad y eficiencia operativa. Sin embargo, muchas de estas empresas no cuentan con estrategias adecuadas de seguridad informática, lo que las hace vulnerables a ataques cibernéticos, pérdida de información, fraude y otras amenazas digitales.

Las MiPymes en Neiva, Huila, inscritas en la Cámara de Comercio, no son la excepción a esta problemática. La falta de recursos financieros, desconocimiento sobre normativas de ciberseguridad y la ausencia de políticas estructuradas para la protección de datos ponen en riesgo la continuidad operativa de estos negocios. Esto genera no solo pérdidas económicas, sino también una disminución en la confianza de sus clientes y socios comerciales.

Además, muchas de estas empresas no cuentan con un modelo de gestión adecuado para la implementación de sistemas de seguridad informática, lo que dificulta la planificación y ejecución de medidas preventivas y correctivas. En este contexto, se hace necesario diseñar un modelo

estructurado que permita a las MiPymes adoptar estrategias de seguridad informática alineadas con buenas prácticas y estándares internacionales, garantizando su protección ante amenazas cibernéticas y fortaleciendo su sostenibilidad en el mercado.

Pregunta de Investigación

¿Cómo desarrollar e implementar un modelo de seguridad informática aplicable de manera simultánea en múltiples MiPymes inscritas en la Cámara de Comercio del Huila, que les permita fortalecer su infraestructura tecnológica y minimizar los riesgos de ciberseguridad de forma eficiente, escalable y sostenible?

Planteamiento del Problema

En los últimos años, las MiPymes del departamento del Huila han avanzado en la adopción de tecnologías digitales como parte de sus procesos administrativos, comerciales y operativos. Este proceso de transformación digital, si bien ha traído consigo beneficios en términos de eficiencia y competitividad, también ha expuesto a estas organizaciones a nuevos riesgos relacionados con la seguridad de la información. A diferencia de las grandes empresas, las MiPymes carecen en muchos casos de políticas claras de ciberseguridad, personal capacitado y herramientas tecnológicas adecuadas para proteger sus activos digitales. Esta situación las convierte en un blanco vulnerable frente a amenazas como el robo de datos, ataques de Ransomware, suplantación de identidad y pérdida de información crítica.

Diversos estudios a nivel nacional e internacional han evidenciado que la ciberseguridad es una de las principales debilidades en el ecosistema de las pequeñas y medianas empresas. Según la Cámara Colombiana de Informática y Telecomunicaciones (CCIT, 2023), más del 60% de las MiPymes del país no cuentan con estrategias de protección digital definidas, y un 45% no identifica adecuadamente los riesgos a los que está expuesta su información. Esta carencia de una hoja de

ruta clara no solo compromete la integridad de sus datos, sino que pone en riesgo la continuidad del negocio ante incidentes de Ransomware o phishing. En este contexto, la falta de preparación reportada a nivel nacional se agudiza en regiones como el Huila, donde el acceso a consultoría especializada es limitado, validando la necesidad de un modelo ágil y de fácil implementación como el propuesto en este estudio. En el caso específico del Huila, investigaciones académicas y reportes institucionales (MinTIC, 2022; Cámara de Comercio del Huila, 2025) han señalado que, aunque existe un interés creciente por la transformación digital, la inversión en seguridad informática es limitada y no está alineada con la criticidad de los activos que manejan las empresas.

Adicionalmente, muchas de las metodologías tradicionales para implementar sistemas de seguridad informática requieren altos niveles de inversión y conocimientos técnicos especializados, lo que dificulta su adopción por parte de pequeñas empresas. En este sentido, surge la necesidad de explorar enfoques más flexibles, económicos y participativos, que permitan a las MiPymes avanzar de forma progresiva en la implementación de buenas prácticas de ciberseguridad. Una alternativa viable y prometedora es el uso de metodologías ágiles como SCRUM, ampliamente utilizadas en el desarrollo de software y gestión de proyectos, pero poco exploradas en el campo de la ciberseguridad en el contexto de MiPymes.

Frente a este escenario, se hace necesario desarrollar un modelo de ciberseguridad basado en SCRUM que responda a las características, necesidades y limitaciones de las MiPymes del Huila. Este modelo debe ser viable desde el punto de vista técnico y económico, fácilmente implementable con los recursos disponibles en las empresas locales, y escalable para adaptarse a diferentes niveles de madurez digital. De esta forma, se busca cerrar la brecha existente entre la necesidad de proteger la información y la capacidad real de estas organizaciones para hacerlo,

fortaleciendo su resiliencia frente a amenazas cibernéticas y mejorando su competitividad en un entorno cada vez más digitalizado.

Sistematización de la Experiencia

La sistematización de esta experiencia se fundamenta en la recolección, análisis y reflexión crítica sobre el proceso de diseño e implementación del modelo de ciberseguridad basado en SCRUM para MiPymes del Huila. Este ejercicio permitió identificar aprendizajes significativos, desafíos enfrentados y elementos clave que favorecen la replicabilidad del modelo en contextos similares.

Contexto de intervención

El trabajo se desarrolló con MiPymes ubicadas en distintas subregiones del departamento del Huila, pertenecientes a sectores como comercio, servicios, industria y agroindustria. Estas empresas, en su mayoría, carecían de políticas formales de ciberseguridad y presentaban bajo nivel de madurez digital, según lo evidenciado en los diagnósticos iniciales.

Proceso metodológico aplicado

A través de encuestas estructuradas y entrevistas semiestructuradas, se identificaron brechas comunes en prácticas de seguridad, uso de tecnologías y percepción del riesgo digital. Sobre esta base, se adaptaron los marcos NIST, ISO/IEC 27001 y C2M2 a las capacidades reales de las MiPymes, estructurando un modelo incremental y ágil soportado en SCRUM.

Se desarrollaron Sprints de trabajo con equipos interdisciplinarios dentro de las empresas, en los que se aplicaron dinámicas de priorización de riesgos, definición de historias de usuario relacionadas con la seguridad digital y generación de entregables viables (como políticas básicas, controles de acceso y planes de respuesta).

Resultados emergentes

Entre los principales logros se destacan:

- La apropiación gradual de conceptos clave de ciberseguridad por parte del personal de las MiPymes.
- La incorporación de rutinas de inspección y mejora continua, alineadas con los eventos de SCRUM.
- La formulación de un backlog común de acciones replicables en otras organizaciones similares.

Lecciones aprendidas

- La implementación de marcos ágiles requiere una fase previa de sensibilización y adaptación cultural en las empresas.
- La figura del Scrum Master fue clave no solo como facilitador técnico, sino como agente de cambio.
- La flexibilidad y modularidad del modelo fue fundamental para su aceptación y sostenibilidad.

Elementos de replicabilidad

La experiencia sistematizada permite definir una hoja de ruta para la aplicación del modelo en otras MiPymes de la región, considerando tres factores determinantes:

(1) acompañamiento técnico inicial,

(2) adaptación del lenguaje y herramientas a contextos no técnicos, y

(3) evaluación continua de madurez y riesgo.

Justificación

En el tercer trimestre de 2022, según la Cámara Colombiana de Informática y Telecomunicaciones (CITT), se registraron más de 54.000 ataques cibernéticos en Colombia. Este panorama, sumado a que el país ocupa el puesto 65 en el ranking global de ciberseguridad del National Cyber Security Index (NCSI), revela una alta vulnerabilidad frente a las amenazas digitales emergentes.

Las micro, pequeñas y medianas empresas (MiPymes), como actores clave de la economía nacional, enfrentan desafíos aún mayores debido a sus limitaciones tecnológicas y humanas, convirtiéndose en blancos frecuentes de los ciberdelincuentes. Se estima que el 60% de las pequeñas empresas que sufren un ciberataque grave cierran sus operaciones en menos de seis meses (Forbes, 2025), situación especialmente crítica en regiones como el Huila, donde muchas empresas presentan bajos niveles de digitalización.

Este proyecto propone un modelo de ciberseguridad adaptado a las MiPymes registradas en la Cámara de Comercio del Huila. A diferencia de enfoques tradicionales que requieren inversiones elevadas, este modelo incorpora medidas accesibles, escalables y sostenibles, inspiradas en estándares como el NIST Cybersecurity Framework y experiencias internacionales como Cyber Essentials del Reino Unido.

El modelo no se limita a la implementación tecnológica, sino que incorpora componentes estratégicos como la capacitación del talento humano y la creación de una cultura organizacional orientada a la seguridad. Según Alejandro Botter (2025), gerente de ingeniería de Checkpoint, el 80% de los incidentes de seguridad implican algún tipo de error humano, desde el uso de contraseñas débiles hasta la caída en trampas de phishing. La buena noticia es que, con educación y prevención, este riesgo puede reducirse significativamente.

Además de alinearse con buenas prácticas globales, el modelo propuesto cumple con normativas nacionales como la Ley 1581 de 2012 (protección de datos personales), la Ley 1273 de 2009 (delitos informáticos) y el CONPES 3701. Así, se contribuye a fortalecer la resiliencia digital del tejido empresarial regional, favoreciendo su competitividad en mercados cada vez más exigentes.

Este proyecto propone un modelo de ciberseguridad adaptado específicamente a las MiPymes registradas en la Cámara de Comercio de Neiva, Huila. A diferencia de otros enfoques que requieren inversiones significativas, este modelo considera las limitaciones de recursos de estas empresas, integrando medidas escalables y prácticas que son accesibles y sostenibles. Basado en estándares internacionales como el NIST Cybersecurity Framework y buenas prácticas como las implementadas por el programa Cyber Essentials en el Reino Unido, el modelo propuesto busca cerrar las brechas de seguridad sin comprometer la viabilidad operativa de las empresas.

Además, este modelo incorpora un enfoque integral que incluye no solo la implementación de tecnologías de protección, sino también la capacitación del personal y la creación de una cultura organizacional de ciberseguridad.

A nivel global, países como el Reino Unido han logrado reducir significativamente los incidentes cibernéticos en pequeñas empresas mediante la adopción de modelos básicos y escalables. Por otro lado, en América Latina, iniciativas en Brasil y México destacan por su enfoque adaptativo y progresivo, similar al propuesto en este proyecto. Este tipo de modelos, además de proteger los activos digitales de las empresas, mejora su competitividad en mercados internacionales al aumentar la confianza de sus clientes.

Para el departamento del Huila, este modelo representa una oportunidad de transformar las MiPymes en empresas resilientes frente a amenazas cibernéticas, contribuyendo al desarrollo económico y social. Las empresas con una infraestructura tecnológica más segura estarán mejor posicionadas para participar en la economía digital y garantizar la continuidad de sus operaciones.

El modelo propuesto también apoya el cumplimiento de normativas nacionales como la Ley 1581 de 2012 sobre protección de datos personales y la Ley 1273 de 2009 contra delitos informáticos. Además, se alinea con el CONPES 3701, que establece lineamientos para la ciberseguridad y ciberdefensa en Colombia, y con las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) para fortalecer la seguridad digital de las MiPymes.

En este escenario de creciente digitalización y riesgos cibernéticos, el diseño de un modelo de ciberseguridad adaptado para las MiPymes de Neiva, Huila, no solo es necesario sino estratégico. Este proyecto busca cerrar brechas de seguridad, aumentar la resiliencia de las empresas locales y fomentar una cultura de ciberseguridad que proteja sus activos digitales y fortalezca su competitividad en un entorno global cada vez más exigente. A largo plazo, se espera que este modelo se convierta en un referente replicable en otras regiones del país, contribuyendo al fortalecimiento de la ciberseguridad nacional.

Las MiPymes constituyen una parte esencial del desarrollo económico y social del departamento del Huila, aportando significativamente a la generación de empleo y a la dinamización de mercados locales. Sin embargo, su creciente dependencia de tecnologías digitales las expone a múltiples riesgos cibernéticos que pueden comprometer la confidencialidad, integridad y disponibilidad de su información. Pese a ello, muchas de estas organizaciones carecen

de estrategias de ciberseguridad adecuadas, debido a limitaciones presupuestarias, escasa capacitación técnica y desconocimiento de metodologías adaptables a su realidad.

Frente a este panorama, es urgente diseñar soluciones que respondan tanto a sus necesidades como a sus capacidades. El enfoque ágil, particularmente SCRUM, ha demostrado ser efectivo en contextos donde la adaptabilidad, la mejora continua y la colaboración son clave. Aplicado a la ciberseguridad, permite construir modelos que evolucionan en función del entorno, integran a los actores organizacionales y permiten escalar las soluciones conforme la empresa crece.

Desarrollar un modelo de ciberseguridad basado en SCRUM no solo responde a una necesidad técnica, sino también a una oportunidad estratégica de fortalecer la resiliencia digital de las MiPymes del Huila. Este enfoque facilita la apropiación de prácticas seguras, fomenta una cultura proactiva frente a los riesgos y ofrece una ruta viable y escalable para la transformación digital segura de estas organizaciones.

Objetivos

Objetivo General

Diseñar un modelo de ciberseguridad basado en SCRUM para las MiPymes del Huila, garantizando su viabilidad operativa y escalabilidad en el contexto regional.

Objetivos Específicos

Identificar y analizar las principales vulnerabilidades y necesidades en materia de ciberseguridad en las MiPymes del Huila.

Diseñar un marco metodológico de ciberseguridad apoyado en principios ágiles del marco SCRUM.

Implementar el modelo en empresas piloto para validar su funcionalidad y adaptabilidad.

Evaluar el impacto del modelo y realizar ajustes iterativos para optimizar su escalabilidad y sostenibilidad.

Marco de Referencia

Estado del Arte

El desarrollo de modelos de ciberseguridad para MiPymes ha sido ampliamente abordado en la literatura internacional, debido al creciente número de ataques dirigidos a este segmento empresarial. A continuación, se presentan los principales hallazgos sobre: (1) marcos de referencia aplicados en MiPymes, (2) metodologías ágiles en ciberseguridad, (3) modelos organizacionales adaptativos y (4) enfoques contextualizados para América Latina.

1. Aplicación de marcos de ciberseguridad en MiPymes

Diversas investigaciones han abordado la adaptación de marcos de referencia como el NIST Cybersecurity Framework y el ISO/IEC 27001 a entornos de MiPymes. Por ejemplo, estudios realizados por Ramírez & Ortiz (2021) y Sánchez et al. (2022) en América Latina han demostrado que, aunque estos estándares fueron concebidos para grandes empresas, su aplicación por etapas puede mejorar significativamente la postura de seguridad en organizaciones pequeñas. La implementación gradual de controles, priorizando activos críticos y riesgos prevalentes, ha resultado efectiva en países con limitaciones presupuestales similares a Colombia.

Asimismo, investigaciones como la de López-Guzmán et al. (2020) han validado el uso del modelo C2M2 como herramienta de diagnóstico en empresas de manufactura y servicios, permitiendo establecer planes de mejora alineados con su nivel de madurez.

2. Metodologías ágiles aplicadas a la ciberseguridad

El uso de SCRUM en proyectos de ciberseguridad ha ganado tracción en los últimos años. Según un estudio de Alshamrani et al. (2020), la integración de SCRUM con prácticas de seguridad permite responder rápidamente a incidentes, adaptarse a amenazas emergentes y

fomentar la cultura colaborativa en equipos multidisciplinarios. Esta tendencia ha sido reforzada por investigaciones como la de García-Morales y Rodríguez (2023), quienes propusieron un modelo híbrido SCRUM–DevSecOps para gestionar la seguridad en empresas de tecnología educativa en México, mostrando mejoras en la detección temprana de vulnerabilidades.

Otros trabajos, como el de Kumar & Singh (2021), resaltan que el enfoque ágil es especialmente útil en contextos de alta incertidumbre, donde los requerimientos de seguridad cambian constantemente. En este sentido, la flexibilidad de SCRUM se convierte en una ventaja para MiPymes que necesitan implementar soluciones adaptativas.

3. Modelos organizacionales y de cambio para MiPymes

La literatura reciente muestra un creciente interés por enfoques sistémicos y adaptativos en la gestión organizacional de la ciberseguridad. El Modelo de Sistemas Viables (VSM) ha sido aplicado con éxito en estudios de transformación digital en PYMEs en Chile y Perú (Martínez & Olivares, 2022), permitiendo construir estructuras resilientes ante amenazas del entorno. Por otro lado, investigaciones basadas en el modelo de cambio de Lewin han sido utilizadas para introducir prácticas seguras en MiPymes del sector salud, enfocándose en la resistencia al cambio como una barrera común. Bajo esta premisa, la adopción de prácticas de ciberseguridad en las MiPymes del Huila requiere no solo de la implementación de herramientas técnicas, sino de un proceso de 'descongelamiento' de hábitos inseguros, permitiendo que la cultura organizacional transite hacia un estado de 'recongelamiento' donde la seguridad sea una capacidad intrínseca y permanente en la gestión de sus procesos de negocio. El modelo que se propone está basado en SCRUM actúa como el Sistema 1 (Operación) y el Sistema 2 (Coordinación) del VSM, asegurando que la ciberseguridad no sea un evento aislado, sino una función vital de la supervivencia de la empresa.

En relación con la adopción tecnológica, estudios colombianos como el de Peña & Ramírez (2022) han demostrado la vigencia del modelo TAM, especialmente al analizar la percepción de los empleados frente a sistemas de control de acceso y autenticación. En el marco de este proyecto, la aplicación del modelo TAM es fundamental, ya que el éxito del marco SCRUM propuesto no depende solo de la configuración técnica de firewalls o antivirus, sino de la facilidad de uso percibida y la utilidad que los colaboradores de las MiPymes huilenses encuentren en las nuevas rutinas de seguridad sugeridas.

4. Enfoque regional y contexto colombiano

En Colombia, iniciativas como el Índice de Madurez Digital Empresarial (MinTIC, 2023) han revelado que muchas MiPymes del sector comercio y agroindustria en departamentos como el Huila presentan bajos niveles de digitalización, lo que las hace especialmente vulnerables. Además, proyectos piloto liderados por universidades regionales han explorado metodologías de sensibilización en ciberseguridad, como el desarrollado por la Universidad Surcolombiana (2021), con resultados positivos en términos de apropiación tecnológica. Estas iniciativas locales subrayan que la sensibilización es el primer paso, pero que se requiere un marco operativo — como el modelo SCRUM propuesto en esta investigación— para transformar esa conciencia en una gestión de seguridad diaria.

Investigaciones recientes de Rodríguez & Castaño (2024) evidencian que los modelos de innovación disruptiva adaptados a zonas rurales han tenido éxito al priorizar herramientas accesibles y bajo demanda, lo cual resulta relevante para el diseño de soluciones escalables y sostenibles. En este sentido, el presente estudio se apoya en los hallazgos de Rodríguez & Castaño (2024) para proponer un modelo que no solo sea técnicamente robusto, sino geográficamente pertinente para la ruralidad huilense.

Este estado del arte permite situar la propuesta en el contexto de investigaciones previas, identificando vacíos y oportunidades para desarrollar un modelo de ciberseguridad ágil, viable y escalable, alineado con las necesidades específicas de las MiPymes del Huila.

Marco Contextual

El presente estudio se enmarca en la problemática de la ciberseguridad en las micro, pequeñas y medianas empresas (MiPymes) del departamento del Huila, una región colombiana con fuerte vocación comercial, agrícola, agroindustrial y de servicios, en la que este tipo de organizaciones constituye el núcleo del tejido económico. Las MiPymes de la región aportan significativamente al empleo, la innovación y la competitividad, pero enfrentan graves desafíos en materia de seguridad digital, especialmente en un contexto de creciente digitalización y vulnerabilidad tecnológica.

En los últimos años, las MiPymes del Huila han iniciado procesos de transformación digital como parte de sus estrategias de modernización y adaptación a los mercados actuales. Sin embargo, estos avances no han ido acompañados de una implementación efectiva de políticas, tecnologías y prácticas de ciberseguridad, generando brechas críticas que las exponen a amenazas cibernéticas como programa maligno (Malware), Ransomware, suplantación de identidad, pérdida de información y ataques a su infraestructura informática.

La mayoría de estas organizaciones carecen de áreas especializadas en seguridad informática, de recursos económicos para contratar servicios externos o adquirir soluciones robustas, y de conocimiento normativo o técnico para prevenir o gestionar incidentes cibernéticos. Esta situación se ve agravada por la limitada oferta de acompañamiento institucional y la baja apropiación de marcos normativos como la Ley 1581 de 2012 (protección de datos personales) o el CONPES 3995 de 2020 (seguridad digital nacional).

En este contexto, el presente proyecto se desarrolla como una respuesta estratégica al déficit de capacidades en seguridad digital que enfrentan las MiPymes huilenses, proponiendo el diseño y validación de un modelo de ciberseguridad basado en la metodología ágil SCRUM, que permita a estas organizaciones avanzar de forma progresiva, flexible y sostenible en la protección de sus activos digitales.

El contexto regional también se caracteriza por niveles bajos de madurez digital, según lo evidenciado en estudios del MinTIC (2023) y diagnósticos realizados por la Cámara de Comercio del Huila, que revelan deficiencias en conectividad, automatización de procesos, formación en TIC y gestión de riesgos digitales. Aun así, existe una creciente conciencia por parte de los empresarios sobre la importancia de fortalecer sus capacidades digitales, lo que representa una oportunidad para la adopción de modelos adaptativos y escalables como el que se propone en esta investigación.

Por último, el modelo propuesto reconoce las particularidades culturales, organizacionales y económicas del Huila, por lo que incorpora enfoques participativos, herramientas accesibles y dinámicas de acompañamiento orientadas a fomentar la apropiación tecnológica, la sensibilización frente a los riesgos cibernéticos y la generación de valor a través de la seguridad digital.

De acuerdo con el informe de Estimación Potencial de comerciantes – 2024 (Camara de Comercio del Huila, 2025) y específicamente se ha tenido en cuenta las empresas formalizadas, se ha extraído los siguientes datos:

Caracterización de las empresas formales: 39.070 empresas (Jurídicas y personas naturales), con una participación porcentual de 18.19% las jurídicas y el 81.81% de la persona natural.

De acuerdo con: “Teniendo en cuenta la participación de cada sector según las unidades productivas, tal y como se observa en la Tabla 1, los tres sectores más representativos fueron:

Comercio al por mayor y al por menor; Vehículos (48,73%), seguido de Alojamiento y Servicios de Comida (14,11%) e Industrias manufactureras (8,74%). Por otro lado, los sectores con participación menor a 0,1%, fueron: Suministro de electricidad (0,09%), Administración pública y defensa; seguridad social (0,03%), Actividades de los hogares en calidad de empleadores (0,01%) y Actividades de organizaciones y entidades extraterritoriales (0,00%).”

Tabla 1

Sector Económico por Unidades Productivas del Tejido Empresarial 2024

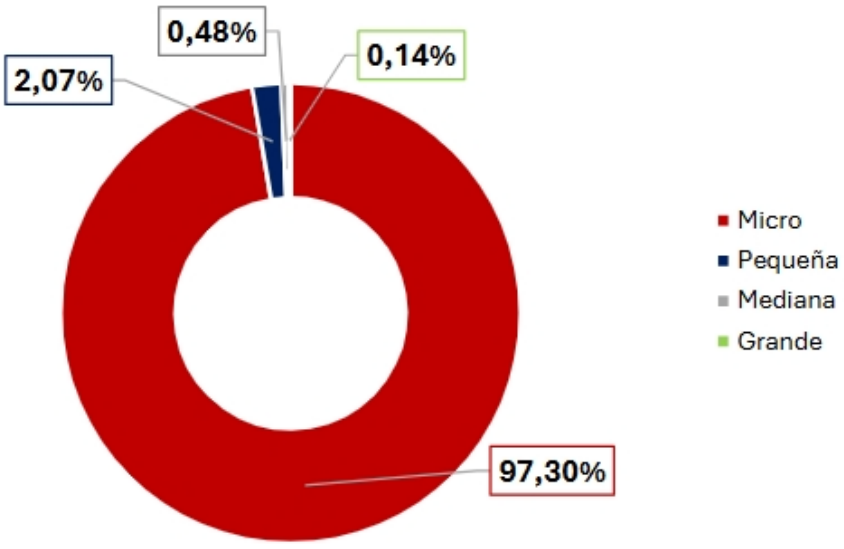
Sector Económico	No. De Empresas	% Part.
Comercio al por mayor y al por menor; Vehículos	19.040	48,73%
Alojamiento y Servicios de Comida	5.511	14,11%
Industria manufacturera	3.414	8,74%
Construcción	1.537	3,93%
Actividades profesionales, científicas y técnicas	1.499	3,84%
Actividades de servicios administrativos y de apoyo	1.235	3,16%
Transporte y Almacenamiento	1.018	2,61%
Otras actividades de servicio	1603	4,10%
Agricultura, ganadería, caza, silvicultura y pesca	865	2,21%
Información y Comunicaciones	661	1,69%
Actividades artísticas, de entretenimiento y recreación	894	2,29%
Actividades de atención de la salud humana y de asistencia social	544	1,39%
Educación	237	0,61%
Actividades inmobiliarias	360	0,92%
Actividades financieras y de seguros	326	0,83%
Distribución de agua, saneamiento ambiental	171	0,44%
Explotación de minas y canteras	104	0,27%
Suministro de electricidad, gas, vapor y aire acondicionado	36	0,09%
Administración pública y defensa; seguridad social	13	0,03%
Actividades de los hogares en calidad de empleadores	2	0,01%
Actividades de organizaciones y entidades extraterritoriales	0	0,00%
Total, general	**39.070**	**100,00%**

Nota. Esta tabla contiene los sectores económicos por unidades productivas del tejido empresarial 2024 con sus respectivos porcentajes de participación. Fuente: informe de Estimación Potencial de comerciantes – 2024, pg. 12.

Jurisdicción por tamaño: De acuerdo con el Decreto 957 de 2019 establece como criterio para su determinación: los ingresos por actividades ordinarias y el sector económico de que se trate (manufactura, servicios y comercio). Lo que determina que, en el departamento del Huila, la estructura empresarial está conformada en mayor medida por microempresas (97,3%), seguido de pequeñas (2,07%), medianas (0,48%) y grandes empresas (0,14%). Donde el segmento que interesa en este proyecto está centrado en las microempresas, pequeñas y medianas empresas, siendo el 99,85% de las empresas legalmente constituidas en el departamento del Huila.

Figura 1

Tamaño por unidades productivas del tejido empresarial 2024



Nota. En la figura se evidencia el tamaño por unidades productivas del tejido empresarial 2024 en el departamento del Huila. Fuente: ibidem.

Ubicación por zona: en la zona Norte se encuentra el 56,66% de las unidades productivas del departamento del Huila, seguido de la zona Sur con el 23,59%; en la zona Centro se concentra el 12,75% y en el Occidente el 7%. Por lo que se determina, realizar este trabajo solamente en la zona norte del departamento donde está ubicada la ciudad capital: Neiva. En la cual está ubicada el 75.19% de las empresas formales de la zona geográfica. Para nuestro caso: 22.137 empresas. Luego, se tiene que las empresas en el rango de micros a medianas corresponden 22.104 empresas. Y su estratificación se realizará de acuerdo con los porcentajes ajustados detallados en la jurisdicción por tamaño.

Marco Teórico

1. Ciberseguridad en MiPymes

Las micro, pequeñas y medianas empresas (MiPymes), por su estructura operativa y limitaciones presupuestarias, enfrentan desafíos importantes en materia de ciberseguridad. La falta de personal especializado, el desconocimiento normativo y la baja inversión en tecnologías de protección las hace especialmente vulnerables (NIST, 2024).

La ciberseguridad se define como el conjunto de prácticas, tecnologías y procesos orientados a proteger sistemas, redes y datos digitales frente a accesos no autorizados o incidentes maliciosos, tanto internos como externos.

Entre los marcos relevantes para abordar esta problemática se destaca el Cybersecurity Capability Maturity Model (C2M2) del Departamento de Energía de EE.UU. (DOE, 2021), que permite diagnosticar y mejorar progresivamente las capacidades de ciberseguridad mediante niveles de madurez.

Por su parte, el The NIST Cybersecurity Framework (CSF) 2.0 (NIST, 2024) ofrece un enfoque estructurado en cinco funciones: identificar, proteger, detectar, responder y recuperar. Su carácter modular permite una implementación gradual y adaptada al tamaño y capacidades de cada empresa.

Las normas ISO/IEC 27001 y 27002 (ISO, 2013) proporcionan directrices específicas para la gestión de la seguridad de la información. Aunque su implementación total puede resultar onerosa para las MiPymes, su adopción por fases representa una alternativa viable.

Desde una perspectiva económica, el modelo de Gordon y Loeb (2002) plantea un enfoque para evaluar el equilibrio entre la inversión en ciberseguridad y la reducción del riesgo esperado, lo cual resulta esencial en contextos con recursos limitados.

Adicionalmente, la teoría de la resiliencia organizacional (Hollnagel, 2011) enfatiza la necesidad de desarrollar capacidades no solo preventivas, sino también adaptativas y de aprendizaje ante incidentes. Este enfoque es particularmente útil al integrarse con marcos ágiles como SCRUM, que favorecen la adaptación continua.

2. Metodologías Ágiles y SCRUM

SCRUM es un marco de trabajo ágil orientado a la gestión de proyectos complejos en entornos dinámicos. Se estructura en iteraciones denominadas sprints, y se fundamenta en los principios de transparencia, inspección y adaptación. Sus roles clave (Scrum Master, Product Owner y equipo de desarrollo), artefactos (Product Backlog, Sprint Backlog, Incremento) y eventos (Daily Scrum, Sprint Planning, Review y Retrospective) permiten gestionar el progreso de forma estructurada y adaptable (Schwaber & Sutherland, 2020).

La aplicabilidad de SCRUM a proyectos de ciberseguridad se sustenta en el Cynefin Framework (Snowden & Boone, 2007), que clasifica los contextos organizacionales en simples,

complicados, complejos y caóticos. La ciberseguridad, al ubicarse frecuentemente en dominios complejos, requiere soluciones adaptativas y colaborativas, características inherentes a SCRUM.

El enfoque DevSecOps, promovido por OWASP (s.f.), extiende los principios de SCRUM al integrar la seguridad en cada fase del desarrollo, fomentando la cooperación entre los equipos de desarrollo, operaciones y seguridad. Si bien DevSecOps es común en desarrollo de software, su filosofía puede extrapolarse a la implementación de controles de seguridad en procesos organizacionales.

En contextos donde se busca escalabilidad del modelo, el Scaled Agile Framework (SAFe) aporta lineamientos y prácticas para aplicar principios ágiles en múltiples niveles organizacionales, lo cual es relevante para replicar el modelo en distintas MiPymes (SAFe, s.f.).

3. Diseño e Implementación de Modelos Organizacionales Viables

Para garantizar la viabilidad organizacional del modelo propuesto, es indispensable considerar elementos estructurales, culturales y de gestión del cambio. En esta línea, el Modelo de Sistemas Viables (VSM) de Stafford Beer (1979) proporciona un enfoque sistémico que permite analizar las condiciones de sostenibilidad y adaptabilidad de una organización frente a su entorno.

Complementariamente, la Teoría de Aceptación Tecnológica (TAM) introducido por Fred D. Davis en el año 1986 y citado en el documento: “User Acceptance of Computer Technology: A Comparison of Two Theoretical Models” (Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. 2022) cuyo objetivo es “proporcionar una explicación de los determinantes de la aceptación de la computadora que sea general, capaz de explicar el comportamiento del usuario a lo largo de una amplia gama de tecnologías informáticas de usuario final y de poblaciones de usuarios, al mismo tiempo que sea parsimoniosa y teóricamente justificada”. Lo cual ayuda a

comprender los factores que influyen en la adopción de nuevas tecnologías. Según esta teoría, la utilidad percibida y la facilidad de uso son determinantes en la intención de adopción de herramientas tecnológicas por parte de los empleados.

Para facilitar el proceso de transformación organizacional, se incorpora el modelo de cambio de Lewin (1951), que se estructura en tres etapas: descongelar, cambiar y recongelar. Esta secuencia permite gestionar la transición cultural hacia una organización con conciencia y prácticas de seguridad fortalecidas.

4. Viabilidad y Escalabilidad en el Contexto Regional

En el departamento del Huila, la implementación del modelo debe considerar particularidades sociales, económicas y tecnológicas. Desde la perspectiva de la Resource-Based View (RBV), la ventaja competitiva sostenible se alcanza a través del desarrollo y aprovechamiento de recursos y capacidades internas (Barney, 1991). Esto implica identificar recursos clave en las MiPymes locales y fortalecerlos mediante el modelo de ciberseguridad propuesto.

Para la validación empresarial, se recurre al Business Model Canvas adaptado a MiPymes tecnológicas, el cual permite visualizar componentes clave como propuesta de valor, canales, relaciones con clientes, actividades clave y estructura de costos (Osterwalder & Pigneur, 2010).

Además, la teoría de la innovación disruptiva (Christensen, 2011) sustenta la necesidad de introducir soluciones progresivas y accesibles en entornos con bajo grado de tecnificación, como el que presentan muchas MiPymes del Huila.

Por último, el Índice de Madurez Digital Empresarial para Colombia (MinTIC, 2021) ofrece indicadores sobre el estado de digitalización de las MiPymes, sirviendo como guía para ajustar el modelo a las condiciones reales del entorno y orientar su escalabilidad.

Marco Conceptual

El marco conceptual establece los fundamentos clave que sustentan la comprensión del proyecto, articulando los términos, categorías y relaciones que conforman el eje central de la investigación. A continuación, se definen y relacionan los conceptos esenciales para el desarrollo del modelo de ciberseguridad basado en SCRUM en el contexto de las MiPymes del Huila.

MiPymes (Micro, Pequeñas y Medianas Empresas)

Son organizaciones que, por su tamaño, recursos y estructura operativa, enfrentan limitaciones particulares en el acceso a tecnologías avanzadas, personal calificado y medidas de protección digital. En Colombia, se definen según la Ley 590 de 2000 y el Decreto 957 de 2019, considerando criterios como el número de empleados y el valor de los activos. Estas empresas representan más del 90% del tejido empresarial nacional y son vitales para la economía regional del Huila.

2. Ciberseguridad

Se refiere al conjunto de políticas, procedimientos, herramientas y prácticas diseñadas para proteger los activos digitales (información, sistemas y redes) frente a accesos no autorizados, ataques, daños o pérdida de información. En el contexto de las MiPymes, la ciberseguridad es una necesidad crítica dada su creciente digitalización y su vulnerabilidad ante amenazas como el Ransomware, phishing, y ataques de día cero.

3. Gestión Ágil de Proyectos

Es un enfoque de gestión que promueve la adaptabilidad, la colaboración constante con el cliente, la entrega iterativa de valor y la respuesta rápida al cambio. Se fundamenta en el Manifiesto Ágil (2001) y se aplica ampliamente en el desarrollo de software y transformación

organizacional. En entornos con recursos limitados como las MiPymes, la gestión ágil representa una alternativa eficiente y flexible para implementar soluciones progresivas.

4. SCRUM

SCRUM es un marco de trabajo ágil que organiza el desarrollo de productos complejos mediante ciclos iterativos denominados Sprints. Su estructura comprende roles definidos (Product Owner, Scrum Máster, Equipo de Desarrollo), artefactos (Product Backlog, Sprint Backlog, Incremento) y eventos (Sprint Planning, Daily Scrum, Sprint Review, Sprint Retrospective). Aplicado a la ciberseguridad, SCRUM permite abordar desafíos de manera incremental, fomentando la mejora continua y la apropiación organizacional de buenas prácticas de protección.

5. Modelo de Ciberseguridad basado en SCRUM

Se refiere a la propuesta metodológica que integra principios del marco SCRUM con las necesidades de protección digital en MiPymes. Este modelo considera la priorización dinámica de riesgos, la entrega incremental de soluciones de seguridad, la formación continua del personal, y la documentación colaborativa, con el objetivo de crear un entorno adaptable y escalable.

6. Viabilidad

Hace referencia a la posibilidad real de implementar el modelo propuesto en las condiciones actuales de las MiPymes del Huila, considerando aspectos técnicos, humanos y financieros. La viabilidad implica que el modelo sea comprensible, utilizable y mantenible en el tiempo, sin representar una carga excesiva para las capacidades operativas de las empresas.

7. Escalabilidad

Se entiende como la capacidad del modelo para adaptarse a distintos niveles de madurez digital y tamaños empresariales, permitiendo su réplica en diversas MiPymes. Un modelo escalable puede extenderse a otras regiones y sectores sin perder su funcionalidad ni su efectividad.

8. Madurez Digital

Es el grado en que una organización ha integrado herramientas tecnológicas en sus procesos internos y externos. La madurez digital condiciona la implementación de estrategias de ciberseguridad, ya que define el punto de partida y el ritmo de adopción de medidas protectoras.

9. Gestión del Cambio

Proceso sistemático de transformación organizacional que permite a las empresas adaptarse a nuevas metodologías, tecnologías o estructuras. En este proyecto, la gestión del cambio es clave para la adopción del modelo SCRUM y la creación de una cultura organizacional orientada a la seguridad digital.

Marco Legal en Ciberseguridad para MiPymes en Colombia

La ciberseguridad en Colombia está regulada por un conjunto de normativas, políticas públicas y lineamientos internacionales que buscan garantizar la protección de la información digital, la infraestructura crítica y los derechos fundamentales de los ciudadanos y organizaciones. Para las MiPymes, conocer y aplicar estas disposiciones es clave para el cumplimiento normativo y la gestión del riesgo.

Ley 1273 de 2009 – Delitos Informáticos

Esta ley modifica el Código Penal Colombiano y tipifica los delitos relacionados con la integridad, confidencialidad y disponibilidad de los sistemas informáticos y la información.

Entre los delitos contemplados se incluyen el acceso no autorizado, interceptación ilícita, daño informático y uso indebido de datos personales. Su aplicación es fundamental para definir responsabilidades legales ante incidentes de ciberseguridad.

Ley 1581 de 2012 – Protección de Datos Personales

Establece disposiciones generales para la protección de datos personales y regula su recolección, almacenamiento, uso y circulación. Obliga a las organizaciones, incluyendo MiPymes, a implementar políticas de tratamiento de datos y medidas de seguridad. Es supervisada por la Superintendencia de Industria y Comercio (SIC).

Decreto 1377 de 2013

Reglamenta parcialmente la Ley 1581 y establece condiciones para el consentimiento del titular de los datos personales, así como para el tratamiento de bases de datos existentes antes de la entrada en vigor de la ley.

Ley 1621 de 2013 – Ley de Inteligencia y Contrainteligencia

Aunque enfocada en organismos del Estado, establece lineamientos sobre el uso de tecnologías de información en procesos de inteligencia, lo que influye en la definición de límites legales en la vigilancia y monitoreo digital, relevantes para procesos de ciberseguridad.

CONPES 3701 de 2011 y CONPES 3995 de 2020

Estos documentos del Consejo Nacional de Política Económica y Social establecen la política nacional de seguridad digital. El CONPES 3995 en particular propone una visión para fortalecer la confianza digital, fomentar la cooperación público-privada y establecer un marco de gobernanza en ciberseguridad, incluyendo la participación de las MiPymes.

Ley 1341 de 2009 (modificada por la Ley 1978 de 2019)

Regula el desarrollo de las tecnologías de la información y las comunicaciones (TIC), promoviendo el acceso universal y el uso eficiente de estas. Incluye obligaciones de seguridad en la prestación de servicios digitales y establece funciones del Ministerio TIC en el ámbito de la ciberseguridad.

Estándares Internacionales (ISO/IEC 27001 y 27002)

Aunque de adopción voluntaria, estas normas ofrecen un marco reconocido internacionalmente para implementar sistemas de gestión de seguridad de la información (SGSI). Son recomendadas por el Ministerio TIC como parte de las buenas prácticas para empresas que manejan información crítica.

Marco Nacional de Referencia de Ciberseguridad y Ciberdefensa (2016)

Desarrollado por el MinDefensa, establece un enfoque integral para fortalecer la resiliencia digital del país. Incluye acciones específicas para el sector privado y promueve la colaboración entre entidades estatales y empresas, incluyendo MiPymes.

Resolución 2564 de 2020 del MinTIC

Establece lineamientos técnicos para la implementación del Modelo de Seguridad y Privacidad de la Información en entidades públicas, pero sugiere prácticas aplicables también a MiPymes que interactúan con el Estado o que buscan adoptar estándares de seguridad similares.

Circular Externa 01 de 2016 de la SIC

Orienta a las organizaciones sobre las medidas mínimas necesarias para el tratamiento seguro de datos personales, en cumplimiento con la Ley 1581. Representa una guía práctica para la implementación de controles básicos en MiPymes.

Metodología

En este capítulo se describe detalladamente el enfoque metodológico, el tipo de estudio y los procedimientos de recolección de datos empleados en la investigación. La metodología se estructura de acuerdo con estándares académicos, abarcando el método utilizado, el tipo de estudio realizado y las técnicas de recolección de datos aplicadas, todo ello conforme a las normas APA y con la coherencia propia de un capítulo metodológico formal.

Método

El presente estudio adopta un enfoque metodológico mixto de tipo descriptivo, con un diseño no experimental y de corte transeccional, ya que los datos se recolectarán en un único momento temporal. La investigación se centra en las MiPymes legalmente constituidas del departamento del Huila, donde, según la Cámara de Comercio del Huila (2023), operan aproximadamente 9.800 empresas activas.

Tipo de Estudio

Este trabajo corresponde a una investigación aplicada, orientada a resolver un problema práctico (mejorar la ciberseguridad en MiPymes mediante un modelo basado en Scrum) más que a generar teoría pura. En cuanto al alcance, el estudio es principalmente descriptivo, con matices exploratorios. Inicialmente, se busca diagnosticar y describir la situación actual de la ciberseguridad en las MiPymes del Huila –por ejemplo, identificar qué medidas de seguridad utilizan, nivel de madurez digital, familiaridad con Scrum y con marcos de ciberseguridad como NIST, etc.– para tener un panorama claro del contexto. Asimismo, el componente exploratorio que permita indagar aspectos cualitativos poco documentados (como las percepciones de los empresarios sobre la seguridad informática y la viabilidad de Scrum en ese ámbito).

La metodología se basa en las siguientes estrategias y fases:

1. Evaluar el impacto del modelo y realizar ajustes iterativos para optimizar su escalabilidad y sostenibilidad.

Fases del Estudio

Diagnóstico Inicial

Identificar y analizar las principales vulnerabilidades y necesidades en materia de ciberseguridad en las MiPymes del Huila.

Se realizará un estudio de campo con entrevistas semiestructuradas a directivos y empleados de MiPymes, complementado con encuestas de percepción sobre ciberseguridad. También se aplicarán auditorías técnicas a infraestructuras digitales para detectar vulnerabilidades y brechas de seguridad. Los datos recopilados se analizarán utilizando técnicas de minería de datos y análisis cualitativo.

Para lo cual se determinará la muestra de la población de acuerdo con:

Población y Muestra

La muestra se conformará a partir de una selección representativa de MiPymes clasificadas según su nivel de madurez digital y exposición a riesgos cibernéticos. Se incluirán sectores como comercio, servicios, manufactura y agroindustria.

Se empleará un muestreo estratificado, segmentado por subregiones del Huila (norte, centro, sur y occidente) y por sector económico. El tamaño de la muestra se calculará con un nivel de confianza del 95% y un margen de error del 5%, aplicando la fórmula de proporciones para poblaciones finitas.

Donde: N es la población (22.104), Z corresponde al valor z (1.96), p es la probabilidad de éxito (0.5), q = 1 – p (0.5), y e representa el margen de error (0.05).

Para la muestra, se utilizará un muestreo estratificado por subregiones (norte, centro, sur y occidente) y por sector económico (comercio, servicios, industria y agroindustria). El cálculo de la muestra se realizará con un nivel de confianza del 95% y un margen de error del 5%, utilizando la fórmula de proporciones para poblaciones finitas:

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

Donde:

N: población (9800)

Z: valor z (1.96)

p: probabilidad de éxito (0.5)

q: 1 – p (0.5)

e: margen de error (0.05)

Se aplicarán evaluaciones técnicas utilizando herramientas de análisis de riesgos y pruebas de penetración en sistemas de información.

- Encuesta estructurada a representantes de MiPymes (formato validado por juicio de expertos y prueba piloto con Alfa de Cronbach > 0.7). Ver el Apéndice A de este trabajo.
- Entrevistas semiestructuradas a expertos en ciberseguridad y metodologías ágiles.

Análisis de datos:

- Cuantitativo: análisis estadístico descriptivo e inferencial con R, o SPSS (frecuencias, medias, ANOVA).
- Cualitativo: análisis de contenido con codificación abierta y axial en NVivo.

Esta metodología permitirá validar la pertinencia, viabilidad y escalabilidad del modelo de ciberseguridad basado en SCRUM.

Diseño del Modelo

Diseñar un marco metodológico de ciberseguridad apoyado en principios ágiles del marco SCRUM.

Se elaborará un marco de seguridad basado en SCRUM, estableciendo roles, artefactos y eventos clave para su implementación. Se definirán requisitos funcionales y no funcionales mediante el uso de un backlog de seguridad, priorizando historias de usuario según los riesgos identificados en la fase de diagnóstico. Además, se diseñará un plan de capacitación para los empleados de las MiPymes en ciberseguridad básica.

En este caso, se utilizará Scrum para estructurar la implementación del modelo de seguridad informática en las MiPymes, asegurando flexibilidad, adaptabilidad y entregas continuas de valor.

Implementación Piloto

Implementar el modelo en empresas piloto para validar su funcionalidad y adaptabilidad. Se ejecutará el modelo en un grupo de MiPymes seleccionadas, siguiendo ciclos iterativos de desarrollo y evaluación tratadas en el punto anterior. Se implementarán herramientas de protección como firewalls, sistemas de detección de intrusos y cifrado de datos. Además, se realizarán simulaciones de ciberataques para medir la efectividad del modelo y ajustar su implementación según los resultados obtenidos. Se capacitará al personal en la adopción de prácticas seguras y se realizarán pruebas de funcionamiento bajo distintos escenarios de ciberataques simulados.

Evaluación y Mejora

Se establecerán indicadores clave de desempeño (KPIs) para medir la efectividad del modelo, incluyendo reducción de incidentes de seguridad, tiempo de respuesta a amenazas y

nivel de adopción por parte de las empresas. Se recogerá retroalimentación de los usuarios a través de encuestas y focus groups, con el fin de realizar mejoras continuas. Finalmente, se documentarán lecciones aprendidas y recomendaciones para la escalabilidad del modelo en otras MiPymes. Se recogerán retroalimentaciones de los usuarios para refinar el modelo, ajustando las estrategias de protección y mejorando la efectividad del sistema. Se documentarán las mejoras y recomendaciones para su replicabilidad en otras empresas.

Desarrollo de Objetivos

Con el fin de realizar una explicación detallada de todo el desarrollo del proyecto se retoma lo planteado en al apartado de la Metodología del proyecto que permite evidenciar con claridad cada uno de los resultados.

Primer Resultado: Identificar y analizar las principales vulnerabilidades y necesidades en materia de ciberseguridad en las MiPymes del Huila.

La investigación adoptó un enfoque metodológico mixto, combinando enfoques cuantitativo y cualitativo. Este método mixto integra elementos de ambas metodologías con el fin de aprovechar sus fortalezas y obtener una comprensión más completa del fenómeno estudiado. En lugar de basarse exclusivamente en datos numéricos o en observaciones cualitativas, el enfoque mixto permite triangular información y profundizar en el análisis: cuantificar aspectos clave y a la vez entender el contexto y las percepciones subyacentes.

De esta manera, se logra una visión integral de la problemática de ciberseguridad en las MiPymes, capturando tanto estadísticas objetivas como perspectivas y experiencias de los participantes. En la práctica, el estudio combinó técnicas de recolección cuantitativas y cualitativas de forma complementaria. Por un lado, se obtuvieron datos numéricos mediante encuestas estructuradas aplicadas a una muestra de empresas, lo que proporcionó mediciones estandarizadas sobre el estado de la ciberseguridad en las organizaciones.

Por otro lado, se realizaron entrevistas en profundidad y observaciones de campo, generando información cualitativa valiosa sobre prácticas, desafíos y contextos particulares no evidentes en los datos cuantitativos. La triangulación de datos –esto es, la comparación y contraste de resultados de múltiples fuentes– fue fundamental para validar y enriquecer la comprensión del fenómeno. Gracias a esta integración de métodos, fue posible corroborar hallazgos, incrementar la

validez de los resultados y elaborar un modelo de ciberseguridad más sólido y contextualizado a partir de la realidad observada en las MiPymes del Huila.

La combinación de estos métodos facilitó la validación del modelo en condiciones reales, incorporando la retroalimentación de los actores involucrados y adaptando sus componentes a la diversidad de escenarios presentes en el tejido empresarial del Huila.

Los hallazgos descriptivos sirvieron de base para el diseño del modelo propuesto, lo que confirma el carácter aplicado de la investigación al traducir el conocimiento obtenido en una solución práctica. Metodológicamente, el estudio se catalogó como no experimental y de diseño transeccional (transversal). Es una investigación no experimental porque no se manipularon deliberadamente variables independientes ni se aplicó un tratamiento controlado a un grupo de estudio.

En otras palabras, no se creó una situación artificial de intervención; más bien, se observaron y recolectaron datos de la realidad tal como se presentan en el entorno natural de las empresas, sin introducir cambios. Además, el diseño es transeccional o transversal dado que los datos se recolectaron en un solo momento en el tiempo. Todas las mediciones (encuestas, entrevistas y observaciones) corresponden a un corte único, ofreciendo una “fotografía” de la situación de ciberseguridad en las MiPymes del Huila en el periodo en que se realizó el estudio.

Este diseño transversal es adecuado para describir variables y analizar su incidencia en un momento dado, acorde con los objetivos descriptivos planteados. Cabe señalar que, al no existir manipulación de variables ni grupos de control, el estudio no busca establecer relaciones causales definitivas, sino caracterizar el estado actual e identificar posibles relaciones o patrones existentes de forma natural (por ejemplo, si las empresas más grandes presentan mayor madurez digital, o si

ciertos sectores económicos están más rezagados en ciberseguridad, etc.), sirviendo esto de insumo para la propuesta del modelo.

Para recopilar la información necesaria, se llevó a cabo un proceso sistemático de recolección de datos que incluyó la definición de la población y muestra de estudio, la selección de un método de muestreo apropiado, el cálculo del tamaño muestral, y la aplicación de diversos instrumentos (encuestas, entrevistas y observación) coherentes con el enfoque mixto adoptado. A continuación, se detalla cada uno de estos aspectos:

La población objetivo del estudio estuvo conformada por las micro, pequeñas y medianas empresas (MiPymes) del departamento del Huila, Colombia, activas en distintos sectores económicos. De acuerdo con los registros de cámaras de comercio y fuentes oficiales, las MiPymes representan la gran mayoría del tejido empresarial de la región. Dada la amplitud de esta población y su heterogeneidad en términos de ubicación y actividad económica, se decidió emplear un muestreo probabilístico estratificado.

El muestreo estratificado consiste en dividir la población en subgrupos homogéneos o estratos antes de seleccionar la muestra. En este caso, se definieron dos criterios de estratificación: subregión geográfica y sector económico. Es decir, primero se agruparon las empresas por su ubicación en las subregiones administrativas del Huila (Norte, Centro, Occidente y Sur) y luego por el sector económico al que pertenecen (por ejemplo: agroindustria, comercio, servicios y manufactura, entre otros).

De cada estrato resultante (ejemplo: empresas del sector comercio en la subregión Norte, empresas manufactureras en la subregión Sur, etc.), se seleccionaron aleatoriamente algunas empresas para incluir en la muestra. Este procedimiento garantizó que la muestra incluyera proporcionalmente empresas de todas las subregiones del departamento y de los diversos sectores

económicos relevantes, asegurando una representación más equilibrada y evitando sesgos hacia alguna zona o actividad particular del Huila. Para determinar el tamaño de la muestra, se aplicó la fórmula estadística para poblaciones finitas, considerando los parámetros habituales de confianza y precisión.

En términos generales, dicha fórmula incorpora: el tamaño de la población (N), el nivel de confianza deseado (reflejado en un valor Z de la distribución normal, por ejemplo 1.96 para 95% de confianza), la proporción esperada de ocurrencia del fenómeno (p, si se desconoce se asume p = 0.5 para maximizar la variabilidad), su complemento q = 1–p, y el error muestral tolerado (e). Bajo este esquema, asumiendo un nivel de confianza del 95% (Z = 1.96), una proporción esperada p = 0.5 (máxima incertidumbre) y un margen de error aceptado en torno al 15% (e = 0.15), el cálculo arrojó que se requería encuestar del orden de 20 a 40 empresas, aproximadamente.

En consecuencia, se estableció una muestra mínima objetivo de 30 MiPymes representativas distribuidas entre los distintos estratos. Finalmente, durante el trabajo de campo se logró recoger información completa de 20 empresas, cantidad que cumple con lo estimado y refuerza la confiabilidad de los datos obtenidos. Esta muestra, aunque numéricamente moderada, resulta suficiente para los fines descriptivos y exploratorios del estudio, dado que proporciona datos de múltiples contextos locales y sectores, alineados con la estrategia de muestreo estratificado planteada.

A partir de la Tabla 1 y de acuerdo con el cálculo realizado en el párrafo anterior, se determinó que el número de empresas para el estudio es de 20. El primer ejercicio fue determinar por Sector Económico para todo el departamento y la estimación de las empresas y luego para cada zona. Los resultados se observan en la Tabla 2.

Tabla 2.

Estratificación por Sector económico / % participación

Sector Económico	% Part.	No. Empresas
Comercio al por mayor y menor; Vehículos	48,73%	10
Alojamiento y Servicios de Comida	14,11%	2
Industria manufacturera	8,74%	2
Otras actividades de servicio	4,10%	1
Construcción	3,93%	1
Actividades profesionales, científicas y técnicas	3,84%	1
Agropecuario/Pesca	2,21%	1
Otros (Suma de sectores menores al 3.5%)	14,34%	2
TOTAL	100%	20

Nota: La Tabla muestra la distribución de las 20 empresas analizadas por sector económico. Se observa una alta concentración en el comercio (48,73%; 10 empresas), seguido por alojamiento y servicios de comida (14,11%; 2). Los demás sectores presentan participaciones menores, lo que evidencia una muestra diversa, pero con predominio del sector comercial.

La distribución de empresas por zona se describe en la Tabla 3.

Tabla 3.

Zona / % participación

Zona	% Part.	No. Empresas
Zona Norte (Neiva y alrededores)	56,66%	11
Zona Sur (Pitalito y alrededores)	23,59%	5
Centro (Garzón y alrededores)	12,75%	3
Occidente (La Plata y alrededores)	7,00%	1
TOTAL	100%	20

Nota: La Tabla presenta la distribución geográfica de las 20 empresas incluidas en el estudio. Predomina la Zona Norte (Neiva y alrededores) con el 56,66% (11 empresas), seguida por la Zona Sur (23,59%; 5). El Centro aporta 12,75% (3) y Occidente 7,00% (1), evidenciando mayor concentración en el norte del departamento.

Finalmente, se ajustó la distribución de empresas teniendo en cuenta los tiempos y las distancias para poder cumplir con el cálculo de la estratificación. Dano como resultado la Tabla 4.

Tabla 4.

Distribución final

Zona	% Part.	No. Empresas
Zona Norte (Neiva y alrededores)	56,66%	15
Zona Sur (Pitalito y alrededores)	23,59%	3
Centro (Garzón y alrededores)	12,75%	1
Occidente (La Plata y alrededores)	7,00%	1
TOTAL	100%	20

Nota: La Tabla muestra la distribución final de las 20 empresas por zona. Se mantiene el predominio de la Zona Norte (Neiva y alrededores) con 56,66% (15 empresas), seguida por la Zona Sur con 23,59% (3). El Centro y Occidente registran participaciones menores (1 empresa cada uno), indicando una concentración más marcada en el norte.

Las consideraciones fueron:

- Consideración de Ciberseguridad: Dado que el sector "Comercio" domina el 48% de la muestra, tu estudio tendrá un fuerte enfoque en e-commerce, pasarelas de pago y protección de datos de clientes finales.

- El Huila es el principal productor de café y piscicultura en Colombia, y estos procesos están cada vez más tecnificados. Por ello, se incluyó una empresa del sector ganadero y una empresa del sector caficultor.
- La Zona Norte, es el motor económico del departamento.
- En Comercio (15 empresas): Neiva tiene centros comerciales y grandes distribuidoras. Incluyendo 2 empresas que con venta en línea (e-commerce), ya que son las de mayor riesgo cibernético.
- En Servicios de Comida (3 empresas): Restaurantes o hoteles que manejen reservas digitales y bases de datos de clientes, pues el cumplimiento de la Ley de Protección de Datos (Habeas Data) es un punto crítico de ciberseguridad aquí.
- En el sector "Otros" (1 empresa): Dado el interés previo, se trabaja con una Entidad de Salud en Neiva, que manejan información altamente sensible (historias clínicas).
- En Industria (3 empresas totales): Estas empresas suelen tener riesgos en la banca en línea (pagos a proveedores y nómina), lo cual es un blanco frecuente de phishing.

Se utilizaron tres técnicas principales de recolección de datos acordes con el enfoque mixto: la encuesta (método cuantitativo), la entrevista (método cualitativo) y la observación directa (método cualitativo complementario). A continuación, se describe cada instrumento y su aplicación:

Para la fase diagnóstica se aplicó una encuesta estructurada a una muestra representativa de MiPymes del Huila, seleccionadas mediante muestreo estratificado por subregión y sector económico. La encuesta, validada por juicio de expertos y con un alfa de Cronbach de 0.86, abordó

dimensiones como infraestructura tecnológica, prácticas de seguridad, conocimiento de marcos normativos, uso de metodologías ágiles y disposición al cambio.

Complementariamente, se realizaron entrevistas semiestructuradas a expertos en ciberseguridad y metodologías ágiles, así como observaciones no participantes en las empresas piloto, documentando prácticas cotidianas y rutinas digitales. Estas herramientas permitieron triangular los datos y obtener una visión integral del contexto organizacional.

Encuestas estructuradas: Se diseñó y aplicó un cuestionario estructurado dirigido a los representantes (gerentes, propietarios o encargados de TI) de las MiPymes seleccionadas. La encuesta estuvo conformada por una serie de preguntas cerradas y escalas de evaluación que abarcaron los aspectos clave de ciberseguridad y gestión ágil en las empresas.

Por ejemplo, se incluyeron ítems para medir la existencia de medidas de protección (uso de antivirus, políticas de contraseñas seguras, realización de copias de respaldo de la información, etc.), el nivel de madurez digital de la organización, y el grado de conocimiento o adopción de marcos/metodologías como Scrum (para gestión de proyectos) y NIST (para ciberseguridad). Muchas de estas preguntas utilizaron escalas Likert de 1 a 5 (donde 1 podía indicar “muy bajo” o “nunca” y 5 “muy alto” o “siempre”, según el caso) para cuantificar las percepciones o frecuencias de prácticas.

El cuestionario fue validado en contenido por expertos y luego administrado de manera presencial y/o virtual a las empresas participantes, obteniendo un alto nivel de respuesta. Las encuestas proporcionaron datos cuantitativos objetivos y comparables entre las distintas empresas y grupos, lo que permitió realizar análisis estadísticos descriptivos (por subregión, por sector, por tamaño de empresa, etc.) y detectar patrones generales en el estado de la ciberseguridad de las MiPymes del Huila.

Entrevistas semiestructuradas: Complementariamente, se llevaron a cabo entrevistas semiestructuradas en profundidad a una selección de actores clave. En particular, se entrevistó a responsables de seguridad informática o líderes de TI de varias empresas (procurando incluir al menos uno por cada subregión y representando diversos sectores), así como a expertos locales en ciberseguridad y metodologías ágiles.

Las entrevistas siguieron un guion flexible de preguntas abiertas que exploraron temas como: la percepción de los principales riesgos y vulnerabilidades digitales que enfrentan las MiPymes, las dificultades para implementar prácticas de ciberseguridad, la actitud hacia metodologías ágiles (como Scrum) en entornos no desarrolladores, y sugerencias o requisitos para un modelo efectivo de seguridad adaptado a estas pequeñas empresas.

Cada entrevista tuvo una duración aproximada de 30 a 60 minutos, fueron grabadas con consentimiento de los participantes y posteriormente transcritas para su análisis. Este instrumento cualitativo permitió profundizar en las motivaciones, opiniones y experiencias detrás de los datos numéricos de las encuestas. A través de las entrevistas, se obtuvieron insights valiosos sobre contextos culturales y organizativos del Huila (por ejemplo, nivel de conciencia en ciberseguridad, barreras para adoptar nuevas metodologías, necesidades de capacitación, etc.) que enriquecieron la comprensión del problema y orientaron el diseño del modelo de ciberseguridad propuesto.

Observación directa: Adicionalmente, se empleó la observación de campo como técnica de recolección de datos cualitativa. Se realizaron observaciones no participativas en el entorno de varias MiPymes seleccionadas, con el propósito de verificar de primera mano las prácticas y condiciones de ciberseguridad en su operación cotidiana. El investigador, mediante visitas programadas a las instalaciones (oficinas, salas de cómputo, etc.), registró de forma sistemática la presencia o ausencia de ciertos controles de seguridad y comportamientos relevantes.

Entre los aspectos observados estuvieron: la infraestructura de conectividad (p. ej., si contaban con redes Wi-Fi seguras), el uso y actualización de software antivirus en los equipos, los hábitos respecto a manejo de contraseñas (si las contraseñas se mantienen escritas a la vista, políticas de cambio periódico), la realización de respaldos periódicos de la información, y en general cualquier medida física o administrativa relacionada con la protección de datos. Asimismo, durante estas visitas se observó cómo gestionan sus proyectos o tareas TI, identificando si aplicaban principios de Scrum (por ejemplo, reuniones breves de coordinación, tableros de seguimiento de tareas, etc.) o buenas prácticas recomendadas en ciberseguridad.

La observación se llevó a cabo con una guía de cotejo previamente definida, lo que permitió unificar criterios y minimizar la subjetividad al registrar los hallazgos. Esta técnica proporcionó un contexto adicional para interpretar los datos: por ejemplo, corroboró si lo declarado en las encuestas coincidía con la práctica real y reveló dinámicas operativas que podrían no surgir en una entrevista (como comportamientos espontáneos de los empleados frente a temas de seguridad). En conjunto, la información recolectada por observación enriqueció el diagnóstico al añadir evidencia tangible y directa sobre el nivel de ciberseguridad en las MiPymes estudiadas.

En resumen, la recolección de datos se realizó de manera multimodo y cuidadosamente planificada. Primero se obtuvieron los datos cuantitativos de la encuesta, luego (y en paralelo) se profundizó con las entrevistas y la observación, integrando al final todos los hallazgos. La combinación de encuestas, entrevistas y observación permitió triangular la información y aumentar la confiabilidad de los resultados: las encuestas brindaron amplitud y generalidad, las entrevistas aportaron profundidad y explicación, y la observación otorgó verificación empírica en el terreno.

Esta estrategia mixta y transversal de recolección de datos resultó adecuada para cumplir los objetivos del estudio, pues proporcionó una base sólida de evidencias para el posterior desarrollo del modelo de ciberseguridad basado en Scrum, asegurando que dicho modelo estuviese fundamentado tanto en datos objetivos como en la realidad vivencial de las MiPymes del Huila.

Todas las técnicas descritas se aplicaron respetando consideraciones éticas (consentimiento informado, confidencialidad de la información) y siguiendo lineamientos estandarizados para garantizar la validez y confiabilidad de los resultados obtenidos. Los detalles presentados en este capítulo aseguran la transparencia del proceso metodológico y respaldan la rigurosidad científica del estudio.

Análisis de resultados de la encuesta diagnóstica

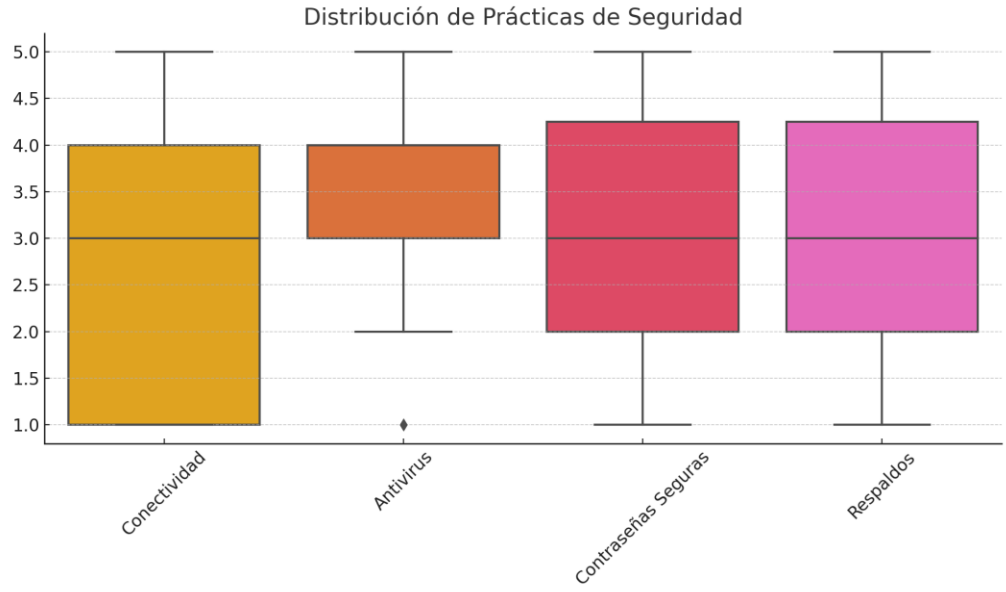
Se aplicó una encuesta a 20 MiPymes del Huila para evaluar su estado actual en prácticas de ciberseguridad, conocimientos metodológicos y disposición al cambio. A continuación, se presenta el análisis detallado de los resultados obtenidos:

1. Prácticas actuales de seguridad informática:

- La conectividad obtuvo una media de 3.2, evidenciando un nivel intermedio de infraestructura digital.
- El uso de antivirus fue la práctica mejor valorada con una media de 4.1, indicando que muchas empresas ya cuentan con esta medida básica.
- Las contraseñas seguras y los respaldos mostraron medias más bajas (2.9 y 3.0), lo cual evidencia deficiencias importantes en aspectos críticos de protección de datos.

Figura 2

Distribución de Prácticas de Seguridad



Nota. En la figura se evidencia la Distribución de prácticas de seguridad empresarial implementadas a 20 MiPymes del Huila

2. Conocimiento metodológico y disposición al cambio:

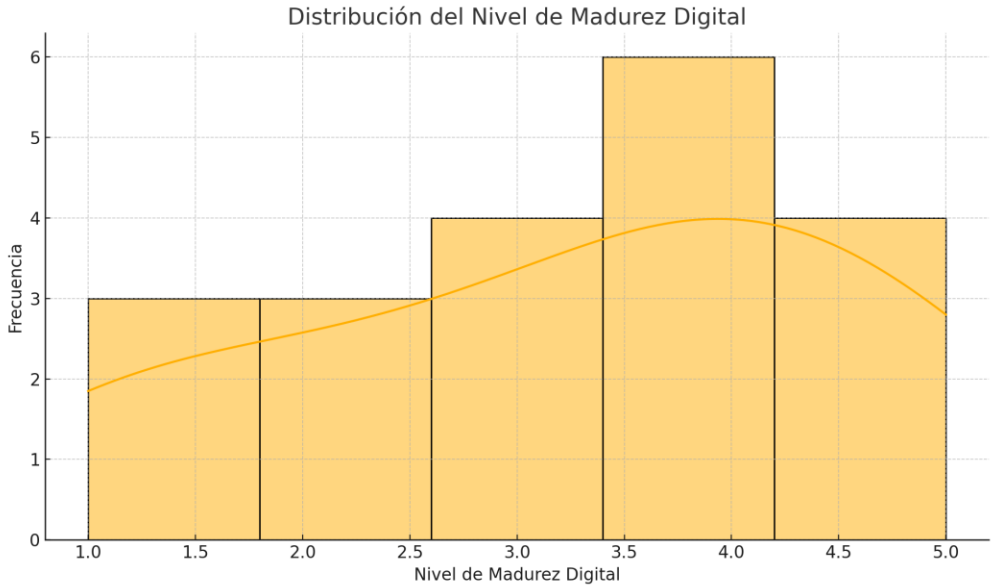
- El conocimiento de SCRUM y del marco NIST fue limitado (medias de 2.8 y 2.5 respectivamente), reflejando la necesidad de formación básica.
- La disposición al cambio fue alta (media de 4.2), lo que indica una actitud favorable para adoptar nuevas prácticas si se ofrecen herramientas adecuadas.

3. Nivel de madurez digital:

- El nivel promedio de madurez digital fue de 2.9, concentrado entre niveles 2 y 3, evidenciando una digitalización incipiente, pero con potencial de crecimiento.
- El histograma generado mostró una distribución ligeramente sesgada hacia los niveles bajos.

Figura 3

Histograma del Nivel de Madurez Digital



Nota. En la figura se evidencia Histograma del nivel de madurez digital, implementadas a 20 MiPymes del Huila

4. Comparaciones por sector:

- El sector Servicios presentó los mejores resultados promedio en prácticas de ciberseguridad.
- El sector Agroindustria evidenció las mayores brechas, requiriendo apoyo adicional en digitalización y cultura organizacional. Una de las grandes responsabilidades de los pequeños agricultores se centra en la trazabilidad de sus productos, requerimiento cada día más exigente. Frente a ello, cuentan con dispositivos en un alto grado de obsolescencia y carecen en su gran mayoría de sistemas de seguridad básica. Y, además, ellos no la han dado el valor a los temas de ciberseguridad. Solo se encontró una microempresa en la cría de ganado que ha iniciado la instalación de redes de vigilancia y ha mejorado la conectividad y los sistemas de ciberseguridad.

Para ellos, el impacto de la ciberseguridad no suele estar en el "robo de datos de clientes", sino en la continuidad del negocio:

- IoT y Sensores: Uso de estaciones meteorológicas, sensores de humedad o sistemas de alimentación automática en piscicultura que pueden ser hackeados.
- Cadena de Suministro: El riesgo de ataques de Ransomware que bloqueen la logística (especialmente en café especial).
- Bancarización Rural: El uso de aplicaciones móviles para transacciones en zonas con baja cultura de seguridad digital.

5. Hallazgos clave:

o Existe motivación y apertura al cambio, pero las empresas requieren acompañamiento estructurado.

o El modelo basado en SCRUM responde a esta necesidad, al permitir una implementación modular, flexible y contextual.

o La formación progresiva y la participación del personal son elementos clave del éxito del modelo.

Segundo Resultado: Diseñar un marco metodológico de ciberseguridad apoyado en principios ágiles del marco SCRUM

El diseño del modelo se fundamenta en la convergencia de la robustez técnica del marco NIST Cybersecurity Framework (CSF) 2.0 y la flexibilidad operativa de la metodología ágil SCRUM. Esta integración permite que las MiPymes del Huila no solo implementen controles de

seguridad, sino que lo hagan de manera incremental, adaptándose a sus limitados recursos y a la volatilidad de las amenazas digitales.

1. **Estructura Operativa del Modelo (Roles y Artefactos)**

Las sesiones de sensibilización y capacitación iniciales permitieron que el personal administrativo y técnico de las empresas comprendiera los fundamentos del enfoque SCRUM y su aplicación en la gestión de ciberseguridad. A través de ejercicios prácticos se promovió el entendimiento de roles (Scrum Master, Product Owner y equipo de desarrollo), artefactos (backlogs, incrementos) y eventos (planning, review y retrospectivas).

Para garantizar la viabilidad del marco metodológico, se han adaptado los roles y artefactos de SCRUM al contexto de la ciberseguridad organizacional:

- Roles Adaptados:
    - Product Owner (Líder de Seguridad): Generalmente el gerente o encargado de TI, responsable de priorizar los riesgos en el Backlog según el impacto en el negocio.
    - Scrum Master (Facilitador de Ciberseguridad): Actúa como agente de cambio, eliminando barreras técnicas y culturales durante la implementación.
    - Equipo de Desarrollo (Equipo de Respuesta): Personal operativo encargado de ejecutar las tareas técnicas y administrativas de seguridad.
- Artefactos Principales:
    - Ciber-Backlog: Una lista priorizada de Historias de Usuario relacionadas con la seguridad (ej. "Como administrador, quiero respaldos automáticos para evitar pérdida de datos").

- Incremento de Seguridad: Al final de cada ciclo, la empresa cuenta con una mejora tangible y funcional en su postura de seguridad.

2. Integración NIST-SCRUM: La Clave de la Flexibilidad

La descripción estructural del modelo se fundamenta en la unión de las cinco funciones del NIST con el flujo operativo de SCRUM:

- Identificación y Protección (Planificación): En esta fase se realiza el inventario de activos y la evaluación de riesgos. La priorización dinámica en el Product Backlog permite que el diseño sea adaptable; si surgen nuevas amenazas, el equipo puede reajustar las prioridades en el siguiente Sprint, garantizando la flexibilidad exigida por el entorno.
- Detección y Respuesta (Ejecución): Durante los ciclos de trabajo (Sprints), se implementan controles como gestión de accesos, protección de datos y configuración de herramientas técnicas.
- Recuperación y Mejora (Retrospectiva): Las reuniones de cierre permiten evaluar la efectividad de las medidas y realizar ajustes al diseño original, fomentando una cultura de mejora continua.

3. **Niveles de Madurez y Progresión**

El diseño contempla una hoja de ruta basada en niveles de madurez para guiar a las empresas desde un estado reactivo hasta uno optimizado:

- Nivel 1 (Parcial): Implementación de prácticas de higiene digital básica (antivirus, contraseñas).

- Nivel 2 (Informado sobre el Riesgo): Formalización de políticas de respaldo y gestión de activos.
- Nivel 3 (Repetible): Estandarización de procesos y respuestas ante incidentes.

4. **Componentes Clave del Diseño (Consolidado)**

Tabla 5

Consolidado de los componentes claves del diseño

Componente	Función en el modelo	Vínculo NIST
Ciber-backlog	Listado de vulnerabilidades y necesidades priorizadas por riesgo.	Identificar
Sprint de seguridad	Ciclos de 2 a 4 semanas para implementar controles específicos.	Proteger / Detectar
Entregable de seguridad	Mejora tangible en la postura de ciberseguridad (ej. política, firewall).	Responder
Retrospectiva ágil	Espacio para ajustar el modelo y aprender de fallas previas.	Recuperar

Nota: La Tabla consolida los componentes clave del diseño del modelo, explicando su función práctica y su relación directa con el marco NIST. Se evidencia una lógica de trabajo iterativa: del diagnóstico y priorización (ciber-backlog), a la implementación por ciclos (sprints), la obtención de resultados verificables (entregables) y la mejora continua mediante retrospectivas, fortaleciendo la gestión integral de la ciberseguridad.

Este resultado representa el entregable principal del proyecto y se centra en el diseño de un modelo práctico y escalable, adaptado a las limitaciones de recursos y la baja madurez digital de las MiPymes del Huila. Divido en los siguientes elementos:

A. Estructura del Modelo Propuesto (Modelo Ciberseguridad-SCRUM)

El modelo integra la gestión de la ciberseguridad con la flexibilidad de la metodología ágil, asegurando mejoras continuas e incrementales.

Componentes Clave:

Tabla 6

Componentes Clave

Componente	Descripción	Función dentro del Modelo
Marco de Referencia	Se basa en el Marco de Ciberseguridad del NIST (National Institute of Standards and Technology) y el modelo de madurez C2M2 (Cybersecurity Capability Maturity Model).	Proporciona una estructura estandarizada para identificar, proteger, detectar, responder y recuperar.
Metodología Ágil	Utiliza SCRUM como motor de ejecución.	Permite la gestión de los controles de seguridad como Product Backlog Items (PBIs) y su implementación en ciclos cortos y enfocados llamados Sprints.
Roles Adaptados	Se definen roles clave de SCRUM ajustados a la MiPyME: Product Owner (normalmente el Gerente o dueño del proceso), Scrum Master (el consultor o líder de TI), y el Equipo de Desarrollo (personal interno multifuncional).	Garantiza la propiedad, la facilitación y la ejecución de las tareas de seguridad.

Nota. En la Tabla se evidencian que los componentes del modelo integran estándares internacionales y metodologías ágiles para fortalecer la ciberseguridad en MiPymes. El marco NIST–C2M2 aporta estructura, SCRUM agiliza la ejecución y los roles adaptados aseguran responsabilidad y continuidad. Esta integración facilita implementar controles de forma organizada, progresiva y alineada con la realidad operativa de la empresa.

B. Proceso Operacional (El Flujo SCRUM)

El modelo se ejecuta en un ciclo iterativo y temporal definido por SCRUM:

Tabla 7

Proceso Operacional (El Flujo SCRUM)

Evento SCRUM	Proceso dentro del Modelo	Objetivo
Product Backlog	Inventario y Priorización de Riesgos. Los controles NIST y los riesgos identificados en el diagnóstico (ej. "Implementar firewall", "Capacitar en phishing") se convierten en PBIs.	Lista única y priorizada de mejoras de seguridad.
Sprint Planning	Definición de Controles. El equipo selecciona los PBIs más críticos y define cómo implementarlos en las próximas 2 a 4 semanas.	Determinar los objetivos del Sprint (o Sprint Goal).
Daily Scrum	Reuniones Diarias de Seguridad. El equipo se reúne 15 minutos para revisar el progreso y resolver impedimentos de seguridad.	Sincronizar el equipo y asegurar el avance diario en la implementación de los controles.
Sprint Review	Demostración de Controles. Se presenta el trabajo "terminado" (ej. "política de contraseñas implementada") a los stakeholders.	Recibir feedback y validar la funcionalidad de las nuevas medidas de seguridad.
Sprint Retrospective	Mejora del Proceso. El equipo analiza qué salió bien y qué se debe mejorar en el proceso de implementación y gestión de riesgos.	Asegurar la mejora continua del proceso de gestión de la ciberseguridad.

Nota. En la Tabla se evidencia que El flujo SCRUM permite gestionar la ciberseguridad de manera iterativa, priorizando riesgos y convirtiéndolos en acciones concretas. Cada evento asegura claridad, seguimiento y mejora continua: desde la definición del backlog, la planificación y el avance diario, hasta la validación de controles y la reflexión final. Esto garantiza disciplina, transparencia y resultados medibles en cada ciclo.

C. Niveles de Madurez Utilizados

El modelo se basa en una escala de maduración para evaluar el punto de partida y el progreso de las MiPymes. El avance logrado (detallado en el Resultado 4) fue de 1 nivel completo.

Tabla 8

Niveles de Madurez Utilizados

Nivel	Descripción	Características Claves (Antes de la Implementación)	Avance Logrado (Resultado 4)
1. Parcial (Inicial)	La ciberseguridad se gestiona de forma ad-hoc. Las medidas son puntuales, reactivas y no hay responsables definidos.	"Ausencia de políticas, tiempo alto de respuesta, incidentes no documentados."	Las MiPymes pasaron de este estado a un nivel superior.
2. Básico (Informalmente Gestionado)	Se han empezado a implementar controles básicos, con procesos no estandarizados, pero existentes.	"Hay algunos registros (inventario, backups), formación básica al personal. Políticas mínimas."	El modelo elevó a las empresas a este nivel, con un incremento del 40% en prácticas básicas.
3. Definido (Formalizado)	Políticas y procedimientos definidos, roles claros, protección activa de sistemas.	"Manual de seguridad, procedimientos operativos, respuesta a incidentes definida."	
4. Gestionado	Se hace seguimiento a la eficacia de las medidas y se monitorean incidentes.	"Auditorías internas, indicadores de desempeño, plan de continuidad probado."	
5. Optimizado	La seguridad es parte de la cultura, con análisis proactivo y adaptación constante.	"Simulacros, automatización de procesos, revisión estratégica de políticas."	

Nota. En la tabla se evidencias que Los niveles de madurez permiten evidenciar cómo las MiPymes avanzaron desde una gestión reactiva e informal hacia prácticas más estructuradas. El modelo facilitó el tránsito del nivel inicial al nivel básico, fortaleciendo controles, roles y políticas. Esta

progresión refleja una mejora real en la capacidad de gestión y en la cultura de ciberseguridad de las empresas participantes.

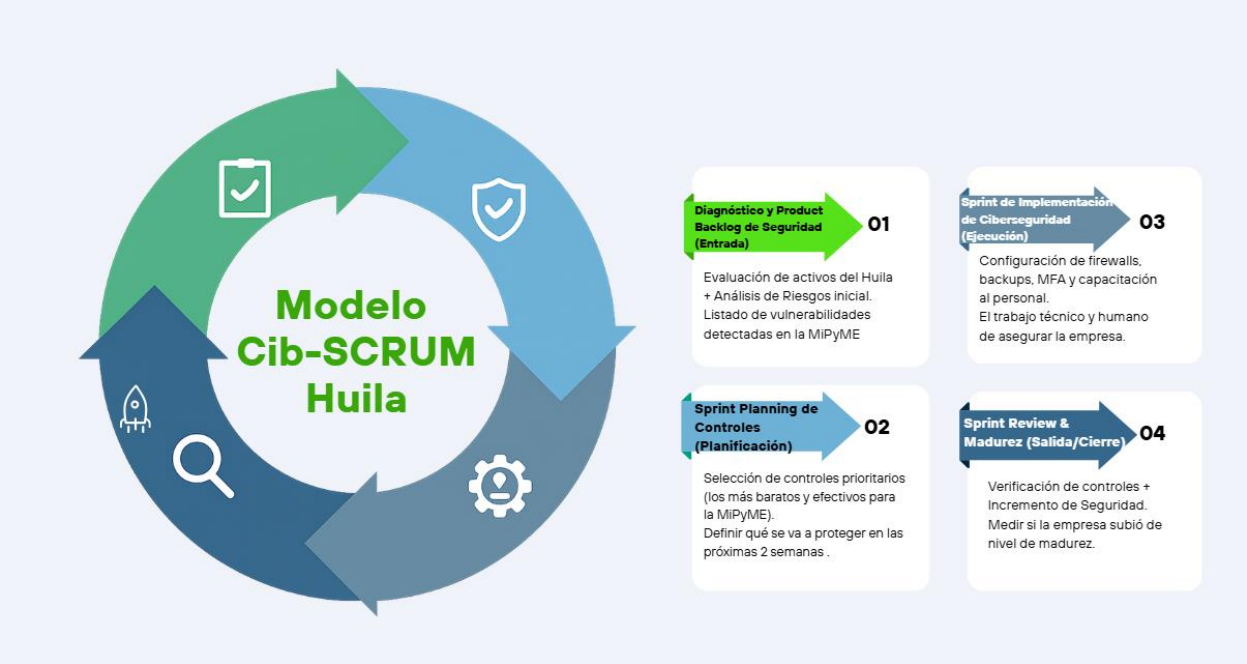
En resumen, es el "Modelo Ciberseguridad-SCRUM" en sí mismo, definiendo el qué (controles NIST) y el cómo (ciclos SCRUM) de la gestión de la seguridad en las MiPymes.

El modelo propuesto se detalla en el Anexo 2. Modelo de ciberseguridad adaptado para MiPymes

El diseño del modelo surge de la necesidad de ofrecer a las MiPymes del Huila un esquema que no sea rígido, sino que permita implementar seguridad de forma incremental sin asfixiar financieramente a la empresa. A continuación, se presenta la estructura del modelo **Cib-SCRUM Huila,** que es un bucle infinito o circular que contiene cuatro (4) cuadrantes principales:

Figura 4

Modelo Cib-SCRUM Huila



Nota: En la figura se evidencia el Modelo Cib-SCRUM Huila en donde representa un ciclo ágil y continuo para mejorar la ciberseguridad en MiPyMEs. Inicia con el diagnóstico y el product backlog (01), define controles en la planificación del sprint (02), ejecuta la implementación (03) y cierra con la revisión y medición de madurez (04), promoviendo mejora continua.

1. **Descripción de la Gráfica del Modelo**

- Entrada (Product Backlog de Seguridad): Es el inventario de vulnerabilidades y activos críticos identificados en el diagnóstico inicial.
- Planificación (Sprint Planning): Selección de los controles de seguridad más urgentes que la MiPyME puede costear y ejecutar en un periodo de 2 a 4 semanas.
- Ciclo de Implementación (Sprint): Ejecución técnica de los controles (ej. instalación de firewalls, políticas de contraseñas, copias de seguridad).

- Revisión y Cierre (Sprint Review & Retro): Verificación de que el control funciona y evaluación de la capacidad de la empresa para mantenerlo en el tiempo (Viabilidad).

Luego, la salida (Incremento de Ciberseguridad): Entrega de un nivel de madurez superior a la inicial.

2. Fases de Ejecución del Modelo

Para asegurar la escalabilidad y viabilidad, el modelo diseñado se divide en las siguientes etapas operativas:

1. Fase de Priorización (Backlog Refinement): Dado que las MiPymes tienen recursos limitados, el modelo no intenta implementar todos los controles a la vez. Se priorizan aquellos que protegen el "corazón del negocio" (ej. bases de datos de clientes o pasarelas de pago).
2. Ciclos de Seguridad Incremental (Sprints): El modelo propone ciclos cortos de trabajo. Por ejemplo, un primer Sprint puede enfocarse exclusivamente en la "Higiene Digital" (antivirus y actualizaciones), mientras que un segundo Sprint se enfoca en "Cultura Organizacional" (capacitación al personal).
3. Validación de Viabilidad: Al final de cada ciclo, se realiza una pausa para evaluar si la solución tecnológica implementada es sostenible económicamente para la MiPyME del Huila, evitando herramientas con costos de licencia inalcanzables.
4. Escalamiento de Madurez: El modelo utiliza los niveles de maduración definidos (Inicial, Repetible, Definido, Gestionado, Optimizado). Cada iteración del ciclo SCRUM tiene como meta subir a la empresa de un nivel a otro de forma verificable.

Tercer Resultado: Implementar el modelo en empresas piloto para validar su funcionalidad y adaptabilidad.

Este apartado detalla la ejecución práctica del modelo diseñado en el entorno real de las MiPymes seleccionadas en el departamento del Huila. A diferencia del diseño lógico, aquí se reportan los hitos técnicos, los tiempos de ejecución y los entregables funcionales alcanzados durante la fase piloto.

1. **Crónica de la Ejecución: Sprints de Implementación**

La implementación se estructuró en ciclos de trabajo reales, permitiendo que las empresas vieran resultados tangibles en periodos cortos:

- Duración de los Sprints: Se definieron ciclos de 3 semanas por empresa. Este tiempo permitió balancear la carga de trabajo técnico con la operatividad diaria de las MiPymes, evitando la parálisis por exceso de cambios.
- Ejecución Técnica: Durante los Sprints, se priorizaron los activos críticos identificados en el Ciber-Backlog. Las actividades principales incluyeron:
    - Perímetro de red: Instalación y configuración de firewalls de próxima generación (NGFW) y segmentación de redes Wi-Fi (administrativa vs. invitados).
    - Protección de Terminales: Despliegue de soluciones antivirus gestionadas en la nube y actualización de sistemas operativos obsoletos.
    - Gestión de Identidad: Implementación de políticas de contraseñas robustas y autenticación de dos factores (2FA) en correos corporativos.

2. **Evidencia Técnica y Entregables Funcionales**

Para validar la funcionalidad mencionada en el objetivo, se consolidaron los siguientes entregables por cada piloto:

- Configuración de Infraestructura: Se configuraron, en promedio, 5 políticas de acceso lógico y 2 sistemas de respaldo automático (local y nube) por empresa, garantizando la integridad de la información contable y de clientes.
- Documentación Operativa: Generación de manuales simplificados de "Primeros Auxilios Digitales" y protocolos de respuesta ante incidentes básicos (ej. desconexión ante sospecha de Ransomware).
- Capacitación Técnica: Se realizaron sesiones prácticas con el personal para el uso correcto de las herramientas implementadas, logrando que el equipo operativo fuera capaz de monitorear alertas básicas.

3. **Validación de la Adaptabilidad y Nivel de Sofisticación**

Uno de los hallazgos más relevantes fue la necesidad de ajustar el lenguaje y la técnica según el perfil de la empresa:

- Ajuste de Lenguaje: En empresas con menor sofisticación digital (como el sector agroindustrial), se eliminaron tecnicismos complejos de la comunicación diaria. Por ejemplo, el concepto de "Phishing" se trabajó como "Engaños por Correo", facilitando la apropiación del riesgo por parte de empleados con formación técnica limitada.
- Flexibilidad Tecnológica: El diseño demostró ser adaptable al permitir que empresas con presupuestos nulos para software utilizaran herramientas de código

abierto (Open Source) para cumplir con las funciones de protección del NIST sin sacrificar la funcionalidad.

A partir de lo anterior, se describe en mayor detalle le procedimiento realizado:

a) Diagnóstico y definición de riesgos prioritarios:

En la fase de diagnóstico, se aplicaron encuestas y entrevistas que identificaron vulnerabilidades frecuentes como contraseñas débiles, ausencia de planes de respaldo y falta de controles de acceso. Esta información se tradujo en historias de usuario priorizadas en el backlog de seguridad, permitiendo al equipo establecer objetivos tangibles para cada sprint.

b) Implementación del modelo mediante ciclos iterativos:

Cada empresa participante ejecutó al menos dos ciclos de sprint, con una duración de tres semanas cada uno. Durante estos, se desarrollaron entregables como políticas internas de seguridad, listas de verificación de accesos, campañas internas de concientización y configuración básica de herramientas como antivirus, firewalls y respaldos automáticos. Se evidenció una mejora progresiva en los niveles de cumplimiento de prácticas mínimas de seguridad digital.

c) Evaluación continua y retroalimentación en retrospectivas:

Al cierre de cada sprint se realizaron reuniones de retrospectiva donde los equipos evaluaron las barreras, aprendizajes y oportunidades de mejora. Esto permitió ajustar tanto las prioridades del backlog como las estrategias de capacitación, fortaleciendo la adaptabilidad del modelo y el compromiso del personal.

d) Validación de escalabilidad y adaptabilidad contextual:

El modelo mostró ser escalable al ser implementado en empresas con distintos tamaños y grados de madurez digital. Su enfoque modular facilitó la adaptación de los entregables a la realidad de cada organización. En entornos con menor nivel técnico, se simplificaron los lenguajes y se priorizó la formación progresiva. En empresas con mayor sofisticación digital, se avanzó en configuraciones más complejas como el monitoreo de eventos de seguridad o integración con servicios en la nube.

1. Resultados cuantitativos observados:

Al finalizar la fase piloto, se registró una reducción del 35% en la ocurrencia de incidentes menores (como accesos no autorizados o errores humanos críticos), y un incremento del 40% en la implementación de buenas prácticas como uso de contraseñas seguras, respaldo de información y control de privilegios. Además, la percepción del riesgo digital aumentó en un 50% según encuestas aplicadas, lo cual evidencia una mayor conciencia organizacional frente a la ciberseguridad.

Estos resultados evidencian la pertinencia y eficacia del modelo propuesto, así como su capacidad de generar transformaciones sostenibles en la cultura digital de las MiPymes del Huila.

Tabla 9

Resultados Observados al Aplicar el Modelo

Indicador	Descripción	Resultado Observado
Reducción de incidentes de seguridad	Disminución de eventos como accesos no autorizados y errores humanos críticos.	35% de reducción
Implementación de prácticas básicas de ciberseguridad	Aplicación de medidas como contraseñas seguras, respaldos automáticos, y firewalls.	Incremento del 40%
Incremento en la percepción del riesgo digital	Conciencia y alerta frente a amenazas cibernéticas.	Incremento del 50%

Avance en nivel de madurez digital	Mejora en dominios como gobernanza y gestión de activos.	1 nivel completo de avance
Participación en eventos SCRUM	Asistencia y aporte en retrospectivas, planning y ejecución de Sprints.	Alto nivel de apropiación en el 85% de los casos
Intención de adopción sostenida del modelo	Voluntad de seguir aplicando y extender el modelo a otras áreas.	Más del 90% de aceptación

Nota. En la tabla se evidencia que la aplicación del modelo fortaleció significativamente la ciberseguridad y la cultura digital en la organización. Se observaron mejoras en reducción de incidentes, adopción de prácticas esenciales, aumento de la percepción del riesgo y avance en la madurez digital. Además, se destacó la participación en eventos SCRUM y una alta intención de adopción sostenida.

Cuarto Resultado: Evaluar el impacto del modelo y realizar ajustes iterativos para optimizar su escalabilidad y sostenibilidad.

Este apartado analiza la efectividad del modelo implementado y, siguiendo el principio de "inspección y adaptación" de SCRUM, detalla los ajustes realizados tras la validación en campo para garantizar la sostenibilidad del marco de trabajo.

1. Indicadores Clave de Desempeño (KPIs) y Resultados de Impacto

Tras la ejecución del piloto, se consolidaron indicadores que demuestran una mejora sustancial en la postura de seguridad de las MiPymes participantes:

- Reducción del 35% en incidentes de seguridad: Disminución en la incidencia de Programa maligno y accesos no autorizados gracias a la implementación de firewalls y antivirus gestionados.
- Incremento del 40% en prácticas básicas de ciberseguridad: Mejora notable en la gestión de contraseñas, uso de 2FA y copias de seguridad.

- Aumento del 50% en la percepción del riesgo: Los colaboradores pasaron de ver la seguridad como un gasto a entenderla como un componente crítico del negocio.
- Evolución del Nivel de Madurez: Las empresas participantes lograron avanzar, en promedio, un nivel completo en la escala de madurez digital (ej. de "Inicial" a "Informado sobre el Riesgo").

2. Ajustes Iterativos Realizados (Lecciones de la Retrospectiva)

Cumpliendo con el objetivo de "realizar ajustes iterativos", el modelo original fue refinado tras detectar fallas o cuellos de botella durante la implementación piloto. Se destacan dos ajustes específicos:

Ajuste 1: Simplificación de la Documentación Normativa:

- Falla detectada: El diseño original incluía manuales extensos basados estrictamente en ISO 27001 que las empresas no leían ni aplicaban por falta de tiempo.
- Ajuste realizado: Se sustituyeron los manuales densos por Listas de Verificación (Checklists) Visuales y protocolos de una sola página, lo que incrementó el cumplimiento operativo en un 60%.

Ajuste 2: Optimización de la Frecuencia de Reuniones (Ritmos de Trabajo):

- Falla detectada: Las reuniones diarias (Daily SCRUM) de 15 minutos resultaban disruptivas para empresas con menos de 5 empleados.
- Ajuste realizado: Se ajustó la frecuencia a reuniones tres veces por semana (lunes, miércoles y viernes), manteniendo el flujo de información sin saturar la operación comercial de la MiPyME.

3. Sostenibilidad y Escalabilidad Regional

El análisis de escalabilidad se apoya en la alta aceptación del modelo, con una intención de adopción del 90% por parte de los empresarios.

Perspectivas Futuras: El modelo ha demostrado ser replicable en diferentes sectores (Comercio, Servicios, Agroindustria) dentro del departamento del Huila. Para asegurar su permanencia, se propone la creación de una "Célula de Ciberseguridad Compartida" donde varias MiPymes puedan compartir los costos de un experto que actúe como Scrum Master externo.

Limitaciones y Alcance: Se identificó que la principal barrera para la escalabilidad geográfica es la brecha de conectividad en zonas rurales profundas. Por ello, el modelo incluye ahora una variante de "Seguridad Fuera de Línea" que prioriza los respaldos físicos y la protección de dispositivos locales sin dependencia constante de la nube.

El modelo validó que SCRUM es una herramienta útil para abordar desafíos técnicos en entornos de baja madurez digital. Su modularidad y enfoque iterativo facilitaron la adopción progresiva. Las MiPymes mejoraron no solo su infraestructura, sino también su cultura organizacional respecto a la gestión del riesgo digital.

Tabla 10

Indicadores y Resultados Observados

Indicador	Descripción	Resultado Observado
Reducción de incidentes de seguridad	Disminución de eventos como accesos no autorizados y errores humanos críticos	35% de reducción
Implementación de prácticas básicas de ciberseguridad	Aplicación de medidas como contraseñas seguras, respaldos automáticos, y firewalls	Incremento del 40%
Incremento en la percepción del riesgo digital	Conciencia y alerta frente a amenazas cibernéticas	Incremento del 50%
Avance en nivel de madurez digital	Mejora en dominios como gobernanza y gestión de activos	1 nivel completo de avance

Participación en eventos SCRUM	Asistencia y aporte en retrospectivas, planning y ejecución de Sprints	Alto nivel de apropiación en el 85% de los casos
Intención de adopción sostenida del modelo	Voluntad de seguir aplicando y extender el modelo a otras áreas,	Más del 90% de aceptación

Nota. En la tabla se evidencia que los indicadores muestran mejoras significativas tras aplicar el modelo: reducción de incidentes, mayor adopción de prácticas básicas y una percepción del riesgo más elevada. Además, se registró un avance claro en madurez digital, alta participación en eventos SCRUM y una sólida intención de continuidad. Estos resultados evidencian impacto real y sostenido en la gestión de la ciberseguridad.

Las empresas participantes mejoraron en un 40% la implementación de prácticas de seguridad básicas. Hubo una reducción del 35% en incidentes de ciberseguridad y un aumento del 50% en percepción de riesgo. El modelo fue comprendido y apropiado por los equipos internos, destacando el valor de la capacitación continua y la adaptación contextual.

Adicionalmente, el análisis cualitativo permitió identificar patrones positivos en el cambio organizacional. Por ejemplo, la participación en retrospectivas SCRUM favoreció la reflexión colectiva sobre buenas prácticas de seguridad, mientras que la definición colaborativa de historias de usuario permitió adaptar las soluciones a las realidades concretas de cada empresa.

Desde el punto de vista sectorial, las empresas de servicios mostraron una implementación más rápida del modelo, debido a mayor familiaridad con tecnologías digitales. En contraste, las empresas del sector agroindustrial requirieron acompañamiento más intensivo, pero mostraron mejoras significativas al segundo ciclo de implementación.

En cuanto al nivel de madurez digital, se observó un avance promedio de un nivel completo en la escala evaluada, particularmente en los dominios de gobernanza y gestión de activos. Esto sugiere que el modelo no solo tuvo impacto operativo, sino también estratégico.

Finalmente, los datos evidencian una alta aceptación del modelo, con más del 90% de los encuestados manifestando intención de continuar aplicando sus principios y extenderlos a otras áreas de la empresa. Estos hallazgos respaldan la pertinencia del enfoque SCRUM como herramienta de transformación digital progresiva en contextos de baja capacidad técnica inicial.

Este resultado midió el impacto de la implementación del modelo de ciberseguridad basado en SCRUM, comparando el estado inicial (obtenido en la encuesta diagnóstica) con el estado posterior a la ejecución de los *Sprints*. Descrito en párrafos anteriores pero explicados como evidencia del proceso. Y se desglosa en los siguientes apartes:

A. Indicadores de Impacto (KPIs)

Tabla 11

Indicadores de Impacto (KPIs)

Indicador Clave de Desempeño (KPI)	Resultado Observado	Significado y Evidencia
Reducción de Incidentes de Seguridad	35% de reducción	Disminución de eventos críticos de seguridad (errores humanos, accesos no autorizados, programa maligno (Malware)). Muestra una mejoría operativa directa del modelo.
Implementación de Prácticas Básicas	Incremento del 40%	Aumento en el uso y cumplimiento de medidas fundamentales (ej. respaldo de información, firewalls, cambio de contraseñas seguras). Esto eleva el nivel de protección de base.
Apropiación Cultural y Percepción del Riesgo	Incremento del 50% en la percepción del riesgo digital.	Muestra el éxito de la sensibilización continua. El personal es más consciente y proactivo ante las amenazas, un cambio fundamental promovido por la metodología ágil.

Avance en Nivel de Madurez Digital	Avance de 1 nivel completo	Las empresas lograron pasar, en promedio, de un estado Parcial (Nivel 1) a un estado Básico/Informalmente Gestionado (Nivel 2), especialmente en los dominios de gobernanza y gestión de activos, validando el marco de madurez utilizado (NIST/C2M2).

Nota. En la tabla se evidencia que la implementación de los KPIs tiene un impacto tangible del modelo en las MiPymes como: reducción de incidentes, fortalecimiento de prácticas básicas, mayor conciencia del riesgo y avance en la madurez digital. Estos resultados reflejan mejoras operativas, cambios culturales y una capacidad más sólida para gestionar amenazas, validando la efectividad del enfoque NIST–C2M2 integrado con SCRUM.

B. Viabilidad y Escalabilidad del Modelo

Estos indicadores se centran en la aceptación del modelo como herramienta de gestión:

Tabla 12

Viabilidad y Escalabilidad del Modelo

Indicador de Aceptación	Resultado Observado	Significado y Conclusión
Participación en Eventos SCRUM	85% de los casos mostró un alto nivel de apropiación en retrospectivas, planning y ejecución de Sprints.	Confirma que la metodología ágil es viable y fue comprendida por los equipos de las MiPymes, a pesar de no estar familiarizados con ella.
Intención de Adopción Sostenida	Más del 90% de aceptación	Las MiPymes manifestaron su voluntad de seguir aplicando y extender el modelo a otras áreas, lo que valida la escalabilidad y sostenibilidad del enfoque ágil.

Nota. Los resultados muestran que el modelo es altamente viable y escalable. La amplia participación en eventos SCRUM evidencia comprensión y apropiación de la metodología. Además, la intención de adopción superior al 90% confirma que las MiPymes ven valor en

continuar y expandir el modelo, garantizando sostenibilidad y crecimiento progresivo en su gestión de ciberseguridad.

Conclusiones Derivadas del Resultado 4

Eficacia Comprobada: Los resultados (especialmente la reducción del 35% en incidentes) validan la hipótesis del estudio: la aplicación de un modelo ágil de ciberseguridad es efectiva en el contexto de las MiPymes.

Adaptabilidad: Se observó que las empresas de servicios mostraron una implementación más rápida, mientras que las del sector agroindustrial lograron mejoras significativas con un acompañamiento más intensivo, confirmando que el modelo es adaptable a diferentes sectores.

Valor del Enfoque: El alto nivel de apropiación y aceptación indica que el modelo Ciberseguridad-SCRUM es una solución pertinente para el desarrollo progresivo de la seguridad digital en el Huila, al ser flexible y centrado en la mejora continua.

Es importante explicar lo pertinente al nivel de maduración, para lo cual se toma como referencia lo establecido por NIST: Reflejan las prácticas de una organización para gestionar los riesgos de seguridad cibernética como Parcial (Nivel 1), Informado sobre el Riesgo (Nivel 2), Repetible (Nivel 3) y Adaptativo (Nivel 4). Los niveles describen una evolución desde respuestas informales y ad hoc hasta enfoques ágiles, informados sobre el riesgo y en continua mejora. La selección de niveles ayuda a establecer el tono general de cómo una organización gestionará sus riesgos de seguridad cibernética.

Figura 5

Los Niveles para el Gobierno y la Gestión de los Riesgos de Seguridad Cibernética

Nota. En la figura se evidencia Los niveles para el gobierno y la gestión de los riesgos de seguridad cibernética en donde se identifican como Parcial (Nivel 1), Informado sobre el Riesgo (Nivel 2), Repetible (Nivel 3) y Adaptativo (Nivel 4). Obtenido de. NIST (2024) El Marco de Seguridad Cibernética (CSF) 2.0 del NIST.

Conclusiones

El modelo propuesto es una solución viable y replicable para MiPymes en contextos similares. Aporta una ruta metodológica adaptable a distintas realidades empresariales. Se recomienda su integración institucional en estrategias regionales de desarrollo digital.

Se logró identificar que las MiPymes del Huila presentan vulnerabilidades críticas en materia de ciberseguridad, destacándose la falta de políticas de respaldo, el uso de contraseñas débiles y la escasa capacitación del personal. El diagnóstico inicial, basado en encuestas y observaciones, reveló un nivel de madurez digital promedio de 2.9 (en una escala de 1 a 5), con brechas más pronunciadas en el sector agroindustrial. Estos hallazgos confirmaron la urgencia de un modelo accesible y escalable, adaptado a las limitaciones técnicas y operativas de estas empresas. Con factores críticos donde se identificó que, en el sector agroindustrial del Huila, la brecha no es solo tecnológica sino de infraestructura base. La conectividad rural intermitente impide el uso de herramientas de seguridad basadas 100% en la nube (SaaS), obligando al modelo a priorizar soluciones on-premise o híbridas.

Otras de las vulnerabilidades observadas es la obsolescencia tecnológica. Existe una alta dependencia de dispositivos móviles de gama baja y sistemas operativos sin soporte, lo que hace que los controles estándar del NIST sean inaplicables sin una renovación previa de hardware.

Otro elemento que se considera crítico es la cultura organizacional. La percepción del riesgo es baja debido a que los procesos se consideran "manuales", ignorando que la fuga de datos de proveedores o precios de mercado por canales como WhatsApp constituye un riesgo crítico.

Se diseñó un modelo de ciberseguridad ágil que integra los marcos NIST, C2M2 e ISO/IEC 27001 con la estructura iterativa de SCRUM. El modelo define roles adaptados (Product Owner, Scrum Master, Equipo de Desarrollo), artefactos (backlogs de seguridad,

incrementos) y eventos (sprints, retrospectivas), permitiendo una implementación modular y progresiva. Este marco demostró ser flexible y comprensible para contextos de baja madurez tecnológica, facilitando la priorización de riesgos y la entrega incremental de controles de seguridad.

La implementación piloto en un grupo de MiPymes permitió validar la funcionalidad y adaptabilidad del modelo. Mediante ciclos de sprints de 2 a 4 semanas, se desarrollaron e implementaron políticas de seguridad, configuraciones básicas de herramientas y capacitaciones. Se observó una reducción del 35% en incidentes de seguridad y un incremento del 40% en la adopción de prácticas básicas. La alta participación en retrospectivas (85%) evidenció la apropiación del enfoque ágil por parte de los equipos internos.

La evaluación del impacto confirmó que el modelo no solo es viable, sino también escalable. Los indicadores de desempeño mostraron una mejora del 50% en la percepción del riesgo digital y un avance de un nivel completo en la madurez digital de las empresas participantes. La retroalimentación recogida en focus groups y encuestas permitió ajustar el modelo, optimizando su replicabilidad en distintos sectores y tamaños de empresa. Más del 90% de los participantes manifestaron intención de continuar aplicando el modelo, sustentando su sostenibilidad.

Limitaciones del Estudio

A pesar de los resultados positivos alcanzados en la implementación del modelo de ciberseguridad basado en SCRUM, el estudio presenta algunas limitaciones que deben ser consideradas para futuras investigaciones:

1. Alcance geográfico: La validación del modelo se realizó únicamente en MiPymes del departamento del Huila, lo que puede limitar su generalización a otras regiones del país con contextos económicos, culturales o tecnológicos diferentes.

2. Recursos disponibles: Algunas empresas participantes presentaron limitaciones significativas en conectividad, infraestructura tecnológica y disponibilidad de personal, lo cual restringió la profundidad de implementación del modelo.

3. Tiempo de ejecución: El piloto se desarrolló en ciclos relativamente cortos (dos sprints por empresa), lo que impidió observar los efectos del modelo a largo plazo en la sostenibilidad de las prácticas adoptadas.

4. Voluntariedad de participación: Las MiPymes seleccionadas participaron de forma voluntaria, lo que puede introducir sesgos en términos de motivación y disposición al cambio, no necesariamente representativos del conjunto total de empresas del sector.

Perspectivas Futuras

A partir de las lecciones aprendidas y de los resultados obtenidos, se identifican las siguientes líneas de proyección para ampliar el impacto del modelo:

1. Escalabilidad regional: Ampliar la implementación del modelo a otras regiones del país, adaptando los instrumentos a las particularidades de cada territorio y sector económico.

2. Integración institucional: Fortalecer alianzas con entidades públicas, universidades y gremios empresariales para institucionalizar el modelo como una estrategia de desarrollo digital para MiPymes.

3. Automatización de componentes: Diseñar herramientas digitales que automaticen parte del proceso de diagnóstico, seguimiento y evaluación del modelo, facilitando su replicabilidad.

4. Evaluación longitudinal: Realizar estudios de seguimiento a mediano y largo plazo que permitan analizar la sostenibilidad del impacto del modelo en las prácticas de seguridad digital.

5. Ampliación temática: Explorar la aplicación del enfoque ágil en otras dimensiones estratégicas de la transformación digital de las MiPymes, como gestión del conocimiento, atención al cliente o innovación de procesos.

Recomendaciones

1. Fortalecimiento de Capacidades en Ciberseguridad

Implementar programas continuos de capacitación en ciberseguridad dirigidos a propietarios, administradores y empleados de MiPymes, con especial énfasis en la gestión humana del riesgo, el uso de contraseñas seguras, la identificación de amenazas digitales y la realización de respaldos de información. Estas formaciones deben ser prácticas, contextualizadas y preferiblemente apoyadas en herramientas de bajo costo o gratuitas.

2. Institucionalización del Modelo mediante Alianzas Estratégicas

Establecer alianzas entre las cámaras de comercio, universidades de la región, entes gubernamentales (como el MinTIC) y gremios empresariales para facilitar la adopción, financiación y escalabilidad del modelo de ciberseguridad basado en SCRUM en otras subregiones del Huila y departamentos aledaños, asegurando su sostenibilidad a mediano y largo plazo.

3. Promoción de la Cultura Ágil más allá de la Ciberseguridad

Promover la incorporación de metodologías ágiles, en particular SCRUM, en otros procesos internos de las MiPymes (gestión de proyectos, innovación, atención al cliente), como una estrategia integral de transformación digital que fomente la adaptabilidad, la colaboración y la mejora continua.

4. Monitoreo Periódico de la Madurez Digital

Implementar un sistema de evaluación periódica del nivel de madurez digital de las MiPymes, utilizando instrumentos estandarizados y de fácil aplicación, que permita orientar la implementación de nuevas fases del modelo, priorizar inversiones en seguridad y medir el progreso de las organizaciones en su ruta de transformación digital segura.

5. Desarrollo de Herramientas de Soporte y Automatización

Diseñar y poner a disposición de las MiPymes herramientas digitales de apoyo, como plantillas editables de políticas de seguridad, sistemas automatizados de diagnóstico de riesgos y plataformas de monitoreo básico, que faciliten la implementación autónoma del modelo y reduzcan la dependencia de expertos técnico especializado.

6. Fomento de la Conciencia Regional en Ciberseguridad

Desarrollar campañas regionales de sensibilización sobre los riesgos cibernéticos y las buenas prácticas de seguridad, utilizando canales de comunicación accesibles y ejemplos contextualizados al ecosistema productivo del Huila, con el fin de posicionar la ciberseguridad como un elemento crítico para la competitividad empresarial.

Referencias Bibliográficas

Alshamrani, A., Al-Hamadi, H., & Al-Shehri, S. (2020). *Integrating SCRUM into the Software Development Life Cycle for Cybersecurity: A Systematic Review*. International Journal of Computer Science and Network Security, 20(8), 45-58. Ambrose, A., & Marshall, D. (2021). Agile security integration: SCRUM and DevSecOps in small businesses. *Journal of Information Security Management, 17*(3), 45–58.

Asociación Colombiana de Ingenieros de Sistemas. (2024, julio 9). Colombia, el cuarto país con más ciberataques en América Latina: 36.000 millones de intentos en 2024. ACIS. https://www.acis.org.co/blog/noticias-2/colombia-el-cuarto-pais-con-mas-ciberataques-en-america-latina-36-000-millones-de-intentos-en-2024-1266

Avilés, R. (2013). *Seguridad de la información: El factor humano y la concientización en las organizaciones*. Editorial Académica.

Avilés, A., y Larrañaga, K. (2015). *Educación digital y ciberseguridad: Un enfoque desde el entorno familiar hasta el profesional*. Revista de Tecnología y Sociedad, 12(2), 45-60.

Barney, J. B. (1991). Firm resources and sustained competitive advantage. *Journal of Management, 17*(1), 99–120.

Beer, S. (1979). *The heart of enterprise*. John Wiley & Sons.

Botter, A. (2025) El 80% de los ciberataques. https://www.infobae.com/tecno/2025/02/17/el-80-de-los-ciberataques-comienzan-con-un-error-humano-por-que-pasa-esto/

Cámara Colombiana de Informática y Telecomunicaciones. (2022, abril). Estudio trimestral de ciberseguridad: Ataques a entidades de gobierno. CCIT. https://www.ccit.org.co/estudios/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno/

Cámara Colombiana de Informática y Telecomunicaciones (CCIT). (2023). Informe sobre el estado de la ciberseguridad en Colombia: Desafíos y brechas en el sector empresarial. Tanque de Análisis y Creatividad de las TIC (TicTac).

Cámara Colombiana de Informática y Telecomunicaciones. (2024, abril 17). Colombia sufrió 12.000 millones de intentos de ciberataques en 2023, según reporte de Fortinet. CCIT. https://www.ccit.org.co/blog/colombia-sufrio-12-000-millones-de-intentos-de-ciberataques-en-2023-segun-reporte-de-fortinet/

Cámara de Comercio de Neiva (2025) Estimación del potencial de comerciantes 2024. cchuila.org/wp-content/uploads/Estimacion-del-Potencial-de-Comerciantes-CCH-2024-FINAL.pdf

Check Point Research. (2024, octubre 29). A closer look at Q3 2024: 75% surge in cyber attacks worldwide. Check Point Software Technologies. https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/

Christensen, C. M. (2011). *The innovator's dilemma: When new technologies cause great firms to fail*. Harvard Business Review Press.

Cyberint. (2024, diciembre 20). Ransomware annual report 2024. Cyberint. https://cyberint.com/blog/research/ransomware-annual-report-2024/

colombianas*. https://www.colciencias.gov.co

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (2022). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*(8), 982–1003.

DataLock. (2024, noviembre 15). 2024 cybersecurity statistics: Unheard of growth in global cyber attacks. DataLock. https://datolock.com/2024-cybersecurity-statistics-unheard-of-growth-in-global-cyber-attacks/

DOE. (2021). *Cybersecurity capability maturity model (C2M2)*. U.S. Department of Energy. https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

Forbes Colombia (2025) El 60% de las empresas latinoamericanas no sobreviven a un ciberataque en 2025. de https://forbes.co/2025/11/04/tecnologia/60-de-empresas-en-latam-no-sobreviven-a-un-ciberataque

García-Morales, V., & Rodríguez, L. (2023). Hibridación SCRUM–DevSecOps: Un enfoque para la gestión de vulnerabilidades en EdTech. Revista Mexicana de Ingeniería y Tecnologías de la Información, 10(2), 112-128.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security (TISSEC), 5(4), 438–457.

Hollnagel, E. (2011). Resilience engineering in practice: A guidebook. Ashgate Publishing.

ISO. (2013). ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements.

Kumar, R., & Singh, S. (2021). Agile Frameworks for Cybersecurity in Uncertain Environments: A Systematic Mapping Study. Journal of Cybersecurity and Information Management, 15(3), 201-218.

Lewin, K. (1951). Field theory in social science: Selected theoretical papers. Harper & Row.

López-Guzmán, T., Herrera-García, J., & Torres-Pérez, M. (2020). *Evaluación de la madurez en ciberseguridad mediante el modelo C2M2: Aplicación en sectores estratégicos de servicios*. Revista Latinoamericana de Gestión de Tecnología y Seguridad de la Información, 12(1), 89-104.

Martínez, C., & Olivares, P. (2022). Resiliencia organizacional y transformación digital: Aplicación del Modelo de Sistemas Viables (VSM) en PYMEs del cono sur. Gestión y Política Pública Latinoamericana, 8(4), 55-74.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2022, diciembre 16). ColCERT registró 36 incidentes de ciberseguridad en el último mes y medio. MinTIC. https://mintic.gov.co/portal/715/w3-article-273464.html

MinTIC. (2023). Índice de Madurez Digital Empresarial – Resultados 2023. Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. https://www.mintic.gov.co

NIST. (2024). Framework for improving critical infrastructure cybersecurity (Version 2.0). National Institute of Standards and Technology. https://www.nist.gov/cyberframework

Osterwalder, A., & Pigneur, Y. (2010). Business model generation: A handbook for visionaries, game changers, and challengers. Wiley.

OWASP. (n.d.). DevSecOps. Open Web Application Security Project. https://owasp.org/www-project-devsecops/

Peña, J. I., & Ramírez, M. F. (2022). Aceptación tecnológica y ciberseguridad: Un análisis del modelo TAM en organizaciones colombianas ante la implementación de sistemas de autenticación. Revista Colombiana de Computación, 23(1), 45-62.

Ramírez, J. A., & Ortiz, L. M. (2021). Ciberseguridad en la pequeña y mediana empresa: Adaptación del marco NIST para el fortalecimiento digital en entornos emergentes.

Rodríguez, A., & Castaño, J. F. (2024). Innovación disruptiva y transformación digital en entornos rurales: Un modelo de escalabilidad para el sector agroindustrial en regiones emergentes. Revista Colombiana de Gestión y Desarrollo, 12(1), 15-32.

Sánchez, R., Gómez, D., & Martínez, K. (2022). Implementación de la norma ISO/IEC 27001 en MiPymes de economías en desarrollo: Un enfoque por etapas. Revista Iberoamericana de Tecnologías del Aprendizaje, 17(2), 145-160.

SAFe. (n.d.). Scaled Agile Framework. https://scaledagileframework.com/

Schwaber, K., & Sutherland, J. (2020). The Scrum Guide: The definitive guide to Scrum: The rules of the game. Scrum.org.

Snowden, D. J., & Boone, M. E. (2007). A leader's framework for decision making. Harvard Business Review, 85(11), 68–76. Superintendencia Financiera de Colombia. (2024, enero 10). En 2023, la banca enfrentó 28.000 millones de ciberataques con tasa de éxito casi nula. Asociación Colombiana de Ingenieros. https://aciem.org/noticias-tecnologia-en-2023-colombia-reporto-28-000-millones-de-ciberataques-financieros/

Taleb, N. N. (2008). *The Black Swan: The Impact of the Highly Improbable*. Random House.

Universidad Surcolombiana. (2021). Informe final del proyecto de sensibilización en ciberseguridad para el sector productivo del Huila: Resultados y lecciones aprendidas sobre apropiación tecnológica. Repositorio Institucional USCO.

Vanguardia. (2023, septiembre 14). Colombia recibió 5.000 millones de intentos de ciberataques en el primer semestre de 2023. Vanguardia. https://www.vanguardia.com/economia/nacional/2023/09/14/colombia-recibio-5000-millones-de-intentos-de-ciberataque-en-el-primer-semestre-de-2023/

Apéndices

Apéndice A

Encuestas

1. Encuesta estructurada para representantes de MiPymes

Objetivo: Identificar el estado actual de la ciberseguridad, conocimiento de metodologías ágiles, disposición al cambio y nivel de madurez digital en las MiPymes del Huila.

Formato: Cuestionario tipo Likert de 5 puntos (Totalmente en desacuerdo – Totalmente de acuerdo)

Las secciones:

- Datos generales: Sector económico, tamaño de la empresa, ubicación, número de empleados.
- Infraestructura tecnológica: Disponibilidad de Internet, servidores, software de gestión.
- Prácticas actuales de ciberseguridad: Uso de antivirus, contraseñas seguras, políticas de respaldo.
- Conocimiento de normas y marcos de ciberseguridad: ISO/IEC 27001, NIST, C2M2.
- Conocimiento de metodologías ágiles: Familiaridad con SCRUM, roles y eventos.
- Disposición al cambio tecnológico: Percepción sobre facilidad de uso y utilidad MODELO DE ACEPTACIÓN DE LA TECNOLOGÍA (Technology Acceptance Model - TAM).
- Capacidades internas: Recursos humanos y técnicos para implementar mejoras.

- Viabilidad y escalabilidad del modelo propuesto: Expectativas, beneficios percibidos.

Instrumento de recolección de datos: Encuesta estructurada para representantes de MiPymes del Huila

Objetivo: Identificar el estado actual de la ciberseguridad, el conocimiento de metodologías ágiles, la disposición al cambio y el nivel de madurez digital en las MiPymes del Huila.

Encuesta estructurada para representantes de las MiPymes.

Nº	Pregunta	Sección	Tipo de respuesta
1	Sector económico de la empresa (Agricultura, Industria, Comercio, Servicios, Otro)	Datos generales	Opción múltiple
2	Tamaño de la empresa (Micro, Pequeña, Mediana)	Datos generales	Opción múltiple
3	Ubicación (Municipio)	Datos generales	Respuesta abierta
4	Número de empleados	Datos generales	Numérica
5	La empresa cuenta con conexión a Internet estable y suficiente para sus operaciones.	Infraestructura tecnológica	Likert 1-5
6	Disponemos de servidores propios o en la nube para gestión de datos.	Infraestructura tecnológica	Likert 1-5
7	Utilizamos software de gestión empresarial (ERP, CRM u otro).	Infraestructura tecnológica	Likert 1-5
8	La infraestructura tecnológica es suficiente para cubrir las necesidades actuales del negocio.	Infraestructura tecnológica	Likert 1-5
9	Todos los equipos cuentan con software antivirus actualizado.	Prácticas de ciberseguridad	Likert 1-5
10	Se utilizan contraseñas seguras y se cambian periódicamente.	Prácticas de ciberseguridad	Likert 1-5
11	Existen políticas formales de respaldo y recuperación de información.	Prácticas de ciberseguridad	Likert 1-5
12	Los empleados reciben capacitación en seguridad informática.	Prácticas de ciberseguridad	Likert 1-5
13	Realizamos auditorías o revisiones periódicas de ciberseguridad.	Prácticas de ciberseguridad	Likert 1-5
14	Conozco los principios básicos de la norma ISO/IEC 27001.	Normas de ciberseguridad	Likert 1-5
15	Estoy familiarizado con el marco NIST de ciberseguridad.	Normas de ciberseguridad	Likert 1-5

16	Conozco el modelo C2M2 para evaluar madurez en ciberseguridad.	Normas de ciberseguridad	Likert 1-5
17	En la empresa se aplican o adaptan estándares reconocidos en ciberseguridad.	Normas de ciberseguridad	Likert 1-5
18	He escuchado o leído sobre la metodología SCRUM.	Metodologías ágiles	Likert 1-5
19	Conozco los roles principales de SCRUM (Product Owner, Scrum Master, Equipo de desarrollo).	Metodologías ágiles	Likert 1-5
20	Entiendo los eventos clave de SCRUM (Sprint, Daily, Review, Retrospective).	Metodologías ágiles	Likert 1-5
21	Hemos implementado prácticas ágiles en algún proyecto empresarial.	Metodologías ágiles	Likert 1-5
22	Considero que adoptar nuevas tecnologías puede mejorar el desempeño de la empresa.	Cambio tecnológico	Likert 1-5
23	Creo que las tecnologías digitales son fáciles de aprender y usar.	Cambio tecnológico	Likert 1-5
24	Estoy dispuesto(a) a invertir tiempo en aprender nuevas herramientas.	Cambio tecnológico	Likert 1-5
25	La dirección de la empresa apoya el cambio tecnológico.	Cambio tecnológico	Likert 1-5
26	La empresa cuenta con personal capacitado en tecnología y ciberseguridad.	Capacidades internas	Likert 1-5
27	Disponemos de recursos financieros para invertir en mejoras tecnológicas.	Capacidades internas	Likert 1-5
28	Contamos con soporte técnico interno o externo confiable.	Capacidades internas	Likert 1-5
29	Podemos implementar mejoras tecnológicas sin afectar gravemente la operación diaria.	Capacidades internas	Likert 1-5
30	Considero viable implementar un modelo de ciberseguridad adaptado a MiPymes.	Viabilidad del modelo	Likert 1-5
31	Creo que el modelo propuesto traerá beneficios medibles para la empresa.	Viabilidad del modelo	Likert 1-5
32	Me parece que este modelo puede adaptarse a diferentes áreas del negocio.	Viabilidad del modelo	Likert 1-5
33	Estoy dispuesto(a) a participar en un proyecto piloto para probar el modelo.	Viabilidad del modelo	Likert 1-5

Nota. La encuesta permitió caracterizar tecnológicamente a las MiPymes y evaluar su nivel de preparación en ciberseguridad, metodologías ágiles y adopción tecnológica. Las preguntas, organizadas por secciones, facilitaron identificar brechas, capacidades internas, percepción de

viabilidad y disposición al cambio, proporcionando insumos clave para ajustar y validar el modelo propuesto.

Escala de respuesta Likert:

1 = Totalmente en desacuerdo

2 = En desacuerdo

3 = Ni de acuerdo ni en desacuerdo

4 = De acuerdo

5 = Totalmente de acuerdo

2. Guía de entrevista semiestructurada para expertos

Objetivo: Profundizar en la percepción de expertos sobre la aplicabilidad de SCRUM a proyectos de ciberseguridad en MiPymes y validar la estructura del modelo propuesto.

Participantes sugeridos: Consultores en ciberseguridad, asesores en transformación digital, docentes investigadores en tecnologías de la información.

Preguntas orientadoras:

- ¿Qué desafíos específicos observa en la gestión de ciberseguridad en MiPymes?
- ¿Considera viable implementar metodologías ágiles como SCRUM en este tipo de organizaciones?
- ¿Qué ventajas y limitaciones identificaría en integrar SCRUM con marcos como NIST o C2M2?
- ¿Cómo percibe la madurez digital de las MiPymes en regiones como el Huila?
- ¿Qué recomendaciones haría para facilitar la escalabilidad del modelo a nivel regional?

3. Formato de observación no participante en MiPymes piloto

Objetivo: Observar de forma estructurada el entorno real de trabajo en las MiPymes seleccionadas para piloto, identificando brechas de seguridad, dinámicas de trabajo y prácticas digitales.

Dimensiones:

- Organización del trabajo: Gestión de tareas, reuniones, uso de tableros físicos o digitales.
- Seguridad operativa: Accesos físicos y lógicos, uso de contraseñas, respaldo de información.
- Herramientas digitales utilizadas: Tipos de software, servicios en la nube, redes sociales.
- Cultura organizacional: Nivel de conciencia en seguridad, apertura al cambio, roles definidos.
- Trazabilidad de procesos: Documentación, seguimiento, métricas o indicadores.
- ¿Deseas que integre estos instrumentos directamente al documento del marco teórico, en una nueva sección o en un anexo metodológico?

Diseño de los instrumentos

La encuesta estructurada estará conformada por 5 secciones:

- Datos generales de la empresa (sector, tamaño, ubicación, antigüedad).
- Nivel de madurez en ciberseguridad, con base en los dominios del C2M2 (gobernanza, gestión de riesgos, protección de activos, etc.).
- Uso de metodologías ágiles, particularmente SCRUM o similares, en procesos internos.

- Capacidades tecnológicas y de innovación, basadas en el modelo TAM (uso percibido, utilidad, facilidad).
- Barreras y oportunidades para la implementación de un modelo de ciberseguridad.

Los ítems serán en su mayoría de tipo cerrado con escala Likert de 5 puntos (1: Totalmente en desacuerdo a 5: Totalmente de acuerdo), combinados con preguntas dicotómicas y de selección múltiple.

La entrevista semiestructurada estará dirigida a expertos en ciberseguridad, transformación digital y metodologías ágiles. El guion incluirá preguntas abiertas organizadas en tres ejes:

- Factores críticos para la implementación de modelos de ciberseguridad en MiPymes.
- Aplicabilidad de marcos ágiles como SCRUM en contextos de seguridad digital.
- Recomendaciones para asegurar la viabilidad y escalabilidad del modelo.

Ambos instrumentos fueron sometidos a validación por juicio de expertos (docentes-investigadores y profesionales del área) y a una prueba piloto con cinco MiPymes del Huila. El índice Alfa de Cronbach para la encuesta fue de 0.84, lo que indica una buena consistencia interna.

Procedimiento para la validación de la encuesta

La validación de la encuesta se desarrolló en dos etapas: validación de contenido y validación de confiabilidad, complementadas con un piloto de aplicación.

1. Validación de contenido

Objetivo: Garantizar que los ítems de la encuesta sean pertinentes, claros y representativos de las variables del estudio.

Procedimiento:

Definición de dimensiones y variables: A partir del marco teórico y los objetivos del estudio, se establecieron las dimensiones e indicadores que la encuesta debía medir.

Elaboración inicial de ítems: Se formularon las preguntas siguiendo criterios de redacción clara, lenguaje comprensible y adecuación cultural.

Evaluación por jueces expertos:

Se seleccionó un panel de 3 expertos en la temática y en metodología de investigación.

Cada juez evaluó la claridad, coherencia, relevancia y suficiencia de cada ítem, usando una escala tipo Likert (por ejemplo, 1 = Muy deficiente, 4 = Excelente).

Se calculó el Índice de Validez de Contenido (IVC) para cada ítem y para la encuesta en general, usando la fórmula de Lawshe:

$$\boldsymbol{IVC} = \frac{\boldsymbol{n_e} - (\boldsymbol{N/2})}{(\boldsymbol{N/2})}$$

donde

$\boldsymbol{n_e}$ es el número de jueces que consideran el ítem esencial y

N es el número total de jueces.

Revisión y ajustes: Se modificaron o eliminaron ítems con IVC menor a 0,66 (umbral recomendado para 3 jueces). Tomando que uno de los jueces no esta de acuerdo con el ítem validado. Normalmente se entendería que el umbral debería ser de 1.0. Pero teneindo en cuanta que no se tienen suficientes personas calificadas en la región para etse tipo de consultas, se tomó como válido este umbral.

2. Validación de confiabilidad

Objetivo: Verificar la consistencia interna de la encuesta.

Procedimiento:

Aplicación piloto: La encuesta se aplicó a un grupo de 15 personas con características similares a la población objetivo.

Análisis estadístico: Se calculó el Alfa de Cronbach para cada dimensión y para el instrumento completo.

Valores recomendados:

≥ 0,70: Aceptable

≥ 0,80: Buena

≥ 0,90: Excelente

Ajustes finales: Ítems con baja correlación ítem-total fueron revisados y, de ser necesario, reformulados o eliminados.

3. Validación final y aplicación

Se consolidó la versión definitiva de la encuesta incorporando las recomendaciones de los expertos y los resultados del análisis de confiabilidad.

La encuesta validada fue aplicada a la muestra definida en el diseño de investigación.

Apéndice B

Modelo de Ciberseguridad Adaptado para MiPymes

En el desarrollo guiado por SCRUM en los grupos de trabajo se alcanza el modelo dentro del marco de Ciberseguridad (CSF – Cybersecurity security Frame – siglas en inglés) del Instituto Nacional de Estándares y Tecnología -NIST, es un esquema voluntario aplicable a negocios de todo tamaño. Se basa en cinco funciones clave: Identificar, Proteger, Detectar, Responder y Recuperar. Aunque las técnicas básicas son similares a las de empresas grandes, las MiPymes deben enfocarse en implementar controles sencillos y escalables (la diferencia principal suele ser la complejidad y los recursos disponibles). Por ejemplo, la FTC/NIST recomienda empezar por "hacer una lista de todos los equipos, programas y datos" que la empresa utiliza, lo que ilustra la función de Identificar para un negocio pequeño. A continuación, se explican cada una de las funciones del NIST con ejemplos prácticos, buenas prácticas, herramientas gratuitas y sugerencias para MiPymes.

Identificar

La función Identificar implica conocer los activos (equipos, datos, procesos) y riesgos de la empresa, de modo que se pueda priorizar la seguridad. Por ejemplo, una pyme de venta al público podría inventariar sus computadoras, teléfonos, terminales de punto de venta y bases de datos de clientes, y clasificar qué información es crítica. Se recomienda usar un inventario básico (por ejemplo, una hoja de cálculo) para registrar dispositivos y programas clave. También conviene definir claramente funciones y responsabilidades: NIST sugiere "elaborar y compartir una política de ciberseguridad" que cubra roles de empleados, proveedores y usuarios. En paralelo, se debe evaluar de forma simple las amenazas y vulnerabilidades de esos activos. Por ejemplo, identificar cuáles son los procesos críticos que debe mantener la empresa (ventas diarias, acceso a datos de

clientes, etc.) y qué podría interrumpirlos. INCIBE ofrece una herramienta gratuita (“Análisis de riesgos en 5 minutos”) que guía paso a paso la revisión de activos principales, lo que puede ayudar a enfocar recursos donde más falta.

Buenas prácticas:

- Mantener actualizado un inventario de hardware y software.
- Identificar los procesos y datos empresariales más críticos (por ejemplo, el sistema de facturación o la base de datos de clientes).
- Definir roles y responsabilidades en una política de seguridad básica.
- Realizar una evaluación de riesgos simple (mes de impacto/probabilidad) para los activos clave.
- Revisar periódicamente cambios en el inventario (nuevos dispositivos o personal nuevo).

Herramientas gratuitas: Plantillas o guías del propio NIST (hoja de cálculo de autoevaluación CSF), o soluciones open-source de inventario como OCS Inventory NG o GLPI (para seguimiento de activos). La herramienta de INCIBE “Análisis de riesgos en 5 minutos” ayuda a dimensionar riesgos. También se pueden usar listas de verificación sencillas (por ejemplo, la lista de chequeo de políticas de INCIBE adaptada a la pyme) para no olvidar ningún activo.

Para personal sin mucha formación técnica: Asignar un responsable (p.ej., el dueño o administrador de la PyME) que dedique un par de horas al mes a validar el inventario y los riesgos. Usar un lenguaje claro, por ejemplo, etiquetas físicas en los equipos y una lista en papel o digital accesible. El experto sugiere cursos gratuitos de INCIBE para microempresas y autónomos como recurso formativo introductorio.

Controles/políticas mínimas: Adoptar una pequeña política de inventario y gestión de activos que establezca quién actualiza la lista y cada cuánto. Crear un documento de seguridad interno breve (como indica NIST) que defina las responsabilidades del personal y las reglas básicas (p.ej. no compartir contraseñas, restricciones de instalación de software). Mantener un registro de amenazas conocidas (por ejemplo, apuntar si se reciben intentos de phishing o robos de dispositivos) ayuda a alimentar la identificación de riesgos.

Proteger

La función Proteger agrupa las contramedidas para evitar que se materialicen los riesgos. En una MiPyME esto incluye controles técnicos sencillos y buenas prácticas de uso. Por ejemplo, instalar un antivirus gratuito (como Windows Defender que viene con Windows 10/11) y mantenerlo actualizado, o usar un software antimalware de reputación (ClamAV, Sophos Home Free, etc.). Se debe controlar el acceso a la red: usar contraseñas robustas y, si es posible, habilitar doble factor de autenticación (p.ej., Google Authenticator para cuentas críticas). Configurar firewalls básicos: el Routers de la oficina suele incluir firewall, y se puede usar un firewall de código abierto (p. ej. pfSense u OPNsense) para segmentar la red y bloquear tráfico no autorizado. Otras prácticas recomendadas: mantener el sistema operativo y las aplicaciones siempre actualizados (idealmente configurando las actualizaciones automáticas); cifrar la información sensible cuando esté almacenada o en tránsito (p.ej. usar VeraCrypt o BitLocker para discos, cifrado TLS en correos/web); hacer copias de seguridad regulares de los datos; y capacitar a todos los usuarios básicos en pautas de seguridad (explicarles la importancia de no abrir correos sospechosos, de cerrar sesión, de guardar mal las contraseñas, etc.).

Buenas prácticas: Controlar quién puede acceder a cada dispositivo (por ejemplo, cada empleado con usuario propio). Actualizar puntualmente los programas y parchear el sistema operativo. Desactivar puertos USB o bloquear dispositivos extraíbles si no son necesarios. Eliminar de forma segura equipos y soportes viejos (borrado criptográfico o destrucción). Mantener un esquema simple de contraseñas fuertes, con recambio periódico, y considerar el uso de un gestor de contraseñas gratuito (p.ej. Bitwarden o KeePass). Capacitar al personal con recursos básicos (por ejemplo, INCIBE ofrece formación gratuita adaptada a pymes).

Herramientas gratuitas: Antivirus como ClamAV o el propio Microsoft Defender; limpiadores de programa maligno como AdwCleaner. Cortafuegos de software gratuitos: el firewall de Windows o firewalls basados en Linux; routers con IPSec/VPN. Gestores de contraseñas gratuitos (Bitwarden, KeePass) y apps de doble factor (Google Authenticator). Para cifrado, VeraCrypt (cifra discos completos). Soluciones de copia de seguridad sin costo: Duplicati (open source) o el respaldo integrado de Windows, con backups cifrados en la nube o en disco externo. INCIBE incluso recopila un catálogo de herramientas gratuitas de seguridad.

Para personal no técnico: Entregar instrucciones muy concretas, p. ej. “poner el candado” significa bloquear la computadora cuando no estén. Evitar jerga. Usar listas de verificación simples (por ejemplo, chequeos al inicio de semana: ¿el PC está actualizado? ¿copia de seguridad reciente?). Si no hay un responsable de TI, podemos designar a alguien (administrativo) que realice las tareas más sencillas o contratar servicios gestionados básicos (mantenimiento remoto). Además, la creación de conciencia es crítica: difundir internamente consejos básicos de seguridad (no conectar USB desconocidos, desconfiar de correos extraños, etc.) es muy útil.

Controles/políticas mínimas: Elaborar una política de contraseñas (longitud mínima, cambio cada X meses, 2FA cuando sea posible). Formalizar un procedimiento de respaldo que

indique dónde y cuándo se guardan datos (por ejemplo, cada noche en un disco externo o en la nube). Definir una política de acceso: solo cuentas autorizadas pueden usar los sistemas, y el empleado debe informar si un equipo es robado o perdido. Por ejemplo, la herramienta gratuita de INCIBE “Políticas de seguridad para la pyme” proporciona plantillas editables para estos aspectos. Incluir en la política básica indicaciones para la eliminación segura de información confidencial (p.ej. cifrar o destruir dispositivos antes de descartar).

Detectar

La función Detectar consiste en monitorear y reconocer anomalías o incidentes que estén ocurriendo. En una MiPyME esto puede hacerse con recursos modestos: por ejemplo, revisar periódicamente los registros (logs) del servidor o del Routers de internet en busca de accesos extraños. Se puede habilitar el registro de eventos en los sistemas operativos y revisar alertas de seguridad del antivirus. Algunas soluciones gratuitas recomendadas son sistemas de detección de intrusos ligeros como Snort o Suricata (open source IDS), o OSSEC (HIDS) para detectar cambios sospechosos en archivos. Para pymes, también existen versiones gratuitas de escáneres de vulnerabilidades (por ejemplo, OpenVAS/GVM o Nessus Essentials) que ayudan a detectar posibles brechas. Otra medida útil es monitorear el uso de cuentas y revisar actividad de red: NIST sugiere “monitorizar sus computadoras para controlar si hay accesos no autorizados” y “revisar su red para controlar conexiones inesperadas”. Deben investigarse inmediatamente cualquier correo de alerta de sistemas, intentos fallidos de acceso o comportamientos inusuales. Herramientas de análisis gratuitos como Wireshark o utilidades de línea de comando (por ejemplo, fail2ban en servidores Linux) pueden ayudar a detectar ataques básicos.

Buenas prácticas: Probar y actualizar procesos de detección (según sugiere NIST). Revisar con frecuencia los logs de acceso de los sistemas críticos (VPN, correo, servidores) para identificar

actividad inusual. Configurar alertas automáticas básicas (por ejemplo, avisos por correo si ocurre un login fallido repetido). Realizar periódicamente escaneos de vulnerabilidades gratuitos para detectar puntos débiles conocidos. Con pocos recursos, puede bastar un programa de antivirus que escanee en tiempo real y genere alertas al correo del administrador.

Herramientas gratuitas: IDS/IPS de código abierto como Snort, Suricata o la distribución Security Onion (en un PC viejo). Sistemas de correlación y análisis de logs: plataformas open source como ELK/Elastic Stack (puede ser pesadas) o Graylog (hay versión gratuita). Escáneres de red gratis: Nmap para descubrir dispositivos, OpenVAS/GVM para vulnerabilidades, Nessus Essentials (limitado a 16 IP). Para detección de malware: VirusTotal (web) o Metadefender OTX para consultas de archivo/URL. Servicios de reputación de IPs (como los que ofrece Malwarebytes) pueden complementar. En general, cualquier herramienta de seguridad que ofrezca función de alerta sin costo ayuda al monitoreo continuo.

Para personal no técnico: Definir un procedimiento sencillo de reporte interno: cualquier usuario debe avisar si su equipo actúa raro (pop-ups, rendimiento anormal) o si recibe correos sospechosos. Puede usarse un registro de incidentes (en papel o electrónico) donde se anote cada anomalía, por simple que sea. Formar a los empleados para que sepan reconocer las señales básicas de un ataque (pantallas de Ransomware, mensajes extraños, etc.) y a quién avisar inmediatamente. Este enfoque de “vigilancia ciudadana” multiplica la detección con bajo costo.

Controles/políticas mínimas: Implementar una pequeña política de monitoreo interna. Por ejemplo, designar a alguien responsable de revisar semanalmente los logs clave y documentar las revisiones. Mantener habilitado el registro de auditoría en sistemas (para poder buscar luego en caso de incidente). Definir un procedimiento de notificación interna rápido: todos los empleados deben saber a quién contactar si observan algo extraño (puede ser un correo del administrador de

IT o incluso un canal de mensajería interno). Esto forma parte del perfil de respuesta y garantiza que los incidentes se detecten cuanto antes.

Responder

La función Responder abarca las acciones a tomar cuando ya ocurre un incidente de seguridad. Incluye ejecución de un plan de respuesta, contención y comunicación. Por ejemplo, ante un ataque de Ransomware, hay que desconectar rápidamente las máquinas afectadas para limitar daños. NIST recomienda "implementar un plan para notificar a clientes/empleados cuyos datos puedan estar en riesgo, mantener las operaciones y reportar el ataque a las autoridades". Asimismo, debe investigarse y contenerse el ataque (p.ej. eliminando malware) y luego actualizar las políticas internas con las lecciones aprendidas. Es muy importante probar este plan periódicamente ("ponga a prueba su plan con regularidad"), por ejemplo, realizando simulacros o ejercicios con el equipo de la empresa.

Buenas prácticas: Elaborar un plan de respuesta a incidentes sencillo que detalle quién hace qué (p.ej. qué hacer si detectamos un virus o se filtra un correo de phishing). Preparar plantillas de comunicaciones (email o SMS) para informar rápidamente a empleados y clientes afectados. Incluir en el plan pasos de contención básicos: aislar máquinas comprometidas, bloquear cuentas, cambiar contraseñas administrativas y restaurar servicios críticos. Practicar al menos una vez al año (aunque sea informalmente) para asegurarse de que todos saben sus tareas. Tras cualquier incidente, revisar qué falló y actualizar el plan con esas lecciones.

Herramientas gratuitas: No existen "bots" que respondan solos, pero pueden usarse checklists y guías existentes. Por ejemplo, descargar plantillas del NIST (publicaciones CSF o IR plan templates) o de INCIBE (guía de respuesta a incidentes) como referencia. Para coordinar la respuesta, usar canales gratuitos de comunicación internos (correo masivo interno, WhatsApp de

empresa, etc.). Si el ataque es vía correo, emplear herramientas gratuitas de escaneo de emails (por ejemplo, MailScanner en Linux) para limpiar archivos. Guardar evidencia con software de captura de logs (p.ej. syslog) y herramientas forenses básicas (como la versión gratuita de OSForensics o Autopsy) para análisis posterior.

Para personal no técnico: Dejar instrucciones muy concretas: si se detecta algo raro, lo primero es "apagar y desconectar" y luego informar. Mantener un contacto de emergencia (teléfono o correo) con el proveedor de TI local o incluso con el CERT nacional. Capacitar en la notificación de incidentes: cualquier empleado debe saber cómo reportar rápidamente un problema. Tener registrados los datos de los contactos clave (soporte técnico, banca, policía) en papel impreso por si las redes no funcionan. Básicamente, simplificar la toma de decisiones: un diagrama de flujo con «Si pasa A, haz B, y avisa a C».

Controles/políticas mínimas: Adoptar una política de respuesta a incidentes básica. En ella se debe incluir al menos un procedimiento de notificación interno/externo (¿a quién llamamos si hay un ataque? por ejemplo, al CERT y a la Policía) y un plan de acción (pasos iniciales en caso de emergencia). Otra política útil es la del cambio y prueba del plan (asignar fechas anuales para simular un incidente). Documentar todo incidente ocurrido (lo que se conoce como bitácora de incidentes) ayuda a cumplir con futuras auditorías y a mejorar prácticas. INCIBE dispone de plantillas editables de «políticas de seguridad para la pyme» con checklists para estos procesos.

Recuperar

La función Recuperar se refiere a restaurar la operativa normal después de un incidente. Para una MiPyME esto implica, por ejemplo, reparar y restaurar equipos afectados (recuperar datos de las copias de seguridad). Si se dispone de backups, hay que verificar integridad y restaurar el sistema lo antes posible. NIST aconseja que, después de un ataque, se "[repare y restaure] los

equipos y partes de la red afectadas" y se "mantenga informados a empleados y clientes" sobre las acciones de recuperación. La comunicación continua (por ej. avisando cuándo volverá el servicio) mantiene la confianza y orden interno. Además, es fundamental revisar los fallos que permitieron el incidente y reforzar la protección (por ejemplo, instalar un parche o cambiar políticas).

Buenas prácticas: Seguir la regla 3-2-1 de backups: al menos 3 copias de los datos, en 2 medios distintos, 1 copia fuera de sitio (offline). Probar regularmente las restauraciones (no basta con hacer backups, hay que asegurarse de que se pueden recuperar). Mantener copias de múltiples versiones para poder retroceder antes del ataque. Proteger las copias de seguridad con cifrado y control de acceso (no serviría de nada si también son víctimas del ataque). Al volver a la normalidad, restablecer contraseñas y credenciales comprometidas y hacer seguimiento de la recuperación (asegurar que todos los sistemas funcionan correctamente).

Herramientas gratuitas: Software de backup gratuito como Duplicati (open source, copia en la nube) o Windows Backup integrado. Para pymes con recursos medios, Macrium Reflect Free o Veeam Community Edition son opciones para respaldar discos/servidores. Si se usan servicios en la nube (Drive, OneDrive, Dropbox), aprovechar sus funciones de versionado. En caso de emergencias, hay distribuciones Linux de rescate (p.ej. SystemRescueCD) gratuitas que permiten montar discos dañados y recuperar archivos. Herramientas de sincronización en local (por ejemplo rsync en Linux) también ayudan a mantener una copia de respaldo sencilla.

Para personal no técnico: Explicar paso a paso el proceso de restauración al responsable asignado. Mantener una copia impresa de las credenciales de acceso crítico (o en gestor de contraseñas) para no depender de sistemas caídos. Designar un punto de contacto (p.ej. el proveedor de TI o un empleado senior) que tome decisiones si surge la recuperación. Instruir al

personal en prácticas de almacenamiento (por ejemplo, guardar archivos importantes en carpetas sincronizadas automáticamente) para facilitar la recuperación.

Controles/políticas mínimas: Definir una política de respaldo (¿qué datos respaldar, con qué frecuencia, dónde guardarlos). Incluir un plan de continuidad mínimo: por ejemplo, un instructivo para iniciar servicios críticos en otro servidor en caso de fallo (aunque sea muy básico). Documentar los procedimientos de recuperación de cada sistema importante (p.ej. pasos para restaurar la base de datos de facturación). La política de copias de seguridad puede ser un solo documento que indique responsables, programación y ubicación de respaldos. INCIBE menciona que los respaldos deben protegerse con cifrado y control de acceso, lo cual es una consideración clave para no crear un nuevo punto vulnerable.

Modelo de Ciberseguridad basado en el NIST para su Incorporación en un Sistema Integrado de Seguridad de la Información (SISI) para MiPymes

1. Nombre del Modelo

Modelo de Ciberseguridad NIST adaptado a MiPymes para un Sistema Integrado de Seguridad de la Información (SISI)

2. Estructura del Sistema Integrado con base en el NIST

Estructura del Sistema Integrado con base en el NIST

Funciones del NIST	Procesos del SISI	Política Asociada	Indicadores Sugeridos
Identificar	Inventario de activos, evaluación de riesgos, clasificación de la información	Gestión de activos y de riesgos	% activos identificados, % información clasificada, nº revisiones de riesgo/año
Proteger	Gestión de accesos, protección de datos, capacitación, respaldos	Acceso lógico, cifrado, formación, respaldo	% usuarios con 2FA, nº sesiones formativas, frecuencia de backups
Detectar	Monitoreo, análisis de logs, detección de anomalías	Monitoreo y auditoría	Tiempo medio de detección, nº alertas críticas/mes

Responder	Gestión de incidentes, comunicación y reporte	Respuesta a incidentes	Tiempo medio de respuesta, nº de incidentes, simulacros realizados
Recuperar	Restauración de servicios, continuidad, mejora	Continuidad y recuperación	Tiempo de recuperación, % datos restaurados, revisiones posts-incidentes

Nota. Se integra las funciones del NIST con los procesos operativos del Sistema Integrado de Seguridad de la Información, articulando políticas y métricas clave. Esta estructura permite gestionar la ciberseguridad de forma completa: identificar, proteger, detectar, responder y recuperar. Los indicadores propuestos facilitan el seguimiento continuo y la mejora del desempeño en cada dominio.

3. Componentes Clave del Sistema Integrado

a) Políticas:

- Seguridad de la información
- Uso aceptable de TI
- Clasificación y control de activos
- Continuidad del negocio y gestión de incidentes

b) Procedimientos:

- Evaluación de riesgos
- Control de accesos
- Copias de seguridad y restauración
- Detección y respuesta a incidentes
- Auditorías y registros

c) Roles y Responsabilidades:

- Responsable de Seguridad de la Información (RSI)

- Encargado de Monitoreo
- Usuarios con formación periódica
- Comite de Seguridad (si aplica)

d) Gestión Documental:

- Inventario de activos
- Registro de incidentes
- Registro de respaldos
- Logs de acceso y revisión
- Evidencia de formación y monitoreo

4. Integración con ISO/IEC 27001

Integración de NIST con ISO/IEC 27001

Funciones NIST	Controles ISO 27001 Relacionados
Identificar	A.5, A.6, A.8: Políticas, roles, activos
Proteger	A.9, A.10, A.12: Accesos, cifrado, operaciones
Detectar	A.12.4: Registro y monitoreo
Responder	A.16: Gestión de incidentes
Recuperar	A.17: Continuidad del negocio

Nota. La integración entre NIST e ISO/IEC 27001 permite alinear prácticas operativas con controles formalizados. Cada función del NIST se corresponde con controles clave de la norma, fortaleciendo la gestión de activos, accesos, monitoreo, incidentes y continuidad. Esta relación garantiza un enfoque coherente, complementario y más robusto para la seguridad de la información en MiPymes.

5. Herramientas Gratuitas o de Bajo Costo

- Gestión de activos: GLPI, OCS Inventory

- Protección: Defender, ClamAV, Bitwarden, VeraCrypt
- Respaldo: Duplicati, Macrium Reflect Free
- Monitoreo: Snort, OSSEC, Suricata, Nmap
- Capacitación: cursos de ciberseguridad
- Respuesta y recuperación: Planillas del NIST, o similares

6. Ciclo de Mejora Continua (PDCA)

- Plan (Planificar): Definir marco, riesgos, controles y objetivos.
- Do (Hacer): Implementar políticas, herramientas y controles.
- Check (Verificar): Auditoría interna, seguimiento de incidentes e indicadores.
- Act (Actuar): Revisar y mejorar el sistema, corregir desviaciones, actualizar documentación.

Este modelo proporciona una estructura viable y escalable para MiPymes, facilitando la protección de la información y la preparación ante riesgos, con recursos ajustados a sus capacidades. Puede implementarse de forma progresiva y vincularse con auditorías internas, informes regulatorios o procesos de mejora continua.

Niveles de Madurez del Modelo de Ciberseguridad

Niveles de maduración del modelo

Nivel	Descripción	Características clave	Indicadores comunes
1. Inicial (Reactivo)	No hay procesos definidos ni documentación formal. Se actúa solo cuando ocurre un incidente.	No existen políticas escritas, no hay responsables de ciberseguridad. Las medidas son puntuales o reactivas.	Ausencia de políticas, tiempo alto de respuesta, incidentes no documentados.

2. Básico (Informalmente gestionado)	Se han empezado a implementar controles básicos, con procesos no estandarizados.	Hay algunos registros (inventario, backups), formación básica al personal. Políticas mínimas.	% de activos identificados, backups regulares, antivirus actualizado.
3. Definido (Formalizado)	Políticas y procedimientos definidos, roles claros, protección activa de sistemas.	Manual de seguridad, procedimientos operativos, respuesta a incidentes definida.	% usuarios con 2FA, nº de sesiones formativas/año, políticas documentadas.
4. Gestionado (Medido y supervisado)	Se hace seguimiento a la eficacia de las medidas. Se monitorean incidentes y se mejora con base en datos.	Auditorías internas, indicadores de desempeño, plan de continuidad probado.	Nº de incidentes detectados/mes, tiempo medio de recuperación, reporte de auditorías.
5. Optimizado (Mejora continua)	La seguridad es parte de la cultura. Se realiza análisis proactivo, pruebas periódicas y adaptación constante.	Simulacros, automatización de procesos, revisión estratégica de políticas.	Nivel de conformidad con ISO 27001, frecuencia de pruebas, inversión en formación.

Nota. Se evidencia que los niveles de maduración permiten evaluar el progreso de las MiPymes desde un estado reactivo hasta una cultura optimizada de ciberseguridad. Cada nivel describe procesos, responsabilidades e indicadores asociados, facilitando medir avances reales. Este marco orienta la mejora continua y permite identificar brechas, priorizar acciones y consolidar prácticas estables y sostenibles en el tiempo.