Modelo Integrado de Gestión de Ciberseguridad y Transformación Digital para Pequeñas Pymes de Servicios Administrativos

Antonella L. Piva, Licenciada en Ciberseguridad,0134961

Bárbara Ayxa Sibler, Licenciada en Sistemas y Gestión – Tutora

Abstract- **Este trabajo presenta un modelo integrado que articula ciberseguridad, gestión de riesgos y transformación digital para micro y pequeñas organizaciones de servicios administrativos que manejan información sensible. A partir de un diagnóstico de madurez (gap analysis) se diseñó un plan estratégico de digitalización segura que integra ISO 31000 (gestión de riesgos), ISO/IEC 27001:2022 (seguridad de la información), Ley 25.326 (Protección de Datos Personales, Argentina) y principios de GRC. El caso práctico se desarrolla en la Inmobiliaria López Lamas, aplicando 33 esenciales, priorizados por impacto y esfuerzo. Los resultados evidencian la viabilidad de replicar el modelo en otros entornos profesionales, aportando una solución practica para mejorar su competitividad y capacidad de respuesta ante amenazas.**

I. NOMENCLATURA

GRC (Governance, Risk and Compliance): Marco de gobierno, gestión de riesgos y cumplimiento.

ISO: Organización que establece normas técnicas y de gestión.

ISO 31000: Norma internacional para la gestión de riesgos.

ISO/IEC 27001:2022: Norma internacional para la seguridad de la información

TPRM: Gestión de riesgos asociados a proveedores o terceros.

GAP ANALYSIS: Método que identifica la diferencia entre la situación actual y el nivel deseado.

CIA: Confidencialidad, Integridad y Disponibilidad.

CSF: NIST Cybersecurity Framework.

PyME: Empresa de tamaño reducido o medio con recursos y estructura operativa limitados.

MiPyME: microempresas dentro del régimen PyME.

AFIP/ARCA: Organismo argentino responsable de la recaudación tributaria y el control fiscal.

Kaspersky: Empresa internacional especializada en ciberseguridad, conocida por sus estudios e informes sobre amenazas digitales y soluciones antivirus.

ENISA: Agencia de la Unión Europea dedicada a fortalecer la ciberseguridad y promover buenas prácticas.

Phishing: Técnica de ingeniería social utilizada para engañar a usuarios y obtener información confidencial, generalmente mediante correos o mensajes fraudulentos.

RGPD: Normativa europea que regula el tratamiento y la protección de los datos personales.

2FA: Mecanismo de autenticación que combina dos factores de verificación independientes (algo que se y algo que tengo).

II. INTRODUCCIÓN

En los últimos años, la tecnología ha transformado radicalmente la mayoría de las industrias, en particular la forma en que las empresas gestionan su información. Este cambio ha sido beneficioso al optimizar tareas y procesos, pero también expone a las organizaciones a riesgos significativos, especialmente en la protección de la información. Muchas organizaciones, en particular las más pequeñas, aún gestionan información sensible de manera informal, utilizando hojas de cálculo o papel, dejando contraseñas visibles o adoptando prácticas donde queda reflejado el desconocimiento de las vulnerabilidades a las que están expuestas.

La creciente digitalización y dependencia de sistemas tecnológicos hace que la ciberseguridad deje de ser un lujo y se convierta en un pilar fundamental para la continuidad y competitividad de cualquier organización. Tradicionalmente, las empresas no contaban con personal especializado en seguridad informática; hoy, incluso contar con un equipo básico de ciberseguridad es considerado indispensable. Aunque la conciencia y adopción de buenas prácticas sigue siendo limitada, dejando brechas importantes que pueden derivar en pérdidas económicas, legales y reputacionales.

Este trabajo propone un modelo integrado de gestión de ciberseguridad y transformación digital para micro y pequeñas organizaciones de servicios administrativos. Más allá de su aporte teórico, se plantea como una oportunidad de negocio aun poco explorada, ya que busca ofrecer soluciones accesibles y adaptadas a un sector que tradicionalmente ha quedado rezagado en materia de digitalización segura. El modelo se aplicará como caso de estudio en una inmobiliaria real, estableciendo bases que puedan replicarse en industrias similares, como estudios de abogados, contadores o consorcios. La intención es trasladar el conocimiento y los controles que aplican las grandes empresas a organizaciones más pequeñas, fortaleciendo la protección compartida y la resiliencia del ecosistema empresarial.

La relevancia de este enfoque se evidencia en los recientes ataques cibernéticos dirigidos a grandes empresas a través de sus proveedores, que incluyen tanto empresas de gran envergadura como pequeñas y microempresas. Esto resalta la importancia de la gestión de riesgos de terceros (TPRM) y la

necesidad de implementar controles adecuados en toda la cadena de valor.

III. Marco teórico

A. Importancia de la transformación digital en PyMEs de servicios administrativos.

La digitalización y presencia digital ya no es una opción, sino una necesidad estratégica para las pequeñas organizaciones que buscan posicionarse y competir en un mercado dominado por grandes corporaciones.

En Argentina, el Estado impulsa esta transición mediante iniciativas como el "Programa Piloto para la Transformación Digital de las PyMEs" argentinas, que ofrece financiamiento, asistencia técnica e infraestructura tecnológica a aquellas organizaciones que cumplen con los requisitos formales, entre ellos poseer el Certificado "MiPyME" y mantener un registro activo ante la AFIP/ARCA. Sin embargo, este esquema puede dejar fuera a los emprendimientos unipersonales o profesionales independientes, que, si bien no encuadran en la categoría de PyME tradicional, también gestionan información sensible y cumplen funciones análogas a las pequeñas estructuras empresarias.

Desde el punto de vista operativo, la digitalización se presenta como una herramienta accesible gracias a soluciones de bajo costo y uso intuitivo, tales como Google Workspace y servicios de gestión en la nube. Estas herramientas permiten optimizar la administración documental, facilitar el acceso remoto y mejorar la eficiencia sin requerir grandes inversiones en infraestructura tecnológica.

No obstante, la incorporación de nuevas tecnologías también expone a las organizaciones a riesgos emergentes. En Argentina, se estima que el 41 % de las PyMEs sufrió un ataque cibernético en el último año, mientras que el 54 % reconoce carecer de preparación para gestionar vulnerabilidades. Además, un informe de Kaspersky indica que el 20 % de las PyMEs delega la ciberseguridad en personal no especializado y que el 72 % experimentó incidentes de seguridad en los últimos dos años, lo cual refleja una brecha crítica en la protección de datos y la continuidad operativa.

En definitiva, la transformación digital ofrece a las PyMEs de servicios administrativos una oportunidad concreta de optimizar su funcionamiento, mejorar la calidad de los servicios y generar mayor confianza en sus clientes. Sin embargo, esta confianza depende de la capacidad de la organización para proteger la información que administra. Al migrar procesos y documentos a entornos digitales, los datos sensibles se convierten en un activo estratégico, pero también en un punto vulnerable frente a amenazas externas e internas.

Por ello, la digitalización debe abordarse no solo como un proyecto tecnológico, sino también como un compromiso con la gestión segura de la información. La identificación de qué datos resultan críticos, y cómo garantizar su confidencialidad, integridad y disponibilidad, constituye el siguiente paso indispensable para que la transformación digital sea sostenible, segura y generadora de valor en el tiempo.

B. Gestión de la información sensible

La transformación digital expone a este tipo de organizaciones a nuevos desafíos en materia de protección de información. Para abordarlos, es fundamental emplear el modelo de la triada CIA (Confidencialidad, Integridad y Disponibilidad), base establecida en el campo de seguridad informática.

- Confidencialidad: se refiere a garantizar que los datos estén accesibles únicamente para personas autorizadas. Por ejemplo, un contrato digitalizado con detalles sensibles de una operación inmobiliaria o un legajo contable con información fiscal de un cliente debe protegerse contra accesos no autorizados.
- Integridad: implica que la información no sea alterada de manera indebida. Si un cambio no autorizado modifica la fecha o el monto de un contrato, o altera un comprobante impositivo, se pone en riesgo la validez legal del documento.
- Disponibilidad: exige que los datos estén accesibles cuando se los necesita, incluso ante fallas técnicas o incidentes de seguridad. Si un sistema de gestión no está operativo en momentos importantes, como la liquidación de sueldos o la firma de una escritura, puede afectar la continuidad del negocio.

Una mala gestión de la información sensible trae consecuencias graves: pérdida de confianza del cliente, errores legales o comerciales, sanciones por incumplimiento de privacidad, y hasta pérdida de continuidad operativa.

C. Capacitación y cultura organizacional

La tecnología, por sí sola, no garantiza seguridad. Su implementación efectiva requiere de una cultura organizacional sólida que acompañe los cambios y dé sostenibilidad a las medidas adoptadas. En este sentido, la capacitación continua, el establecimiento de políticas claras y su cumplimiento efectivo (no solo formal) son pilares esenciales para fortalecer la resiliencia digital de las pequeñas organizaciones de servicios administrativos.

Todos los colaboradores constituyen la primera línea de defensa frente a amenazas. Por ello, la concientización en materia de ciberseguridad debe integrarse como parte de las rutinas de trabajo. Conceptos como la ciberhigiene, definida por ENISA como el conjunto de prácticas básicas para prevenir ataques digitales, han demostrado ser altamente efectivos cuando se incorporan de manera sistemática en el día a día (ENISA,2023). Estas prácticas incluyen desde la correcta gestión de contraseñas y el uso responsable del correo electrónico hasta la aplicación de actualizaciones y parches de

seguridad.

La documentación de políticas y procedimientos es otro componente crítico. Lineamientos claros respecto al manejo de documentos digitales, la realización periódica de copias de seguridad, la clasificación de la información según su criticidad y los protocolos de respuesta ante incidentes permiten reducir la improvisación y mejorar la capacidad de reacción. Sin embargo, es fundamental que estas políticas no queden limitadas a un manual archivado, sino que se traduzcan en capacitación práctica y hábitos concretos dentro de la organización.

La experiencia muestra que iniciativas como simulaciones de phishing, capacitaciones breves adaptadas al lenguaje del negocio, y la revisión periódica de los procedimientos son herramientas eficaces para convertir la teoría en práctica. Tal como señala ISACA, la concientización y el entrenamiento continuo no solo reducen la probabilidad de incidentes, sino que también incrementan la confianza de clientes y socios comerciales, convirtiéndose en una ventaja competitiva sostenible (ISACA, 2022).

D. Normativas y marcos de referencia

Un elemento diferenciador clave de este modelo es la integración de normas internacionales y marcos regulatorios que tradicionalmente son aplicados en grandes corporaciones, pero rara vez en micro y pequeñas organizaciones de servicios administrativos.

La ISO 31000 establece principios y directrices para la gestión de riesgos, brindando un marco que permite identificar, analizar y tratar amenazas de manera sistemática (NIST), esta es aplicable a todas las organizaciones, independientemente de su tipo, tamaño, actividades y ubicación, y abarca todos los tipos de riesgo. Por su parte, la ISO/IEC 27001 se focaliza en la seguridad de la información, proporcionando requisitos para establecer, implementar, mantener y mejorar un sistema de gestión que proteja la confidencialidad, integridad y disponibilidad de los datos.

En el contexto argentino, la Ley de Sociedades Comerciales impone a los administradores y socios un deber de diligencia y responsabilidad sobre la gestión de la organización, lo que incluye garantizar la seguridad y confidencialidad de la información. De manera complementaria, la Ley 25.326 de Protección de Datos Personales establece la obligación de un tratamiento adecuado de la información de clientes y terceros, convirtiendo al cumplimiento normativo no solo en un requisito legal, sino también en un factor de confianza y reputación en el mercado.

Como complemento, el modelo considera buenas prácticas internacionales como el NIST Cybersecurity Framework (CSF) y el Reglamento General de Protección de Datos (RGPD) europeo, que sirven como referencia comparativa para fortalecer las medidas de ciberseguridad y privacidad. De esta forma, se establece un diferencial competitivo frente a aquellas empresas que no aplican estándares reconocidos, aportando un valor agregado tangible.

La aplicación de estas normas se convierte en un factor de diferenciación competitivo. No solo posiciona a la organización como confiable y profesional, sino que abre la puerta a nuevas oportunidades comerciales, ya que los clientes cada vez valoran más el cumplimiento normativo y la seguridad en el manejo de su información

E. Diagnóstico de madurez y mejora continua

El punto de partida para la implementación del modelo es la realización de un diagnóstico de madurez en ciberseguridad, a través de la herramienta conocida como Gap Analysis. Esta metodología permite comparar el estado actual de la organización frente a estándares o marcos de referencia, identificando brechas específicas que deben ser cerradas para alcanzar un nivel de madurez deseado.

Este diagnóstico no solo facilita la asignación eficiente de recursos, sino que también establece un mapa de ruta estratégico hacia la digitalización segura. En sectores donde habitualmente no existen métricas objetivas de seguridad, contar con indicadores de madurez brinda un lenguaje común para comunicar avances a clientes, auditores y socios. De este modo, la evaluación se convierte en una herramienta que, además de guiar mejoras internas, puede funcionar como un diferencial de confianza y transparencia en el mercado.

La mejora continua constituye un pilar fundamental del modelo. Tal como lo plantean las normas ISO, la seguridad de la información no es un proyecto estático, sino un proceso dinámico que requiere revisiones periódicas, auditorías internas y retroalimentación constante. Incorporar esta lógica en pequeñas organizaciones resulta fundamental para sostener en el tiempo la efectividad de las medidas implementadas y adaptarse a nuevas amenazas.

F. Satisfacción y confianza del cliente

En mercados como el inmobiliario, jurídico o contable, la confianza es la base de la relación con los clientes. Incorporar la ciberseguridad como parte del servicio no solo protege datos, sino que también se convierte en un sello de calidad y prestigio profesional. Esta confianza, sustentada en prácticas concretas de seguridad, se traduce en fidelización de clientes existentes y en un diferencial competitivo frente a competidores que aún gestionan la información de manera rudimentaria.

De esta manera, la ciberseguridad deja de ser vista como un costo operativo para transformarse en un activo estratégico intangible, que incrementa la reputación, genera ventaja competitiva y contribuye al crecimiento sostenible de la organización.

G. Relevamiento empírico complementario

Ante la ausencia de estudios académicos específicos sobre el nivel de madurez en ciberseguridad y protección de datos personales en pequeñas empresas de servicios administrativos, se decidió incorporar un **relevamiento empírico exploratorio** como complemento del marco teórico.

El objetivo fue obtener evidencia directa sobre las prácticas, percepciones y comportamientos de las PyMEs argentinas frente a los desafíos de la seguridad digital, particularmente en sectores como el inmobiliario, contable, jurídico y administrativo, que comparten características similares al caso de estudio principal.

Se diseñó una encuesta estructurada en formato digital (Google Forms), compuesta por 25 preguntas distribuidas en cuatro ejes temáticos:

1. Datos generales de la empresa: sector, tamaño y existencia de responsables de TI o ciberseguridad.
2. Prácticas de ciberseguridad: capacitación, políticas o procedimientos, controles básicos de protección, auditorías, preparación ante incidentes y principales amenazas percibidas.
3. Protección de datos personales: tipo de datos tratados, responsables designados, uso de cláusulas de privacidad y consentimiento, almacenamiento, plazos de conservación y canales para que los titulares ejerzan sus derechos (acceso, rectificación, supresión).
4. Percepción y madurez digital: prioridad asignada por la dirección a la ciberseguridad y acciones consideradas necesarias para mejorar la seguridad y la protección de datos.

La encuesta fue difundida a través de redes profesionales y grupos académicos, obteniéndose 50 respuestas válidas de personas que trabajan o colaboran en pequeñas y medianas empresas argentinas. La participación fue voluntaria, anónima y confidencial.

Los datos obtenidos reflejan tendencias consistentes con la hipótesis de este trabajo:

- El 52 % de las PyMEs no cuenta con un responsable formal de ciberseguridad.
- El 64 % nunca realizó capacitaciones en temas como phishing o ingeniería social, y solo un 18 % lo hace una vez al año.
- El 40 % dispone de políticas documentadas de seguridad de la información.
- En cuanto a mecanismos de protección, la mayoría utiliza antivirus y copias de seguridad (80 %), aunque solo el 44 % implementa políticas de contraseñas o doble factor de autenticación (2FA); un 4 % carece completamente de estas medidas.
- El 56 % no realiza auditorías ni revisiones internas sobre seguridad o gestión de riesgos.
- El 86 % trata datos personales, principalmente de clientes (88 %), pero el 76 % no tiene un responsable designado para su protección. Asimismo, un 76 % utiliza la nube para resguardar datos sin definir tiempos de conservación ni canales para que los titulares ejerzan sus derechos.
- El 60 % considera que su nivel de madurez digital es bajo o medio.

En la pregunta abierta *"¿Qué considera que ayudaría a su empresa a mejorar en materia de seguridad digital y protección de datos?"*, la respuesta más reiterada fue la necesidad de mayor capacitación y concientización del personal. Los participantes coincidieron en que la formación continua es el pilar para reducir errores humanos y fortalecer la cultura organizacional.

IV. FODA.

A. Contexto

Para complementar el marco teórico y estratégico presentado, se incorpora un análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas). Esta herramienta permite evaluar los factores internos y externos que influyen en la viabilidad del modelo propuesto de gestión de ciberseguridad y transformación digital para pequeñas PyMEs de servicios administrativos.

El propósito es doble: por un lado, identificar los aspectos que potencian o limitan la implementación del modelo; por otro, mostrar cómo estos factores se manifiestan en un caso real, la Inmobiliaria López Lamas, generando aprendizajes que pueden replicarse en otros entornos profesionales. De esta manera, el FODA no se limita a un ejercicio descriptivo, sino que aporta una visión estratégica aplicada.

B. Desarrollo

Fortalezas

El modelo se apoya en estándares internacionales como ISO 31000 e ISO/IEC 27001, lo cual otorga legitimidad y solidez metodológica frente a un sector que rara vez aplica este tipo de marcos. En el caso de la inmobiliaria, esto se traduce en la posibilidad de estructurar políticas de seguridad de la información por primera vez. Además, la propuesta ofrece una solución adaptada a micro y pequeñas organizaciones, históricamente relegadas en los procesos de digitalización segura. En la práctica, esto facilita a la inmobiliaria migrar procesos en papel hacia una gestión digital más organizada y segura.

La integración de la Ley 25.326 como eje central del modelo refuerza el cumplimiento normativo y genera confianza en clientes y proveedores. En la inmobiliaria, por ejemplo, garantizar la protección de datos de inquilinos y propietarios se convierte en un diferencial en la relación comercial. También la capacitación en ciberhigiene fortalece a los colaboradores como primera línea de defensa frente a

amenazas. Incluso en un entorno no técnico como el de la inmobiliaria, breves entrenamientos permiten que el personal contribuya activamente a la seguridad.

Oportunidades

El mercado de estudios jurídicos, contables e inmobiliarios representa un segmento aún poco atendido que requiere soluciones accesibles y específicas en materia de ciberseguridad. La experiencia de la Inmobiliaria López Lamas constituye un ejemplo ilustrativo de cómo actores de pequeña escala pueden beneficiarse con herramientas ya disponibles en el mercado, demostrando que la digitalización segura no es exclusiva de grandes corporaciones. En paralelo, el aumento sostenido de incidentes en PyMEs ha generado una mayor conciencia sobre la necesidad de adoptar medidas preventivas, como se evidencia en la detección de intentos de phishing en la inmobiliaria, que refuerza la percepción de valor de implementar controles básicos. Finalmente, el cumplimiento normativo emerge como un factor de diferenciación competitiva, capaz de atraer clientes que valoran la gestión responsable de la información y de consolidar la confianza como un activo estratégico dentro de la relación comercial.

Debilidades

La carencia de recursos humanos especializados en pequeñas organizaciones puede dificultar la implementación inicial del modelo. En la inmobiliaria, la falta de un área técnica dedicada es un claro ejemplo. El cambio cultural requerido para adoptar políticas de seguridad puede generar resistencia interna. Pasar de contraseñas compartidas en papel a gestores digitales, como sucede en la inmobiliaria, puede producir fricciones. La inversión inicial en capacitación y herramientas, aunque mínima en comparación con grandes empresas, puede ser percibida como un gasto en lugar de una inversión estratégica. Por último, la ausencia de métricas estandarizadas en el sector dificulta demostrar el retorno inmediato de las medidas implementadas, lo que puede desalentar a algunos tomadores de decisión.

Amenazas

El incremento sostenido de ciberataques dirigidos a la cadena de valor convierte a las pequeñas empresas en blancos atractivos para los atacantes. En el caso de la inmobiliaria, una brecha en el correo corporativo podría comprometer datos sensibles de operaciones y contratos.

El incumplimiento de la Ley 25.326 conlleva riesgos de sanciones económicas y daños reputacionales, lo que representa una amenaza latente para cualquier organización que gestione información personal.

Además, la rápida evolución de las amenazas tecnológicas obliga a mantener procesos y controles en constante actualización, algo que puede superar la capacidad de pequeñas organizaciones.

Finalmente, competidores que adopten soluciones digitales más rápidas o estandarizadas podrían captar clientes que prioricen la inmediatez por sobre la seguridad, generando presión adicional en el mercado.

V. PROPUESTA ESTRATEGICA.

A. Misión

Brindar a micro y pequeñas organizaciones de servicios administrativos un modelo accesible y práctico que integre ciberseguridad y transformación digital, permitiéndoles gestionar su información de manera segura, eficiente y conforme a la normativa vigente.

B. Visión

Convertirse en un referente nacional en la aplicación de marcos internacionales de gestión de riesgos y seguridad de la información en sectores tradicionalmente relegados, contribuyendo a un ecosistema empresarial más resiliente, competitivo y confiable

C. Objetivos estratégicos

La propuesta estratégica busca facilitar la digitalización segura de procesos en organizaciones de pequeña escala, lo que permite reducir costos operativos y mitigar riesgos asociados, al tiempo que se promueve el cumplimiento normativo como un valor competitivo y diferenciador en el mercado. Además, se plantea el desarrollo de una cultura de ciberhigiene en sectores con bajo nivel de madurez digital, fortaleciendo a los colaboradores como primera línea de defensa frente a amenazas. Por lo tanto, el modelo está concebido para ser replicable y adaptable en distintos ámbitos de servicios administrativos, tales como inmobiliarias, estudios contables, jurídicos o consorcios, garantizando su escalabilidad y pertinencia en diversos entornos profesionales. Esto le otorga un alcance más amplio y posiciona al modelo como una respuesta innovadora ante una necesidad relevante del mercado.

D. Propuesta: ¿Qué se ofrece?

La propuesta consiste en un modelo integrado de gestión especialmente diseñado para pequeñas organizaciones de servicios administrativos que carecen de estructuras tecnológicas complejas y de personal especializado en seguridad informática. Este modelo comienza con un diagnóstico de madurez en ciberseguridad a partir de la aplicación de un gap analysis, cuyo propósito es identificar de manera precisa las brechas en la gestión de riesgos y en la protección de la información. A partir de dicho diagnóstico se elabora un plan estratégico de digitalización segura sustentado en marcos de referencia reconocidos, tales como ISO 31000, ISO/IEC 27001 y la Ley 25.326 de Protección de Datos Personales, que aseguran legitimidad metodológica y cumplimiento normativo.

El modelo contempla además la capacitación en ciberhigiene adaptada al lenguaje del negocio, con el fin de involucrar a todos los colaboradores como primera línea de defensa frente a amenazas digitales. Este componente se

complementa con documentación estandarizada que incluye políticas, procedimientos y protocolos de respuesta ante incidentes, concebidos para ser aplicados de manera inmediata y sin necesidad de conocimientos técnicos avanzados.

De forma adicional, la propuesta incorpora un análisis de alineación con las buenas prácticas del mercado, lo que permite evaluar en qué medida la organización se aproxima a estándares internacionales y a modelos de gestión ya consolidados en sectores más maduros. Esta mirada comparativa facilita no solo la identificación de oportunidades de mejora, sino también la elaboración de un plan de acción concreto, priorizado en función de la criticidad de los riesgos y la factibilidad de implementación de las medidas.

En conjunto, se ofrece un paquete metodológico asequible, escalable y replicable, que no se limita a diagnosticar las debilidades de una organización, sino que propone soluciones prácticas y sostenibles para robustecer la seguridad de la información, mejorar la eficiencia operativa y consolidar la confianza del mercado. De esta forma, el modelo no solo representa un instrumento técnico, sino también una oportunidad de negocio para organizaciones que necesitan digitalizarse de manera segura y accesible.

E. Problema / Solución

El modelo propuesto se presenta como una solución concreta al trasladar marcos de gestión reconocidos internacionalmente a la escala de las micro y pequeñas empresas. Se ofrece un enfoque que concibe la ciberseguridad como un servicio estratégico, más que como un costo operativo. A través de un diagnóstico inicial y un plan de digitalización segura, se logran mejoras tangibles en la eficiencia administrativa y la protección de datos, garantizando además el cumplimiento normativo. De este modo, las organizaciones no solo reducen riesgos y previenen pérdidas, sino que también se posicionan de forma diferencial en el mercado, construyendo confianza y consolidando su reputación profesional. Al resolver una brecha histórica en este segmento, el modelo se convierte en un factor competitivo que aporta seguridad, eficiencia y valor de marca.

F. Plan de marketing / ventas

La propuesta se orienta a un segmento compuesto por inmobiliarias, estudios jurídicos y contables, administraciones de consorcios y profesionales independientes, que gestionan información sensible y requieren soluciones prácticas y accesibles. A diferencia de las grandes organizaciones, este grupo carece de áreas tecnológicas internas o presupuestos amplios, lo que evidencia una necesidad concreta.

La estrategia de entrada se basa en alianzas con colegios profesionales, cámaras PyME y programas públicos de digitalización. Estos canales permiten llegar a públicos que han quedado rezagados en los procesos de transformación digital, generando legitimidad desde espacios de confianza.

La propuesta de valor se resume en ofrecer una digitalización segura, simple y adaptada al negocio. Se incluirán acciones de sensibilización gratuitas (charlas, seminarios) y diagnósticos de bajo costo como puerta de entrada. El modelo contempla distintos niveles de servicios (básico, intermedio, avanzado), permitiendo una adopción progresiva y sostenible.

G. Análisis de riesgo

La propuesta estratégica requiere considerar los riesgos tanto internos como externos que podrían afectar su implementación y sostenibilidad en el tiempo. Desde una perspectiva interna, uno de los principales desafíos radica en la resistencia cultural al cambio. Muchas pequeñas organizaciones mantienen prácticas arraigadas, como el uso de contraseñas compartidas en papel o la falta de protocolos claros, lo que genera fricciones cuando se introducen nuevas metodologías de ciberseguridad. A ello se suma la percepción del costo de capacitación y herramientas como un gasto innecesario, en lugar de visualizarlo como una inversión estratégica. La ausencia de métricas claras que evidencien el retorno inmediato de la inversión en seguridad refuerza esta percepción y dificulta, en algunos casos, la toma de decisiones orientadas a la prevención.

En cuanto a los riesgos externos, el modelo debe enfrentarse a un entorno marcado por la rápida evolución de las amenazas cibernéticas, que obliga a revisar y actualizar los controles de forma constante para evitar obsolescencia. Asimismo, los cambios en la normativa, ya sea en el plano nacional con la Ley 25.326 o a nivel internacional con marcos de referencia como el RGPD, imponen la necesidad de una adaptación continua que podría resultar compleja para organizaciones de pequeña escala. Otro factor para considerar es la competencia proveniente de soluciones más estandarizadas o “enlatadas”, que, aunque menos personalizadas, pueden resultar atractivas para ciertos clientes debido a su bajo costo y facilidad de implementación.

Para mitigar estos riesgos, el modelo plantea estrategias específicas. En el plano interno, la educación continua se convierte en un mecanismo esencial para disminuir la resistencia cultural, mientras que el diseño de esquemas de precios progresivos permite adaptar la inversión a las posibilidades de cada organización, favoreciendo la adopción gradual. A nivel externo, la actualización periódica del modelo y su alineación con buenas prácticas internacionales aseguran que las soluciones propuestas mantengan vigencia y relevancia. Finalmente, las alianzas estratégicas con cámaras sectoriales y programas estatales de apoyo funcionan como una red de respaldo institucional que refuerza la confianza y legitima el modelo frente a los potenciales clientes.

De esta manera, el análisis de riesgo no solo identifica posibles obstáculos, sino que también ofrece un marco de mitigación que fortalece la propuesta y contribuye a su viabilidad en un mercado caracterizado por la volatilidad

tecnológica y la alta sensibilidad en materia de seguridad de la información.

H. Estrategia de salida al mercado

La estrategia de salida se plantea de forma gradual. Como primera etapa, el modelo se aplicará en la Inmobiliaria López Lamas a modo de experiencia piloto, permitiendo validar su viabilidad y generar un caso de éxito real.

Luego, se escalará hacia otros sectores similares a través de presentaciones en colegios profesionales y cámaras empresariales, apuntando a generar legitimidad y promover su adopción. Se desarrollará una estrategia de comunicación digital y se buscarán alianzas con programas estatales y proveedores tecnológicos para ampliar la propuesta y facilitar su implementación en organizaciones con bajo nivel de madurez digital.

VI. DESARROLLO.

El desarrollo metodológico del modelo se basa en la construcción de un análisis de brechas (Gap Analysis) adaptado a pequeñas organizaciones de servicios administrativos, tales como inmobiliarias, estudios contables y jurídicos. Este instrumento funciona como una consultoría simplificada, que permite identificar de manera estructurada las diferencias entre el estado actual de la organización y un nivel de referencia deseado en materia de ciberseguridad.

Para ello, se integraron normas y buenas prácticas internacionales, que constituyen la base conceptual y normativa del modelo:

- ISO/IEC 27001:2022, que define requisitos para un sistema de gestión de seguridad de la información.
- ISO 31000:2018, que establece directrices para la gestión integral de riesgos.
- Ley 25.326 de Protección de Datos Personales, como marco regulatorio aplicable en Argentina.

A partir de estas fuentes se elaboró un kit de 33 controles esenciales, organizados conforme a los pilares del NIST Cybersecurity Framework (Identificar, Proteger, Detectar, Responder y Recuperar) y agrupados en cinco categorías prácticas:

1. Controles físicos (protección de oficinas, resguardo de notebooks)
2. Controles de acceso y autenticación (contraseñas robustas, doble factor).
3. Controles de respaldo y continuidad (backups, planes de recuperación).
4. Controles normativos y organizacionales (políticas de seguridad, registros de proveedores).
5. Controles de concientización y cultura (capacitaciones, simulacros de phishing).

Es importante destacar que los 33 controles definidos en este modelo no buscan reemplazar la totalidad de los requisitos contemplados en marcos como ISO/IEC 27001, ISO 31000 o la Ley 25.326, los cuales incluyen un número significativamente mayor de lineamientos y exigencias.

En esta propuesta se integran 38 controles del Anexo A de la norma ISO/IEC 27001:2022, seleccionados de un total de 93, priorizando aquellos de mayor impacto, menor costo y rápida aplicabilidad dentro del contexto operativo de las PyMEs de servicios administrativos.

El propósito del modelo es ofrecer un mínimo viable de ciberseguridad, que permita a las organizaciones alcanzar un nivel de madurez superior al promedio del sector, estableciendo una base sólida para la mejora continua y consolidando un enfoque replicable, escalable y sostenible en organizaciones de características similares.

La elección de Inmobiliaria López Lamas como caso piloto se justifica por tratarse de una empresa con más de treinta y cinco años de trayectoria, que combina procesos analógicos y digitales y carece de un área especializada en seguridad de la información. Este perfil la convierte en un caso representativo e idóneo para validar la viabilidad del modelo y proyectar su aplicación a otros sectores equivalentes.

Para evaluar el grado de cumplimiento del modelo y establecer brechas accionables, se aplicó una escala de madurez de cinco niveles (1 = Inicial / Ad hoc a 5 = Optimizado / Mejora continua). La calificación de cada control se asigna a partir de la evidencia disponible (políticas, registros, capturas, actas, etc.). A partir de estas puntuaciones se generan tres niveles de síntesis:

a) El puntaje por control, que refleja la situación puntual de cada práctica;

b) El promedio por categoría, obtenido como media aritmética de los controles que la integran; y

$$\text{Madurez categoría} = \frac{\sum \text{Puntajes controles de la categoría}}{\text{Cantidad de controles en la categoría}}$$

c) El promedio por pilar NIST, que resume el nivel de madurez alcanzado en cada pilar (Identificar, Proteger, Detectar, Responder, Recuperar).

$$\text{Madurez pilar} = \frac{\sum \text{Puntajes controles del pilar}}{\text{Cantidad de controles del pilar}}$$

Con estos valores se construye un Índice de Madurez Global, complementado con visualizaciones gráficas (gráfico radar) que facilitan la identificación inmediata de fortalezas, brechas y oportunidades de mejora.

El gap se define como la diferencia entre el valor observado y el nivel objetivo de referencia. Cada brecha se prioriza

mediante una matriz impacto–esfuerzo, atendiendo en primer lugar las brechas críticas de bajo esfuerzo (por ejemplo, activación del doble factor de autenticación, formalización de políticas existentes o designación de responsables) y posteriormente aquellas de mayor impacto y complejidad (como pruebas semestrales de recuperación o simulacros de incidentes).

Este enfoque permite estimar la madurez por categorías tal como figura en la tabla, alinear las acciones de mejora con los pilares del NIST, y convertir los hallazgos en un plan de acción concreto, medible y trazable, vinculado a cada control y su evidencia correspondiente.

A. Análisis de resultados por Categoría

El análisis de madurez por categorías evidencia un nivel inicial generalizado, con valores entre 1 y 1,7 sobre 5. Esto refleja la ausencia de políticas formales, documentación sistemática y mecanismos de control interno consolidados.



- Controles de respaldo y continuidad (1,71) presentan el valor más alto, lo que indica cierta conciencia sobre la importancia de preservar la información y garantizar la continuidad operativa, aunque sin procesos estandarizados ni pruebas de restauración.

- Controles físicos (1,5) y normativos y organizacionales (1,43) muestran avances puntuales vinculados a la infraestructura y a la gestión informal de algunos procesos, pero sin un marco de seguridad integral.

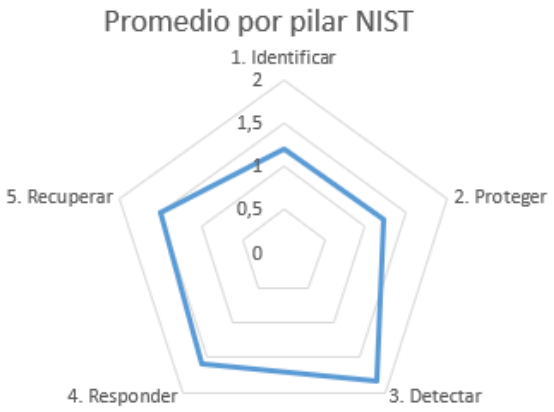
- Controles de acceso y autenticación (1,16) reflejan la falta de procedimientos técnicos básicos, como contraseñas robustas o doble factor de autenticación.

- Finalmente, controles de concientización y cultura (1,0) evidencian la mayor debilidad, dado que no existen actividades de capacitación, simulacros ni difusión de buenas prácticas.

En conjunto, el promedio global de la categoría se ubica en torno a 1,36, lo que posiciona a la organización en un nivel "Inicial / Ad hoc", caracterizado por acciones reactivas, dependientes del criterio individual y sin estandarización formal.

B. Análisis de resultados por Pilar NIST

El promedio por pilar del NIST Cybersecurity Framework permite observar la madurez relativa de cada fase del ciclo de gestión de ciberseguridad.



Los resultados muestran que el pilar "Detectar" (1,83) es el más desarrollado, debido principalmente a prácticas informales de control de disponibilidad y a la atención reactiva frente a incidentes. En contraste, los pilares "Proteger" (1,23) e "Identificar" (1,2) son los más débiles, evidenciando la falta de políticas, inventarios, clasificación de información y medidas preventivas.

El pilar "Responder" (1,6) muestra una capacidad incipiente de resolución de incidentes, aunque basada en la experiencia personal y no en protocolos formales. Finalmente, "Recuperar" (1,5) refleja una recuperación empírica sin documentación ni métricas ante interrupciones o fallas.

Estos valores confirman que la empresa se encuentra en un estado de madurez inicial (Nivel 1-2), donde las acciones de seguridad existen de manera informal pero no están sistematizadas ni verificadas.

C. Síntesis General

De la evaluación integral se desprende que el caso de estudio presenta un Índice de Madurez Global de 1,47, correspondiente a un nivel "Inicial / Ad hoc", caracterizado por prácticas reactivas, ausencia de políticas formales y una gestión de seguridad aún en desarrollo.

El nivel objetivo sugerido (5 – Optimizado / Mejora continua) representa una meta de largo plazo que, si bien resulta ambiciosa para una PyME de estructura reducida, permite orientar el proceso de mejora continua. En este sentido, el plan de acción elaborado se basa en la viabilidad temporal y económica de cada mejora, priorizando las iniciativas de alto impacto y bajo costo.

De implementarse las mejoras sugeridas, se estima que la organización podría incrementar su madurez al menos en un punto en cada categoría, y en algunos casos hasta dos puntos, acercándose de manera realista a un nivel "Definido / Documentado" o incluso "Gestionado / Verificado".

Este proceso no debe interpretarse como la búsqueda de un estado ideal inalcanzable, sino como un camino gradual de fortalecimiento que acompañe el crecimiento natural de la empresa, su infraestructura y sus capacidades internas.

El modelo de análisis desarrollado fue reconocido por la organización como una herramienta útil y comprensible, al facilitar la identificación de brechas concretas y orientar las acciones de mejora. Se espera que su aplicación sirva también como referencia para otras PyMEs del sector administrativo, contribuyendo a elevar el nivel general de ciberseguridad y resiliencia en este tipo de entornos empresariales.

VII. Conclusión

La presente investigación desarrolló y validó un modelo integrado de gestión de ciberseguridad y transformación digital orientado a micro y pequeñas organizaciones de servicios administrativos. Su principal aporte radica en haber operacionalizado marcos y normas de referencia. como ISO/IEC 27001, ISO 31000 y la Ley 25.326. en un kit mínimo viable de 33 controles, diseñado para ser implementado con recursos limitados y verificado mediante una matriz de evidencias en formato Excel. El modelo incorpora 38 de los 93 controles del Anexo A de ISO/IEC 27001, priorizando aquellos de alto impacto, bajo costo y rápida adopción, organizados en función de los pilares del NIST Cybersecurity Framework y agrupados en cinco categorías prácticas: controles físicos, acceso y autenticación, respaldo y continuidad, normativos/organizacionales, y concientización y cultura.

El caso piloto en la Inmobiliaria López Lamas permitió medir el nivel de madurez inicial y validar la viabilidad práctica del enfoque. A partir de dicho diagnóstico se elaboró un plan de acción priorizado por impacto–esfuerzo, que pone en primer lugar las mejoras críticas y de rápida ejecución: activación del doble factor de autenticación (2FA), formalización de políticas básicas, asignación de responsables, clasificación de la información y establecimiento de copias de seguridad automáticas con pruebas de restauración. La implementación de estas medidas permitiría elevar la madurez de la organización al menos un punto en cada categoría y, en algunos casos, hasta dos puntos, alcanzando de forma realista los niveles Definido/Documentado (3) y Gestionado/Verificado (4).

Cabe destacar que el propósito del modelo no es alcanzar un estado ideal inmutable, sino promover un proceso continuo de mejora, adaptable al crecimiento, la infraestructura y los recursos reales de cada PyME.

Desde una perspectiva teórico–práctica, el modelo propuesto aporta:

- Un mecanismo simple de evaluación basado en una escala de madurez de 1 a 5 con evidencias verificables.
- Una traducción aplicada de estándares internacionales a controles operativos comprensibles para entornos no técnicos.
- Un instrumento replicable y escalable, sustentado en una planilla de evaluación y guías prácticas, adaptable a otras PyMEs del sector.
- La integración de los principios de GRC dentro de la lógica de la transformación digital segura, alineando cumplimiento legal, gestión de riesgos y continuidad operativa.

Entre las limitaciones identificadas se destaca la ausencia de mediciones longitudinales que permitan observar el impacto posterior a la implementación del plan. Sin embargo, estas limitaciones no invalidan los hallazgos obtenidos; por el contrario, delinean una agenda futura de investigación y aplicación práctica, orientada a consolidar y expandir el modelo propuesto.

VIII. Aplicaciones futuras

A partir de los resultados obtenidos, se identifican diversas líneas de continuidad y ampliación del presente trabajo. En primer lugar, se busca replicar la aplicación del modelo en una muestra más amplia de organizaciones de servicios administrativos (inmobiliarias, estudios jurídicos, contables y administraciones de consorcios) con el fin de fortalecer la validez externa y validar su escalabilidad en distintos contextos operativos.

En segundo lugar, se recomienda realizar mediciones semestrales del nivel de madurez en ciberseguridad, con el fin de monitorear la evolución de los indicadores, evaluar el impacto de las mejoras implementadas y consolidar la mejora continua como parte de la cultura organizacional.

Como tercera línea de trabajo, se plantea profundizar el relevamiento sobre barreras culturales y económicas, ampliando la encuesta de percepción a un mayor número de PyMEs del sector. Esto permitirá obtener evidencia empírica complementaria que respalde el diagnóstico cualitativo y cuantitativo y ayude a comprender los factores que condicionan la adopción de buenas prácticas.

Además, se prevé ampliar el kit operativo incorporando modelos de plantillas estandarizadas (políticas mínimas, procedimientos de gestión de incidentes, matrices de roles y permisos, y listas de verificación de offboarding) junto con módulos de capacitación breve en ciberhigiene, orientados a la sensibilización y entrenamiento práctico de los colaboradores.

Finalmente, se sugiere profundizar en la medición de indicadores de retorno (reducción de incidentes, mejora en

tiempos de recuperación, costos evitados y satisfacción del cliente), a fin de vincular directamente la seguridad con el valor de negocio, fortaleciendo el argumento de que la inversión en ciberseguridad genera ventajas competitivas sostenibles.

Este trabajo propone dejar evidenciado la viabilidad y efectividad de elevar gradualmente el nivel de ciberseguridad en pequeñas organizaciones administrativas, sin requerir grandes inversiones ni equipos técnicos especializados. El modelo desarrollado y validado fue aceptado por la organización piloto y se proyecta como una herramienta replicable y adaptable, capaz de mejorar la competitividad, la confianza de los clientes y la resiliencia del ecosistema PyME.

IX. Referencias

[1] https://news.microsoft.com/source/latam/noticias-de-microsoft/7-tendencias-de-ciberseguridad-y-consejos-para-que-las-pymes-se-mantengan-protegidas/
[2] https://www.pwc.com.ar/es/servicios/consultoria/regulaciones-riesgos-seguridad-fraude/pymes-soluciones-ciberseguridad-ciso.html
[3] https://www.docusign.com/es-mx/blog/desarrolladores/lciberseguridad-en-las-pymes
[4] https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes
[5] https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/the-essentiality-of-cybersecurity-for-small-businesses
[6] https://www.isaca.org/resources/isaca-journal/issues/2023/volume-2/considerations-for-developing-cybersecurity-awareness-training
[7] Digital-Transformation-of-SMEs-policy-highlights-en.pdf
[8] https://www.argentina.gob.ar/economia/pymes-emprendedores-y-economia-del-conocimiento/programa-piloto-para-la-transformacion
[9] https://www.a24.com/pymes/ciberseguridad-4-cada-10-empresas-argentinas-sufrieron-un-ciberataque-como-protegerse-n1309048
[10] https://argentina.revistafactordeexito.com/posts/60442/20-de-las-pymes-de-america-latina-deja-su-ciberseguridad-en-manos-inexpertas
[11] https://www.argentina.gob.ar/economia/pymes-emprendedores-y-economia-del-conocimiento/capacitar/rutas-de-aprendizaje-capacitar
[12] https://www.fortinet.com/resources/cyberglossary/cia-triad
[13] https://www.enisa.europa.eu/topics/cyber-hygiene
[14] https://www.nist.gov/baldrige/enterprise-risk-management-requires-systems-perspective
[15] https://sprinto.com/blog/cybersecurity-gap-assessment/
[16] https://asana.com/es/resources/gap-analysis
[17] https://www.eccu.edu/blog/leveraging-cybersecurity-for-customer-trust/
[18] https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm
[19] https://www.iso.org/standard/65694.html

X. Biografia



Antonella L. Piva (1996) nació en Buenos Aires, Argentina. Es Martillera Pública por la Universidad Nacional de San Martín (UNSAM), con diplomaturas en gestión y dirección de PyMEs (UNSAM) y seguridad de la información (Universidad Tecnológica Nacional - UTN) y auditora líder 27001 (TUV Rheinland). Actualmente se desempeña como Senior Information Security Analyst en BASE4 Security, liderando auditorías internas y externas, diseño de marcos de Gobierno de TI y ejercicios de preparación ante incidentes (TTX). Anteriormente trabajó en TPRM en Aquanima, Grupo Santander y como consultora de ciberseguridad en EY, participando en auditorías (SOX y SOC), evaluación de riesgos y desarrollo de controles en entornos corporativos.