Ciencia y Reflexión
Revista Científica Multidisciplinaria

Recibido: 23/12/2025
Aprobado: 26/03/2026

DOI: https://doi.org/10.70747/cr.v5i1.999

Desarrollo de un Modelo de Ciberseguridad basado en Scrum para MiPyMEs del Huila: Una Propuesta de Gestión Ágil para la Resiliencia Digital

Hernando Arbey Robles Puentes
haroblesp@unadvirtual.edu.co
https://orcid.org/0000-0002-2790-0864
Universidad Nacional Abierta y a Distancia - UNAD
Neiva - Colombia

Freskmann Danilo Silva Marín
freskdasilva99@gmail.com
https://orcid.org/0009-0009-2033-8408
Universidad Nacional Abierta y a Distancia - UNAD
Neiva - Colombia

Jaime Rubiano Llorente
jaimerubiano1961@gmail.com
https://orcid.org/0000-0002-5490-3497
Universidad Nacional Abierta y a Distancia - UNAD
Neiva - Colombia

Pablo Francisco Hernández Lugo
pablof.hernandez@unad.edu.co
https://orcid.org/0000-0001-9892-9288
Universidad Nacional Abierta y a Distancia - UNAD
Neiva - Colombia

Pedro Torres Silva
pedro.torress@unad.edu.co
https://orcid.org/0000-0003-3649-2281
Universidad Nacional Abierta y a Distancia - UNAD
Neiva - Colombia

Rodolfo Andrés Villarreal Pazos
rodolfoandresvillarrealpazos@gmail.com
https://orcid.org/0009-0005-2119-9084
Universidad Nacional Abierta y a Distancia - UNAD
Neiva - Colombia

RESUMEN

Las micro, pequeñas y medianas empresas (MiPyMEs) del departamento del Huila enfrentan un aumento sostenido del riesgo cibernético, impulsado por la digitalización acelerada y por limitaciones comunes en talento, presupuesto y capacidad tecnológica. Este artículo presenta el diseño de un modelo de ciberseguridad apoyado en el marco de trabajo Scrum, orientado a implementar controles de seguridad de manera incremental y priorizada, de acuerdo con la madurez digital de cada organización. Se desarrolló un diagnóstico mediante encuestas (n=20), entrevistas semiestructuradas (n=10) y observación directa, con el fin de identificar brechas en gobernanza, prácticas técnicas y cultura de seguridad. Los resultados evidenciaron ausencia de políticas formalizadas (85%) y baja capacitación (20%), con prácticas concentradas en antivirus (80%) y contraseñas (60%). A partir de estos hallazgos se estructuró un modelo cíclico que traduce las brechas en un backlog de seguridad y las gestiona por sprints, integrando lineamientos de NIST CSF e ISO/IEC 27001 y criterios de madurez C2M2 para priorizar inversiones. Se concluye que el enfoque ágil es pertinente para Las micro, pequeñas y medianas empresas (MiPyMEs) por su escalabilidad, su énfasis en entrega continua de valor y su potencial para fortalecer la resiliencia digital.

Palabras clave: *seguridad informática, pequeñas y medianas empresas, gestión de proyectos, métodos ágiles, transformación digital*

Los autores declaran no tener conflicto de intereses.

El Editor y los Revisores declararon no tener conflicto de intereses.

Development of a Cybersecurity Model based on Scrum for Micro, Small, and Medium Enterprises in Huila: An Agile Management Solution for Digital Resilience

ABSTRACT

Micro, small, and medium-sized enterprises (MSMEs) in Huila, Colombia, face rising cybersecurity risk driven by rapid digitalization and constrained human, financial, and technological resources. This paper presents the design of a cybersecurity model supported by the Scrum framework, aiming to implement security controls incrementally and by priority according to each organization's digital maturity. A baseline assessment was conducted through surveys (n=20), semi-structured interviews (n=10), and direct observation to identify gaps in governance, technical practices, and security culture. Findings showed a lack of formalized cybersecurity policies (85%) and limited security training (20%), while common practices were mostly limited to antivirus use (80%) and strong passwords (60%). Based on these results, an iterative model was structured to transform gaps into a security backlog managed through sprints, integrating NIST CSF and ISO/IEC 27001 guidance and C2M2 maturity criteria to prioritize investments. The model suggests that an agile approach is suitable for MSMEs due to scalability, continuous value delivery, and its potential to strengthen digital.

Keywords: *information security, small and medium enterprises, project management, agile methods, digital transformation*

The authors declare no conflict of interest.

The Editor and the Reviewers declared no conflict of interest.

INTRODUCCIÓN

El crecimiento acelerado de la digitalización en los procesos empresariales (facturación, ventas en línea, medios de pago, almacenamiento en la nube y comunicación con clientes) ha ampliado la superficie de ataque de las organizaciones. En este escenario, las micro, pequeñas y medianas empresas (MiPyMEs) suelen estar expuestas de manera desproporcionada: la evidencia reciente muestra que sus principales barreras para fortalecer la ciberseguridad se relacionan con baja alfabetización en riesgos, restricciones presupuestarias y falta de soluciones realmente ajustadas a su contexto operativo (Rombaldo Junior et al., 2025).

En Colombia, la adopción de tecnologías digitales avanza, pero con brechas significativas en capacidades de gestión y control. Informes nacionales sobre madurez digital evidencian avances heterogéneos entre sectores y tamaños empresariales, donde las micro, pequeñas y medianas empresas (MiPyMEs) tienden a reportar mayores dificultades para institucionalizar prácticas de seguridad de la información (CINTEL, 2023). En el departamento del Huila con un tejido empresarial dominado por unidades productivas pequeñas y de servicios estas limitaciones se combinan con dinámicas de competitividad local que presionan la continuidad del negocio y la confianza del cliente (Cámara de Comercio del Huila, 2025).

Más allá de la tecnología, la literatura coincide en que la resiliencia digital depende de factores humanos y organizacionales: cultura, roles claros, aprendizaje continuo, toma de decisiones y coordinación interfuncional. Revisiones y estudios recientes resaltan que los “errores humanos” suelen ser consecuencia de diseños organizacionales deficientes y de estrategias de formación no sostenidas, por lo que se requiere una aproximación socio-técnica que integre procesos, personas y controles técnicos. (Khadka & Ullah, 2025; Colabianchi et al., 2025).

Frente a este desafío, marcos de referencia como el NIST Cybersecurity Framework 2.0 y normas de sistemas de gestión como ISO/IEC 27001:2022 ofrecen una estructura para

identificar, priorizar e implementar controles; no obstante, su adopción suele resultar compleja para organizaciones con recursos limitados, baja especialización y escasa formalización documental. En respuesta, diversos trabajos académicos han propuesto adaptar y simplificar enfoques de evaluación y gestión del riesgo específicamente para PYMEs, reconociendo la necesidad de herramientas prácticas, incrementales y de fácil trazabilidad (El-Hajj & Mirza, 2024).

En paralelo, los enfoques ágiles aportan mecanismos de gestión que favorecen la entrega incremental, la priorización basada en valor y la retroalimentación continua.

En el ámbito de seguridad, se han documentado extensiones de Scrum y propuestas de "secure Scrum" que incorporan actividades, criterios y artefactos para hacer visible el trabajo de seguridad (p. ej., ítems de backlog, criterios de aceptación y definición de terminado), reduciendo el riesgo de que la seguridad compita y se diluya frente a otras demandas funcionales (Maier et al., 2017; Pohl & Hof, 2015; Türpe & Poller, 2017). Asimismo, se han planteado aproximaciones que combinan NIST CSF con prácticas ágiles para organizar la mejora continua de la gestión de ciberseguridad a través de sprints y un backlog priorizado (Lampe et al., 2021; Asprion et al., 2023).

Con base en lo anterior, este artículo se enfoca en Las micro, pequeñas y medianas empresas (MiPyMEs) del departamento del Huila (Colombia) y delimita el estudio al levantamiento diagnóstico y diseño del modelo durante el año 2025. En este marco, se plantea la siguiente pregunta de investigación: ¿cómo estructurar un modelo de ciberseguridad basado en Scrum, alineado con NIST CSF e ISO/IEC 27001, que permita a Las micro, pequeñas y medianas empresas (MiPyMEs) priorizar e implementar controles de forma incremental y verificable? Como hipótesis de trabajo (H1), se propone que la traducción de brechas de seguridad a un backlog priorizado y ejecutado por sprints, con evidencias mínimas por incremento, mejora la

viabilidad de adopción de prácticas de ciberseguridad en Las micro, pequeñas y medianas empresas (MiPyMEs) con restricciones de tiempo, presupuesto y talento especializado.

A pesar de la existencia de marcos ampliamente reconocidos como el NIST Cybersecurity Framework y la norma ISO/IEC 27001, su implementación en micro, pequeñas y medianas empresas (MiPyMEs) presenta limitaciones significativas debido a su complejidad técnica, requerimientos de formalización y demanda de recursos especializados. Si bien la literatura ha propuesto enfoques simplificados para pequeñas organizaciones, persiste una brecha en la integración de metodologías ágiles que permitan operacionalizar la ciberseguridad de manera incremental, adaptable y alineada con las capacidades reales de estas empresas. En particular, se identifica la ausencia de modelos aplicados que articulen marcos de referencia en ciberseguridad con prácticas ágiles como Scrum en contextos regionales específicos, como el departamento del Huila. En este sentido, la presente investigación busca contribuir al cierre de este vacío mediante el diseño de un modelo de ciberseguridad basado en gestión ágil, orientado a facilitar la adopción progresiva de controles de seguridad en MiPyMEs.

MATERIALES Y MÉTODOS

Enfoque y diseño

Se desarrolló un estudio de enfoque mixto (cuantitativo–cualitativo), de alcance descriptivo y aplicado, cuyo propósito fue analizar el nivel de madurez en ciberseguridad de las micro, pequeñas y medianas empresas (MiPyMEs) del departamento del Huila y, a partir de ello, diseñar un modelo de mejora incremental basado en Scrum, alineado con marcos de referencia en ciberseguridad. La recolección de información se realizó durante el periodo comprendido entre enero y junio de 2025.

Población, muestra y muestreo

La población objetivo estuvo conformada por micro, pequeñas y medianas empresas

(MiPyMEs) del departamento del Huila (Colombia) con uso operativo de tecnologías de la información y comunicación, tales como correo corporativo, herramientas ofimáticas, sistemas de facturación, servicios en la nube o presencia web.

Se empleó un muestreo no probabilístico por conveniencia, complementado con selección intencional de informantes clave, considerando las limitaciones de acceso y disponibilidad de las organizaciones. La muestra estuvo conformada por 20 empresas para la aplicación de la encuesta diagnóstica y 10 entrevistas semiestructuradas dirigidas a personal con roles directivos, administrativos o responsables de tecnologías de la información.

Aunque el tamaño de la muestra es reducido, se considera adecuado para estudios de carácter exploratorio y descriptivo en contextos regionales, permitiendo identificar tendencias, brechas y oportunidades de mejora en ciberseguridad.

En cuanto a su caracterización, las empresas participantes pertenecen a los sectores de comercio (45%), servicios (35%) y actividades productivas (20%). En términos de tamaño, el 60% corresponde a microempresas, el 30% a pequeñas empresas y el 10% a medianas empresas.

Instrumentos y escala

Para la recolección de información se emplearon tres instrumentos: una encuesta diagnóstica, una entrevista semiestructurada y una lista de verificación de evidencias.

El instrumento de encuesta estuvo compuesto por 32 ítems distribuidos en seis dimensiones: gobernanza, factor humano, protección básica, gestión de accesos, continuidad del negocio y respuesta a incidentes. Este instrumento permitió evaluar el nivel de madurez en ciberseguridad de las organizaciones participantes.

Las entrevistas semiestructuradas se orientaron a profundizar en prácticas reales, limitaciones, percepciones y cultura organizacional frente a la seguridad de la información. Por su parte, la

lista de verificación de evidencias permitió contrastar la información declarada con soportes documentales, configuraciones técnicas y prácticas observables.

La encuesta utilizó una escala tipo Likert de cinco puntos, donde 1 corresponde a no implementado, 2 a nivel inicial o ad hoc, 3 a parcialmente implementado, 4 a implementado y estandarizado, y 5 a implementado, medido y en mejora continua.

Criterio de evaluación de madurez

Para la evaluación del nivel de madurez en ciberseguridad, se empleó una escala operativa de cinco niveles, adaptada de modelos de madurez como el Cybersecurity Capability Maturity Model (C2M2). Esta escala permitió clasificar el grado de implementación de prácticas de seguridad en las organizaciones participantes.

Los niveles de madurez se definieron de la siguiente manera:

Nivel 1: prácticas no implementadas o de carácter ad hoc.

Nivel 2: prácticas básicas, repetibles y con documentación mínima.

Nivel 3: prácticas definidas e implementadas de manera consistente.

Nivel 4: prácticas gestionadas y medidas mediante indicadores.

Nivel 5: prácticas optimizadas con procesos de mejora continua.

Esta clasificación facilitó la evaluación comparativa entre organizaciones y permitió establecer una línea base para la priorización de acciones de mejora.

Validez y confiabilidad

La validez de contenido del instrumento se aseguró mediante la evaluación de tres expertos en ciberseguridad y gestión de tecnologías de la información, quienes analizaron la pertinencia, claridad y coherencia de los ítems. A partir de sus observaciones, se realizaron ajustes en la redacción y estructura del instrumento.

Adicionalmente, se llevó a cabo una prueba piloto para verificar la comprensión de los ítems

y el tiempo de aplicación.

La confiabilidad del instrumento se evaluó mediante el coeficiente alfa de Cronbach, obteniendo un valor global de $\alpha = 0{,}81$, lo cual indica un nivel adecuado de consistencia interna.

Procedimiento

El desarrollo de la investigación se estructuró en cuatro fases articuladas. En primer lugar, se realizó el diagnóstico mediante la aplicación de encuestas, entrevistas y verificación de evidencias. Posteriormente, se llevó a cabo el análisis de brechas por dimensión, utilizando estadísticas descriptivas y contrastes cualitativos.

En una tercera fase, las brechas identificadas fueron traducidas en un backlog de ciberseguridad, formulando ítems accionables con criterios de aceptación y evidencias mínimas de cumplimiento. Finalmente, se realizó la priorización del backlog considerando criterios de impacto en el riesgo, dependencias y esfuerzo requerido, lo cual permitió definir una ruta de implementación basada en sprints.

Análisis de datos

El análisis de datos cuantitativos se realizó mediante estadística descriptiva, utilizando herramientas como Microsoft Excel para el cálculo de frecuencias, porcentajes y niveles de madurez por dimensión. La información cualitativa fue procesada mediante análisis temático, identificando patrones y categorías emergentes relacionadas con gobernanza, cultura organizacional, capacidades técnicas y barreras en la implementación de prácticas de ciberseguridad. Este análisis se desarrolló a partir de la codificación manual de la información recolectada. La integración de los enfoques cuantitativo y cualitativo se llevó a cabo mediante triangulación, permitiendo consolidar los hallazgos y fortalecer la validez de los resultados obtenidos.

RESULTADOS

Resultados del diagnóstico

Brechas en políticas y cultura organizacional

El diagnóstico evidenció que el 85% de las empresas participantes no cuenta con políticas de ciberseguridad formalizadas, lo cual refleja debilidades en la gobernanza. En cuanto a prácticas técnicas, el uso de antivirus (80%) y la adopción de contraseñas seguras (60%) se identifican como las medidas más comunes. Sin embargo, la capacitación en seguridad es limitada, ya que solo el 20% de las empresas reportó acciones formativas, lo que incrementa el riesgo asociado al factor humano.

En términos generales, el nivel de madurez digital promedio se ubicó en un nivel intermedio (nivel 3), lo que indica que las organizaciones cuentan con prácticas parcialmente estructuradas, pero aún presentan oportunidades de mejora en estandarización, medición y optimización de sus procesos de ciberseguridad.

Tabla 1. Diagnóstico de ciberseguridad en Las micro, pequeñas y medianas empresas (MiPyMEs): evidencias, resultados y nivel de madurez

Dimensión	Evidencia del diagnóstico	Resultado	Nivel de madurez (1–5)	Implicación / prioridad sugerida
Gobernanza (políticas)	Política formal documentada y aprobada	85% sin políticas formalizadas	2	Alta: define reglas, roles y criterios mínimos
Factor humano (capacitación)	Plan de sensibilización/inducción	Solo 20% reportó capacitación	2	Alta: reduce phishing y errores operativos
Protección básica	Antivirus/EDR instalado y actualizado	80% usa antivirus	—	Media: complementar con actualizaciones y hardening

Gestión de accesos	Contraseñas fuertes/gestión de cuentas	60% adopta contraseñas seguras	—	Media-alta: fortalecer MFA y mínimos de acceso
Madurez digital global	Evaluación global por rúbrica	Promedio nivel 3	3	Ruta por sprints: consolidar base y medir avances

Nota. la tabla sintetiza los hallazgos del diagnóstico por dimensiones (gobernanza, factor humano, protección y accesos) y su nivel de madurez estimado (1–5). Las implicaciones orientan la priorización de acciones por sprints, privilegiando controles base de gobernanza y formación para reducir riesgos frecuentes y elevar la capacidad de respuesta.

Modelo de ciberseguridad basado en Scrum

El modelo propuesto concibe la ciberseguridad como un proceso de mejora continua. A partir del diagnóstico, las brechas se transforman en un Product Backlog de Seguridad, priorizado por impacto, probabilidad, costo-esfuerzo y nivel de madurez. Cada sprint entrega un incremento verificable (por ejemplo, política aprobada, procedimiento operativo, control técnico implementado o evidencia de capacitación).

De brechas a backlog: mecanismo de traducción

El paso clave del modelo consiste en transformar hallazgos del diagnóstico en ítems accionables del Product Backlog de Seguridad. Para ello se propone: (1) redactar cada brecha como necesidad de negocio (qué se protege y por qué importa), (2) ubicarla en una función del CSF (Govern, Identify, Protect, Detect, Respond, Recover), (3) asociar controles de referencia de ISO/IEC 27001:2022 (Anexo A) y buenas prácticas, (4) estimar esfuerzo y dependencias, y (5) priorizar con criterios simples: impacto, probabilidad, urgencia regulatoria/contractual y costo-esfuerzo.

A continuación, se presenta un ejemplo ilustrativo de backlog mínimo (MVS: Minimum Viable Security) que suele ser viable en Las micro, pequeñas y medianas empresas (MiPyMEs) en ciclos cortos. Los ítems deben

adaptarse a la realidad y a los riesgos específicos de cada empresa.

Tabla 2. Product Backlog de Ciberseguridad: ítems priorizados, mapeo al NIST CSF y evidencias de cumplimiento

Ítem de backlog (incremento esperado)	Función CSF	Tipo (gob./proc./téc./personas)	Evidencia de cumplimiento	Criterio de priorización
Política básica de seguridad aprobada y socializada	Govern	Gobernanza	Documento + acta + comunicado	Obligatorio (base de gobernanza)
Inventario de activos críticos (equipos, cuentas, datos)	Identify	Proceso	Listado versionado + responsables	Impacto (visibilidad de riesgo)
Gestión de accesos: cuentas nominativas y mínimos de privilegio	Protect	Proceso/Técnico	Matriz de accesos + revisión	Riesgo (credenciales)
Activación de MFA en correo y aplicaciones críticas	Protect	Técnico	Capturas/registro de configuración	Probabilidad (phishing)
Rutina de actualizaciones y parches (mensual) definida	Protect	Proceso	Calendario + bitácora	Reducción de vulnerabilidades
Copias de seguridad y prueba de restauración	Recover	Técnico/Proceso	Registro de backups + evidencia de prueba	Continuidad del negocio
Plan y roles de respuesta a incidentes (mínimo)	Respond	Gobernanza	Procedimiento + roles + contactos	Tiempo de respuesta

Capacitación corta anti-phishing y reporte de incidentes	Protect	Personas	Lista asistencia + evaluación breve	Factor humano
Registro básico de eventos y revisión periódica	Detect	Técnico	Logs habilitados + checklist	Detección temprana
Simulacro de incidente y retrospectiva de mejora	Respond/Recover	Proceso	Acta simulacro + acciones	Aprendizaje continuo

Nota. los ítems representan incrementos mínimos viables por sprint para Las micro, pequeñas y medianas empresas (MiPyMEs). Cada elemento se vincula a una función del NIST CSF y a un tipo de control (gobernanza, proceso, técnico o personas). La priorización combina obligatoriedad, impacto, riesgo y continuidad del negocio.

Métricas mínimas para seguimiento

Para evitar que el modelo se convierta en "cumplimiento documental", se propone medir avances con indicadores simples y trazables por sprint, por ejemplo: porcentaje de ítems del backlog completados con evidencia, porcentaje de usuarios con MFA habilitado, porcentaje de personal capacitado, porcentaje de copias de seguridad con prueba de restauración, tiempo promedio para aplicar parches críticos y número de incidentes reportados y gestionados con procedimiento.

Cadencia y alcance sugeridos

En Las micro, pequeñas y medianas empresas (MiPyMEs) suele funcionar una cadencia de sprints de 2 a 4 semanas, con objetivos realistas. El primer sprint debe apuntar a un "mínimo viable" (gobernanza básica + controles de alto impacto) y, a partir de allí, iterar hacia controles más avanzados. La retrospectiva permite ajustar la carga de trabajo al ritmo real del negocio.

Fases iterativas

Diagnóstico inicial: evaluación rápida de postura de seguridad y madurez digital.

Planificación y priorización: selección de brechas/controles de mayor impacto para el sprint

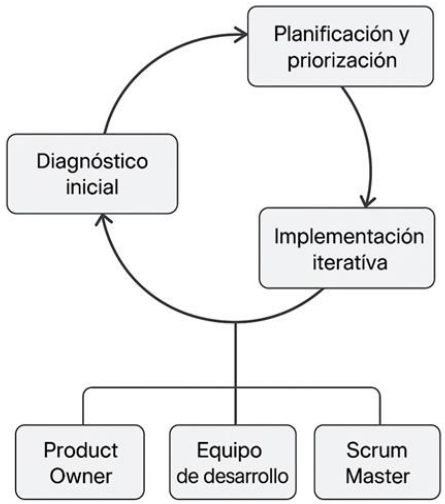
(backlog).

Implementación iterativa: ejecución de tareas, incluyendo sensibilización, controles básicos y validación colaborativa.

Revisión y retroalimentación: verificación del valor entregado, ajustes y re-priorización.

Evaluación global: retrospectiva para mejorar la forma de trabajo y fortalecer el aprendizaje organizacional.

Figura 1. Modelo circular iterativo de ciberseguridad basado en SCRUM para Las micro, pequeñas y medianas empresas (MiPyMEs) del Huila



Fuente: elaboración propia (2025).

Adaptación de roles en Las micro, pequeñas y medianas empresas (MiPyMEs)

Para facilitar la adopción, los roles de Scrum se adaptan al contexto de Las micro, pequeñas y medianas empresas (MiPyMEs):

- Product Owner: representante de la empresa (frecuentemente gerencia) que prioriza el backlog de seguridad.
- Scrum Master: facilitador del cambio (líder interno o apoyo externo) que cuida el proceso y remueve impedimentos.

Equipo de desarrollo: personal interno o proveedor externo que implementa controles y produce evidencias.

DISCUSIÓN

- Los hallazgos muestran que las principales brechas no se concentran únicamente en tecnología, sino en gobernanza y factor humano: ausencia de políticas, poca capacitación y protocolos limitados de respuesta a incidentes. Esto coincide con la
- literatura que ubica la cultura organizacional y la gestión de riesgos como determinantes críticos para la efectividad de cualquier control técnico. En ese sentido, un enfoque iterativo como Scrum puede ser especialmente útil porque convierte el avance en seguridad en entregables pequeños, verificables y priorizados, evitando proyectos extensos que requieren inversiones altas desde el inicio.
- Desde la perspectiva de gestión de proyectos, el enfoque ágil también reduce el riesgo clásico de "proyectos de seguridad que no terminan": cada sprint produce un incremento verificable y útil, y la organización decide de manera informada el siguiente mejor paso. Esto es coherente con la lógica de inversión escalonada: primero controlar los riesgos más probables y de mayor impacto, y luego profundizar en capacidades de detección y respuesta.

En términos de adopción, un elemento crítico es la participación de la gerencia como Product Owner. En Las micro, pequeñas y medianas empresas (MiPyMEs), la decisión de asignar tiempo y recursos suele depender de liderazgo directo, por ello, el modelo enfatiza acuerdos simples de priorización y evidencias claras de valor (por ejemplo, reducción de exposición a phishing con MFA y capacitación, o mejora de continuidad con copias de seguridad verificadas).

- Como limitación, el diagnóstico se basa en una muestra acotada y en el contexto regional; por tanto, los resultados deben interpretarse como una aproximación descriptiva y no como generalización estadística. Una validación adicional del modelo, mediante

implementación piloto con indicadores antes/después, fortalecería la evidencia de efectividad.

- Asimismo, se sugiere complementar futuras aplicaciones con métricas de línea base y seguimiento (por ejemplo, estado de MFA, cumplimiento de respaldos, tiempos de parcheo) para evaluar cambios de forma más objetiva. Una implementación piloto en 2–3 organizaciones, con medición antes/después y retrospectivas documentadas, permitiría refinar el modelo y ajustar su backlog mínimo a distintos sectores.

CONCLUSIONES

Más allá de los porcentajes reportados, el diagnóstico deja un mensaje central: en estas Las micro, pequeñas y medianas empresas (MiPyMEs) la ciberseguridad no falla por ausencia total de herramientas, sino por falta de gobernanza y de prácticas sostenibles. Es decir, existen controles aislados (antivirus, contraseñas), pero sin políticas, capacitación y procesos que los conviertan en una capacidad organizacional.

El modelo basado en Scrum aporta precisamente ese puente: convierte la seguridad en un portafolio de mejoras pequeñas, priorizadas y medibles, que se integran al trabajo cotidiano. Al adoptar ciclos cortos, la empresa aprende y ajusta, en lugar de depender de grandes proyectos que suelen detenerse por presupuesto, carga operativa o resistencia al cambio.

El diagnóstico evidenció brechas relevantes en gobernanza (políticas) y factor humano (capacitación), además de debilidades en gestión de incidentes.

El modelo basado en Scrum es pertinente para Las micro, pequeñas y medianas empresas (MiPyMEs) por su enfoque incremental, su capacidad de priorizar inversiones y su orientación a entrega continua de valor.

La integración de NIST CSF e ISO/IEC 27001, apoyada por criterios de madurez C2M2, ofrece una ruta estructurada para planear, ejecutar y sostener mejoras de seguridad con recursos limitados.

Recomendaciones

Como recomendación operativa, se sugiere iniciar por un backlog mínimo de alto impacto (política y roles, MFA, copias de seguridad con prueba de restauración, capacitación anti-phishing y procedimiento básico de incidentes). Estos elementos

suelen reducir de forma significativa la exposición a ataques frecuentes sin exigir inversiones complejas.

Se propone como trabajo futuro: (i) ejecutar un piloto del modelo con indicadores antes/después durante al menos 3 sprints, (ii) construir una rúbrica de madurez explícita y validada para Las micro, pequeñas y medianas empresas (MiPyMEs) del Huila, y (iii) evaluar la transferencia del modelo a otros departamentos con características productivas similares, ajustando el backlog según sector y criticidad.

- Formalizar políticas básicas y asignar responsabilidades claras (gobernanza).
- Implementar un plan continuo de sensibilización y capacitación (factor humano).
- Definir y probar protocolos de respuesta a incidentes con roles, tiempos y evidencias.
- Adoptar herramientas de monitoreo y respaldo acordes al tamaño de la empresa.
- Promover alianzas entre sector académico, empresarial y gubernamental para escalar buenas prácticas.

REFERENCIAS BIBLIOGRÁFICAS

Department of Energy. (2014). Cybersecurity Capability Maturity Model (C2M2) (Version 1.1). https://energy.gov/oe/downloads/cybersecurity-capability-maturity-model-february-2014

Hollnagel, E. (2011). Resilience engineering in practice: A guidebook. CRC Press.

International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security management systems - Requirements. ISO. https://www.iso.org/standard/27001

McAfee. (2022). The human factor in cybersecurity incidents: Global threat report 2022.

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

Schwaber, K., & Sutherland, J. (2020). The Scrum Guide: The definitive guide to Scrum. https://scrumguides.org/docs/scrumguide/v2020/2020-Scrum-Guide-US.pdf

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

CINTEL. (2023). Informe Índice de Madurez de Transformación Digital Colombia 2023. https://cintel.co/wp-content/uploads/2023/12/Informe-Indice-de-Madurez-de-Transformacion-Digital-Colombia-2023-VF.pdf

Agencia de los Estados Unidos para la Ciberseguridad y la Seguridad de las Infraestructuras (CISA). (2023). #StopRansomware Guide. https://www.cisa.gov/stopransomware/ransomware-guide

Congreso de Colombia. (2012). Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

ENISA. (2024). ENISA Threat Landscape 2024. https://securitydelta.nl/media/com_hsd/report/690/document/ENISA-Threat-Landscape-2024.pdf

Verizon. (2025). 2025 Data Breach Investigations Report (DBIR). https://www.verizon.com/business/resources/T16f/reports/2025-dbir-data-breach-investigations-report.pdf

SGS. (2022). Key Changes in ISO/IEC 27002:2022. https://www.sgs.com/en/news/2022/07/key-changes-in-iso-iec-27002-2022

National Institute of Standards and Technology. (2024). NIST Cybersecurity Framework 2.0: Resource & Overview Guide (NIST SP 1299). https://doi.org/10.6028/NIST.SP.1299

Department of Energy. (s. f.). Cybersecurity Capability Maturity Model (C2M2). https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

La Revista utiliza códigos para identificar al Revisor y al equipo de PARES REVISORES. Si tiene dudas o consultas, contacte a: contacto@cienciayreflexion.org
Código de Editor: 106
Código de Revisores: 999