UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA DE DERECHO

COMPLIANCE EN PROTECCIÓN DE DATOS PERSONALES EN PYMES: OBLIGACIONES IGNORADAS Y PROPUESTAS DE CUMPLIMIENTO PROGRESIVO

Trabajo de titulación previó a la obtención del
Título de Abogado/a

AUTOR: RICHARD DANIEL RODRÍGUEZ RENGIFO
TUTOR: EDISSON ALEJANDRO MORALES PAZMIÑO

Quito-Ecuador
2026

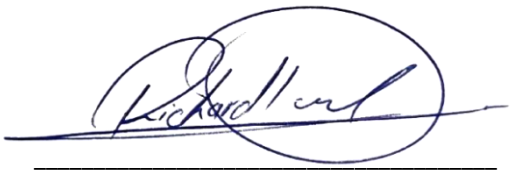
CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Richard Daniel Rodríguez Rengifo con documento de identificación N° 1719243428 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 20 de enero del año 2026

Atentamente,



Richard Daniel Rodríguez Rengifo

1719243428

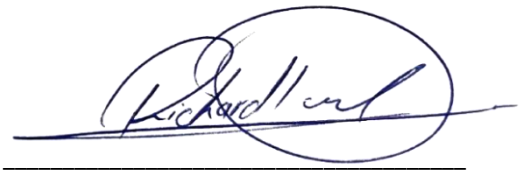
CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Richard Daniel Rodríguez Rengifo con documento de identificación N° 1719243428, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del Ensayos o Artículos Académicos: "Compliance en Protección de Datos Personales en PYMES: Obligaciones Ignoradas y Propuestas de Cumplimiento Progresivo", el cual ha sido desarrollado para optar por el título de: Abogado, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, 20 de enero del año 2026

Atentamente,



Richard Daniel Rodríguez Rengifo

1719243428

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Edisson Alejandro Morales Pazmiño con documento de identificación N° 1803122843, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: COMPLIANCE EN PROTECCIÓN DE DATOS PERSONALES EN PYMES: OBLIGACIONES IGNORADAS Y PROPUESTAS DE CUMPLIMIENTO PROGRESIVO, realizado por Richard Daniel Rodríguez Rengifo con documento de identificación N° 1719243428, obteniendo como resultado final el trabajo de titulación bajo la opción Ensayos o Artículos Académicos que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 20 de enero del año 2026

Atentamente,

_____

Abg. Edisson Alejandro Morales Pazmiño

1803122843

DEDICATORIA

Dedico el presente trabajo de titulación y todo lo que ha significado esta carrera a mi familia, en especial a Azucena y Ricardo, que, con ejemplo de trabajo, esfuerzo y mucho amor, han sabido guiar mis pasos y forjar mi carácter, permitiéndome soñar e ir detrás de esos sueños.

También, a dos mujeres que siempre estuvieron para cuidar de mí y enseñarme de la vida, lo último que aprendí de ellas, es que el amor trasciende más allá de la presencia física, su ausencia Amada y Diana no es silencio, es guía constante.

RESUMEN

El artículo analiza hasta qué punto las PYMES ecuatorianas cumplen la Ley Orgánica de Protección de Datos Personales y la manera en la que pueden avanzar hacia un modelo de compliance compatible con sus capacidades, analizado desde un enfoque cualitativo, exploratorio y descriptivo, se desarrolla un estudio de casos en dos PYMES de los sectores tecnológico y de videovigilancia, mismas que tratan datos de identificación, contacto, geolocalización y, en un caso, datos biométricos. Se combinan análisis documental de la Constitución, la Ley Orgánica de Protección de Datos Personales, su Reglamento y doctrina especializada a la par de entrevistas semiestructuradas a directivos y revisión de políticas de privacidad, cláusulas contractuales y prácticas internas de seguridad de la información. Los resultados ponen en evidencia un cumplimiento parcial e informal, debido a que existen medidas intuitivas de protección, pero faltan registros de actividades de tratamiento, delegados de protección de datos, protocolos frente a incidentes, capacitación al personal y políticas escritas, pese a tratarse de actividades calificadas como de alto riesgo. No obstante, se observa disposición a mejorar y a cuidar la confianza de clientes y trabajadores; a partir de lo cual, el trabajo propone un modelo de cumplimiento progresivo en tres niveles (básico, intermedio y avanzado) que busca reducir brechas de cumplimiento, prevenir riesgos jurídicos y aportar a una cultura de paz en las relaciones laborales y comerciales.

PALABRAS CLAVE: protección; datos personales; PYMES; compliance; cultura; paz.

ABSTRACT

This article analyzes the extent to which Ecuadorian SMEs comply with the Organic Law on the Protection of Personal Data and how they can move towards a compliance model compatible with their capabilities, using a qualitative, exploratory, and descriptive approach, a case study is conducted with two SMEs in the technology and video surveillance sectors, both of which process identification, contact, geolocation, and, in one case, biometric data. The study combines documentary analysis of the Constitution, the Organic Law on the Protection of Personal Data, its Regulations, and specialized doctrine with semi-structured interviews with executives and a review of privacy policies, contractual clauses, and internal information security practices. The results reveal partial and informal compliance, as intuitive protection measures exist, but there is a lack of records of processing activities, data protection officers, incident protocols, staff training, and written policies, despite these activities being classified as high-risk. However, there is a willingness to improve and to safeguard the trust of clients and employees; based on this, the work proposes a progressive compliance model in three levels (basic, intermediate and advanced) that seeks to reduce compliance gaps, prevent legal risks and contribute to a culture of peace in labor and commercial relations.

KEYWORDS: protection; personal data; SMEs; compliance; culture, peace.

ÍNDICE DE CONTENIDO

1. TÍTULO

Compliance en Protección de Datos Personales en PYMES: Obligaciones Ignoradas y Propuestas de Cumplimiento Progresivo

Introducción:

En muy pocos años los datos personales dejaron de ser ese dato que antes se quedaba quieto en un formulario o perdido en una base de datos y pasaron a convertirse en uno de los elementos más sensibles de la economía, como un rastro que acompaña a cada persona cuando entra a una página web, hace una compra, se conecta para trabajar o revisa sus redes sociales, rastro que se alimenta de su nombre, de lo que hace a diario, de lo que le gusta, de los lugares donde está, de lo que busca en internet y de muchas decisiones pequeñas que, casi sin que uno se dé cuenta, terminan almacenadas en sistemas públicos y privados (Moreano et al., 2024).

Con la expansión de las plataformas digitales, el uso constante de redes sociales y la digitalización de los procesos empresariales se han multiplicado las formas de recoger y usar información, pero al mismo tiempo han crecido los riesgos de trato inadecuado, filtraciones, sesgos, discriminación y vulneración de derechos (Guerrero, 2020).

En el plano internacional, la Agenda 2030 ha insistido en que el desarrollo no puede medirse solo por el crecimiento económico o por indicadores ambientales, sino también por la manera en que se protegen los derechos, se garantiza la paz y se construye sostenibilidad institucional, de ahí que los Objetivos de Desarrollo Sostenible incorporen de forma expresa la idea de contar con instituciones sólidas, abiertas y responsables (CEPAL, 2018).

Dentro de ese conjunto, el ODS 16, orientado a la paz, la justicia y las instituciones eficaces, ofrece un marco claro para leer la protección de datos personales como parte de la gobernanza democrática y de la construcción de confianza entre ciudadanía, empresas y Estado, porque la forma en que se recoge, se almacena y se usa la información no es neutra, refleja cómo se mira a las personas titulares de esos datos y qué lugar ocupan en la relación con las organizaciones (Cevallos & Delgado, 2023).

En Ecuador, este cambio de enfoque se ha visto en el reconocimiento constitucional del derecho a la protección de datos personales y, de forma más reciente, en la aprobación de la Ley Orgánica de Protección de Datos Personales, en adelante como

"LOPDP", (2021) y de su Reglamento General (2023), que pretenden ordenar el manejo de información en todos los sectores, fijar principios y deberes para responsables y encargados y dar a las personas herramientas reales para vigilar qué se hace con sus datos.

Todo ello ocurre en un contexto de digitalización rápida de administraciones y empresas, en el que el trabajo con documentos y el paso a sistemas electrónicos no siempre han ido acompañados de políticas claras de seguridad, confidencialidad y acceso a la información, como se advierte en experiencias previas de organización de archivos y procesos de digitalización en instituciones del ámbito local (Gutiérrez & Uchuari, 2020).

Los primeros estudios sobre la LOPDP resaltan su aporte al fortalecimiento de los derechos y su conexión con la agenda del ODS 16, porque ofrece instrumentos para frenar abusos, mejorar la transparencia y fijar obligaciones concretas de rendición de cuentas frente al uso de datos personales (Cevallos & Delgado, 2023).

Al mismo tiempo, los análisis que se centran en sectores específicos, como los sistemas judiciales o ciertas plataformas digitales, muestran que sigue habiendo una distancia importante entre lo que dicen las normas y lo que ocurre en la práctica, con problemas muy claros relacionados con la confidencialidad, la seguridad de la información y la confianza ciudadana en los sistemas digitales (Asqui et al., 2024), a lo que se añaden reflexiones más amplias sobre los desafíos de regular la protección de datos en la era digital, entre ellos la dificultad de adaptar los marcos legales a tecnologías que cambian rápido, la debilidad de los aparatos de supervisión y una cultura de cumplimiento todavía débil en muchos espacios empresariales (Barzola & Núñez, 2025).

Desde hace años, la literatura sobre empresa y responsabilidad social viene recordando que las organizaciones no solo producen bienes o prestan servicios, sino que generan impactos sociales que deben reconocerse y gestionarse con cuidado, y que la Responsabilidad Social Corporativa es un marco a través del cual la empresa asume compromisos frente a sus grupos de interés que van más allá del cumplimiento mínimo de la ley (Morán, 2012).

En paralelo, los programas de compliance han ido ganando peso en el derecho y en la regulación empresarial, en la medida en que los ordenamientos comienzan a exigir a las personas jurídicas la adopción de sistemas internos para prevenir, detectar y reaccionar ante riesgos legales, lo que tiene efectos directos en su responsabilidad y en cómo se

valora su conducta cuando se presentan infracciones (Nieto et al., 2025).

La experiencia acumulada por ejemplo en ámbitos como el derecho ambiental ha dejado ver que el compliance puede funcionar como una pieza muy útil para que la actividad económica no vaya por un carril distinto al del cuidado del entorno ni al de la lucha contra la corrupción, y al mismo tiempo sirve para empujar una gobernanza empresarial más abierta, verificable y sujeta a controles internos y externos (Ferré, 2021).

Ahora bien, muchas de estas reflexiones se han construido mirando sobre todo a grandes corporaciones y a sectores sometidos a una fuerte regulación, cuando en el caso ecuatoriano la realidad productiva está compuesta principalmente por pequeñas y medianas empresas que trabajan con equipos pequeños, presupuestos limitados y grados muy distintos de formalización (Ramírez & Ferré, 2021).

Para un número importante de PYMES, la protección de datos aparece como una exigencia lejana, demasiado técnica y costosa, casi pensada para "grandes ligas", aunque en su día a día gestionan información sensible de clientes, proveedores y trabajadores y apoyan buena parte de sus estrategias comerciales en redes sociales, plataformas digitales y herramientas de marketing que dependen precisamente del uso de datos (Moreano et al., 2024).

La ausencia de políticas internas mínimamente estructuradas, de procedimientos definidos para obtener y dejar constancia del consentimiento, de controles eficaces sobre quién entra y qué puede hacer dentro de las bases de datos o de protocolos claros para reaccionar ante incidentes de seguridad termina colocándolas en una posición débil no solo frente a la autoridad de control, sino también frente a sus propios grupos de interés y frente al riesgo permanente de erosión de la confianza (et Silva, 2024).

El cuadro se complica aún más si se tiene presente que la protección de datos se entrelaza con otros derechos, como la privacidad, la libertad de expresión o el libre desarrollo de la personalidad y, que un manejo descuidado de la información personal puede concretarse en episodios de acoso, discriminación o violencia simbólica en los espacios digitales, tal como advierten los estudios sobre ciberacoso y uso de redes sociales (Guerrero, 2020).

Desde esa óptica, la forma en que las empresas administran los datos va más allá de un asunto estrictamente técnico o vinculado solo al área de sistemas, debido a que se convierte en una manera de situarse frente a la dignidad de las personas y frente a la

prevención de conflictos, lo que enlaza con la noción de cultura de paz entendida como un conjunto de prácticas que colocan en primer plano el respeto, la transparencia y la búsqueda de salidas no violentas a las tensiones cotidianas.

En paralelo, las discusiones respecto a la celeridad, eficiencia y calidad en la administración de justicia y en la actuación del Estado recuerdan que los principios constitucionales necesitan concretarse en mecanismos efectivos, y que la información y la forma en que se trata ocupan un lugar central cuando se trata de garantizar derechos y de cerrar el paso a arbitrariedades (Cabrera & Zamora, 2024).

Si esa lógica se traslada al espacio empresarial, los programas de compliance en protección de datos pueden leerse como un puente entre el mandato legal y la vida diaria de las organizaciones, en virtud de que traducen principios y declaraciones generales en procesos definidos, en asignación de responsabilidades y en hábitos institucionales que se repiten y se consolidan.

Sobre este telón de fondo, el artículo se propone examinar hasta qué punto las PYMES ecuatorianas están cumpliendo con la Ley Orgánica de Protección de Datos Personales y su Reglamento, identificar los obstáculos más relevantes que enfrentan al momento de aplicar las obligaciones previstas y explorar si la puesta en marcha de programas de cumplimiento en materia de protección de datos puede convertirse en una estrategia razonable para disminuir riesgos.

Reforzar la responsabilidad social corporativa y aportar a la construcción de una cultura de paz organizacional, para ello se articula la revisión del marco normativo y doctrinal sobre protección de datos, responsabilidad empresarial y compliance con un acercamiento a la experiencia concreta de las PYMES, que permita observar con mayor nitidez la distancia que existe entre lo que la ley manda y lo que efectivamente ocurre en la práctica (Alcivar, 2024).

En coherencia con este propósito, primero se presenta el contexto normativo y conceptual que relaciona protección de datos, gobernanza corporativa y desarrollo sostenible, luego se explica la metodología utilizada, después se exponen e interpretan los principales resultados sobre el cumplimiento de la LOPDP en las PYMES y, finalmente, se discuten estos hallazgos a la luz de la literatura revisada, proponiendo orientaciones para un modelo de cumplimiento progresivo que resulte asumible para este tipo de empresas y que se mantenga alineado con los compromisos en materia de derechos asumidos por

el Estado ecuatoriano.

Metodología

El estudio se enmarca en un enfoque cualitativo puesto que le interesa comprender cómo las pequeñas y medianas empresas interpretan y aplican la Ley Orgánica de Protección de Datos Personales en su quehacer cotidiano, más que medir variables numéricas o buscar relaciones causales rígidas, de modo que el centro está en reconstruir percepciones, prácticas y dificultades concretas alrededor del cumplimiento normativo y, a partir de esa experiencia, perfilar rutas realistas para un modelo de compliance en protección de datos.

En cuanto a su alcance, la investigación es de carácter exploratorio y descriptivo, ya que se sitúa en un campo todavía incipiente en el contexto ecuatoriano, donde la LOPDP y su Reglamento tienen pocos años de vigencia y los trabajos empíricos centrados en PYMES son escasos, por eso se pretende por un lado describir el conjunto de obligaciones legales que recaen sobre estas empresas y, por otro, ofrecer un primer panorama sobre el nivel de conocimiento y cumplimiento que manifiestan sus directivos, así como las barreras que perciben para implementar la normativa.

Al mismo tiempo el estudio tiene una dimensión jurídico-propositiva, porque no se limita a fotografiar la realidad, sino que utiliza los hallazgos para formular una propuesta de cumplimiento progresivo adaptada a las capacidades reales de las PYMES.

La población de referencia está integrada por las pequeñas y medianas empresas formalmente constituidas en el Ecuador que realizan tratamiento de datos personales de clientes, proveedores, trabajadores u otros grupos de interés en el desarrollo de sus actividades económicas. Dado que resulta inviable abarcar ese universo y que el objetivo es profundizar en experiencias concretas, se optó por un diseño de estudio de casos múltiples y se trabajó con una muestra intencional compuesta por dos PYMES.

Seleccionadas por criterios de accesibilidad y relevancia para el problema de investigación, ubicadas en sectores donde el uso de datos personales resulta especialmente intenso, como los servicios y el entorno digital. En cada una de estas empresas se entrevistó a la persona que ejerce la representación legal o la dirección general, por ser quien concentra la información sobre la toma de decisiones y sobre la existencia o no de políticas internas de protección de datos.

Para la construcción del marco teórico-normativo se empleó el análisis documental, revisando la Constitución de la República del Ecuador (en adelante, "CRE" o "Constitución"), la Ley Orgánica de Protección de Datos Personales y su Reglamento General, así como doctrina especializada en protección de datos, responsabilidad social corporativa, derecho económico y programas de compliance, además de documentos de organismos internacionales relacionados con la Agenda 2030 y el Objetivo de Desarrollo Sostenible 16, que aportan el contexto de derechos, gobernanza y paz que atraviesa la discusión; este trabajo documental permitió identificar los principios rectores del tratamiento de datos, las obligaciones que la LOPDP impone a responsables y encargados, las posibles consecuencias jurídicas del incumplimiento y los elementos mínimos de un sistema de cumplimiento en materia de datos personales.

En la fase empírica se utilizó como técnica principal la entrevista semiestructurada dirigida a las personas representantes de las dos PYMES seleccionadas, a partir de una guía que combinó preguntas cerradas y abiertas, con el fin de indagar tanto el nivel de conocimiento que tienen sobre la LOPDP, las medidas que declaran haber adoptado y la percepción de riesgos y beneficios asociados al cumplimiento, como ejemplos concretos de prácticas internas vinculadas a la obtención del consentimiento, el manejo de bases de datos, la gestión de incidentes de seguridad y la capacitación del personal. El carácter semiestructurado de las entrevistas permitió mantener un hilo común para la comparación entre casos y, al mismo tiempo, dejar espacio para que las personas entrevistadas relataran experiencias, dudas o preocupaciones no previstas en la guía.

De forma complementaria se realizó una revisión puntual de documentos internos que las empresas estuvieron dispuestas a compartir, tales como políticas de privacidad, avisos de tratamiento de datos o cláusulas contractuales, sin acceso a datos personales específicos, con el único propósito de contrastar el discurso de los entrevistados con algunos elementos formales de sus esquemas de cumplimiento.

En el plano de los métodos de análisis se combinaron el método analítico-sintético y el inductivo-deductivo, el primero permitió descomponer el marco legal en sus componentes principales y fragmentar el discurso de las entrevistas en categorías como conocimiento de la norma, medidas técnicas, medidas organizativas, obstáculos y oportunidades, para luego integrar estos elementos en una visión más amplia sobre el estado del cumplimiento en PYMES.

Mientras que el segundo facilitó partir de los casos concretos y de las narrativas recogidas para inferir patrones de comportamiento y contrastarlos después con los principios generales del derecho a la protección de datos y de la responsabilidad empresarial; se recurrió además al método hermenéutico jurídico para interpretar la LOPDP y su Reglamento a la luz de los derechos fundamentales y de los compromisos internacionales asumidos por el Estado ecuatoriano, lo que fue clave al momento de traducir obligaciones legales en componentes de un programa de compliance.

El procesamiento de la información empírica se realizó mediante un análisis de contenido de tipo temático, organizando las respuestas en categorías definidas a partir de los objetivos de investigación y del marco teórico, pero permitiendo la aparición de subcategorías nuevas cuando los testimonios l o exigían, las entrevistas se sistematizaron en matrices donde se registraron convergencias, divergencias y particularidades de cada caso, lo que hizo posible identificar tendencias comunes en el nivel de cumplimiento así como algunas buenas prácticas que luego se incorporaron a la propuesta de cumplimiento progresivo dividida en niveles básico, intermedio y avanzado.

La cual fue pensada para que las PYMES puedan avanzar de manera escalonada en la adecuación a la LOPDP sin desbordar sus capacidades económicas y organizativas y para que el cumplimiento contribuya no solo a evitar sanciones, sino a consolidar una cultura interna de respeto a los datos personales y a la paz en las relaciones laborales y comerciales.

Interpretación de Resultados

Los resultados del trabajo de campo permiten mirar de cerca cómo se concreta, en la vida diaria de dos pequeñas y medianas empresas ecuatorianas, ese mandato abstracto de “proteger datos personales” que recogen la Constitución y la LOPDP, y lo que aparece no es un vacío absoluto, sino más bien un mapa irregular, con zonas donde hay cierto orden y cuidado, y otras donde persisten huecos importantes de cumplimiento.

En primer lugar, el tipo de información que tratan ambas empresas deja claro que las PYMES no están en una “orilla menor” del riesgo, sino en el corazón del problema, aunque a veces no lo perciban así.

La primera empresa del estudio se dedica a servicios tecnológicos y de telecomunicaciones y maneja de forma rutinaria datos de identificación y contacto de sus clientes, información sobre los equipos que instalan, así como datos de sus trabajadores

vinculados a contratación, control de horarios y seguimiento de tareas. La segunda empresa opera en el marco de la seguridad y la videovigilancia, por lo que además de nombres, cédulas, teléfonos y direcciones, trata datos de geolocalización de los inmuebles que protege y, en ciertos proyectos, datos biométricos de reconocimiento facial asociados a sistemas de acceso; este último tipo de tratamiento se ubica entre los más sensibles de conformidad con la normativa emitida por la Superintendencia de Protección de Datos Personales, que incluye a estos sujetos entre los obligados a adoptar medidas reforzadas de protección y a designar un Delegado de Protección de Datos Personales (Resolución Nº SPDP-SPD-2025-0028-R, 2025).

En ambos casos los datos personales son materia prima del servicio, no un detalle accesorio, de modo que cualquier falla en la gestión repercute directamente en la confianza de clientes y usuarios.

Cuando se explora el nivel de conocimiento que tienen sus directivos al respecto de la Ley Orgánica de Protección de Datos Personales, se gráfica un contraste interesante. En la primera empresa, el gerente se reconoce con un conocimiento "moderado" de la norma, identifica nociones básicas como consentimiento, finalidad, seguridad y confidencialidad, y es capaz de relacionar la LOPDP con ciertos cambios internos que han hecho, por ejemplo al restringir quién ingresa a determinadas carpetas o al modificar la forma en que se comparte información con proveedores o colaboradores externos; sin embargo, admite que ese conocimiento no se traduce todavía en un cumplimiento integral y que falta mucho por hacer para "estar al día".

En la segunda empresa, la representante legal reconoce una familiaridad menor con la ley y delega gran parte del tema en la asesoría externa, lo cual desemboca en una percepción algo difusa de las obligaciones: se asume que, por tratar datos "solo con fines de seguridad", las exigencias podrían ser menos intensas, cuando en realidad la naturaleza de los datos tratados, en particular los datos biométricos, que la Ley Orgánica de Protección de Datos Personales (2021) califica expresamente como datos personales sensibles en su artículo 4, en concordancia con los artículos 25 y 26 ibidem respecto a categorías especiales y tratamiento de datos sensibles, y el uso sistemático de datos de geolocalización, en ese sentido su tratamiento intensivo y combinado configura un escenario de alto riesgo que exige análisis de riesgos y evaluaciones de impacto (arts. 40 y 42 LOPDP), los sitúa en un marco de especial sensibilidad regulatoria y demanda

medidas reforzadas de cumplimiento.

En cuanto a las medidas de protección de datos que ya se aplican, los discursos revelan una suerte de "compliance intuitivo" o de sentido común que, sin ser irrelevante, se queda corto frente al estándar normativo. La primera empresa ha ido construyendo, a partir de su propia experiencia y de recomendaciones generales, un conjunto de prácticas que incluyen el uso obligatorio de contraseñas, niveles diferenciados de acceso a sistemas y carpetas, acuerdos de confidencialidad con el personal, copias de seguridad periódicas y verificaciones antes de enviar información a terceros; incluso mencionan la existencia de un aviso sencillo de privacidad para sus clientes.

No obstante, todo esto descansa más en costumbres internas que en documentos formales o en un programa de cumplimiento estructurado, y no existe un registro sistemático de las actividades de tratamiento ni procedimientos detallados para responder a incidentes.

La segunda empresa, por su parte, pone el énfasis en la seguridad técnica de las soluciones que ofrece, menciona el uso de plataformas con sistemas de cifrado, mecanismos de autenticación robustos en aplicaciones móviles y restricciones de acceso a las imágenes de videovigilancia, lo cual resulta coherente con la sensibilidad del servicio que presta; sin embargo, todavía no cuenta con políticas escritas de tratamiento de datos, cláusulas contractuales específicas sobre protección de datos en sus contratos con clientes o protocolos internos desarrollados para la atención de derechos de los titulares y la gestión de brechas de seguridad.

De modo que una parte importante del esfuerzo se concentra en la tecnología mientras que los componentes organizativos y jurídicos del cumplimiento permanecen poco desarrollados, el vacío llama la atención si se considera que la Resolución Nº SPDP-SPD-2025-0028-R (2025) incluye a las empresas de seguridad privada y a quienes prestan servicios de videovigilancia masiva y geolocalización entre los sujetos obligados a designar y registrar un delegado de protección de datos personales, de manera independiente a su tamaño, obligación que en este caso no se ha implementado y ni siquiera es percibida con claridad por la propia empresa, lo que evidencia una distancia entre el encuadre normativo y la autopercepción de sus deberes.

Las principales brechas de cumplimiento se repiten, con matices, en ambos casos; ninguna de las dos empresas ha elaborado un registro detallado de actividades de

tratamiento que identifique bases legales, finalidades, plazos de conservación y flujos de datos, pese a que esta es una obligación expresa del ordenamiento jurídico ecuatoriano, pues el artículo 38 del Reglamento General a la Ley Orgánica de Protección de Datos Personales (2023) exige expresamente al responsable del tratamiento que cuente con cien o más trabajadores llevar un registro detallado de todas las actividades de tratamiento bajo su competencia, lo cual incluye al menos los fines del tratamiento, las categorías de destinatarios, la identificación de los titulares y categorías de datos, las bases legitimadoras, los plazos de retención y una descripción general de las medidas técnicas, jurídicas, administrativas y organizativas adoptadas, obligación que el artículo 39 del ibidem, extiende a responsables con menos de cien trabajadores cuando el tratamiento entrañe riesgo para los derechos y libertades de los titulares, no sea ocasional o incluya categorías especiales de datos, y que se complementa con el artículo 44, que impone al encargado mantener ese registro cuando el responsable esté obligado.

De igual manera el artículo 51 de la Ley Orgánica de Protección de Datos Personales (2021), que regula el Registro Nacional de Protección de Datos Personales y exige reportar y mantener actualizada ante la autoridad de control la información relativa a la identificación de la base de datos o tratamiento, los datos del responsable y del encargado, la finalidad y las características esenciales del tratamiento.

Tampoco se ha designado formalmente una persona encargada de protección de datos, aunque en la práctica recaiga en los directivos la responsabilidad de tomar decisiones en la materia. La capacitación al personal es casi inexistente: se confía en que los trabajadores “ya saben” que la información de los clientes es delicada, pero no se han desarrollado sesiones específicas sobre derechos de los titulares, deberes de confidencialidad ni manejo seguro de dispositivos y credenciales.

En relación con la gestión de riesgos e incidentes, se puede evidenciar otro vacío, las empresas sostienen que nunca han sufrido “grandes problemas”, pero al profundizar en la conversación emergen episodios que, a la luz de la Ley Orgánica de Protección de Datos Personales (2021), encajan en la noción de incidente de seguridad, entendida por el artículo 4, numeral correspondiente a definiciones, como todo evento que afecte la confidencialidad, integridad, disponibilidad o resiliencia de los datos personales o de los sistemas que los tratan.

La primera empresa relata un envío erróneo de un archivo con información de un

cliente a un destinatario equivocado, situación que se resolvió únicamente con una disculpa y con la solicitud de eliminación del mensaje, a pesar de que, de acuerdo a esa definición, dicho envío constituye un incidente de seguridad que debió activar procedimientos internos de registro, análisis y, en su caso, notificación a la autoridad y al titular, de acuerdo con las obligaciones previstas para el responsable del tratamiento en la propia LOPDP.

Además de ciertos ajustes internos en la revisión de correos y en la segmentación de accesos a archivos; la segunda empresa cuenta un conflicto con un cliente por la imposibilidad de recuperar imágenes y registros biométricos más allá de cierto tiempo, debido a que los equipos sobrescribían de manera automática la información almacenada. En ambos casos el aprendizaje llega a *posteriori*, a partir del problema, y no desde un plan previo de respuesta que haya sido definido, documentado y difundido entre el personal.

En cuanto a la óptica subjetiva de los directivos, los obstáculos para avanzar hacia un cumplimiento más robusto son claros y consistentes; mencionan, en primer lugar, la falta de tiempo en estructuras pequeñas donde una misma persona asume tareas de gestión, operación, ventas y administración, lo que deja poco espacio para proyectos de ordenamiento interno que no se perciben como urgentes.

En segundo lugar, señalan la ausencia de personal especializado en protección de datos o en derecho tecnológico, lo que los obliga a depender de asesorías externas puntuales que a veces se perciben como costosas o alejadas de la realidad de una PYME. En tercer lugar, aluden a la sensación de que las obligaciones están pensadas desde la lógica de grandes empresas, y que trasladar las exigencias de la LOPDP “tal cual” a su escala puede resultar desproporcionado, sobre todo cuando el negocio opera con márgenes estrechos. A ello se suma, en el caso de la segunda empresa, una crítica a la comunicación institucional: perciben que las autoridades informan poco, no ofrecen modelos claros y se concentran en la amenaza de sanciones.

Pese a ese panorama, las entrevistas también dejan ver disposiciones favorables que abren espacio para una propuesta de cumplimiento progresivo. Las dos personas entrevistadas comparten la idea de que proteger datos personales “es lo correcto” y de que, más allá de las multas, es una forma de cuidar la relación con sus clientes y de diferenciarse frente a competidores que son más descuidados con la información. Ambas expresan interés en contar con guías claras y materiales adaptados a PYMES: plantillas

sencillas para políticas de privacidad, avisos de tratamiento y cláusulas contractuales; ejemplos de registros de actividades de tratamiento que puedan completarse sin necesidad de un departamento jurídico y listas de verificación que les permitan saber si están cumpliendo lo mínimo indispensable. Subrayan, además, que un modelo útil debería organizarse en etapas o niveles, de modo que una empresa pueda comenzar por un piso básico (identificar qué datos trata, para qué los usa, quién accede a ellos y cómo se protegen) y luego ir incorporando medidas más avanzadas conforme disponga de más recursos y experiencia.

Un elemento interesante es la forma en que los directivos hablan de la confianza; en ambos casos se reconoce que un manejo deficiente de los datos puede traducirse en reclamos, rupturas de contratos y deterioro de la imagen, pero también en conflictos internos si los trabajadores sienten que se les controla de manera excesiva o se utilizan sus datos con fines no transparentados; dentro de las entrevistas no se aprecia una política explícita sobre este tema, pero sí una preocupación constante por evitar reclamos, malos entendidos y quiebres en la confianza con clientes y trabajadores cuando algo sale mal con los datos; los directivos hablan de disculparse, explicar lo ocurrido y ajustar procesos para que no se repita, lo que pone en evidencia que ven en la gestión de la información un foco potencial de conflicto que conviene anticipar.

En las entrevistas aplicadas, no se puede apreciar una política explícita de "cultura de paz", pero sí una preocupación constante por evitar reclamos, malentendidos y quiebres en la confianza con clientes y trabajadores cuando algo sale mal con los datos; los directivos hablan de disculparse, explicar lo ocurrido y ajustar procesos para que no se repita, lo que muestra que ven en la gestión de la información un foco potencial de conflicto que conviene anticipar.

Desde esa mirada, un programa de cumplimiento en protección de datos no se reduce a "poner candados" técnicos, sino que también implica definir cómo se informa a las personas, cómo se atienden sus quejas y cómo se reacciona ante un error, es decir, incorporar pautas claras de comunicación y de manejo de desacuerdos. Sin afirmar que exista ya una cultura de paz consolidada, estos elementos permiten entender el compliance como una herramienta que puede ayudar a disminuir tensiones y a tramitar de forma menos confrontativa los problemas vinculados al uso de datos personales en las relaciones empresariales.

En síntesis, la interpretación de los resultados muestra que las PYMES estudiadas se encuentran en una fase de cumplimiento parcial y, en buena medida, informal: han desarrollado prácticas que apuntan a proteger la información y a evitar daños evidentes, pero todavía no han traducido las obligaciones de la LOPDP en un sistema ordenado de políticas, procedimientos, registros y mecanismos de respuesta.

La distancia entre la norma y la práctica no se debe solo a desinterés, sino a una combinación de desconocimiento, restricciones de recursos y ausencia de herramientas adaptadas a su escala. Al mismo tiempo, existe conciencia de la importancia del tema y disposición a avanzar si se les ofrecen rutas claras y progresivas. Sobre este terreno es que se construye, en la parte siguiente del artículo, la propuesta de un modelo de cumplimiento escalonado que recoge tanto las exigencias jurídicas como las necesidades y posibilidades reales de las PYMES ecuatorianas.

Discusión y propuesta de modelo de cumplimiento progresivo

El problema jurídico que atraviesa este trabajo no se reduce a constatar que las PYMES conocen poco la Ley Orgánica de Protección de Datos Personales, sino a preguntarse qué obligaciones concretas les impone este cuerpo normativo y qué significa, en términos jurídicos, que dichas obligaciones no se estén cumpliendo en sectores calificados como de alto riesgo.

La LOPDP (2021), a partir del principio de responsabilidad proactiva y demostrada, exige que todo responsable del tratamiento pueda acreditar que cada uso de datos personales se apoya en alguna de las bases de licitud previstas para el tratamiento legítimo (art. 7, en relación con el art. 10 lit. k LOPDP); que informe de manera completa y comprensible a los titulares sobre fines, bases legales, plazos de conservación, destinatarios y vías de reclamación (art. 12 LOPDP); que implemente medidas técnicas, organizativas, físicas y jurídicas proporcionales a la naturaleza de los datos y al nivel de riesgo, incluyendo la protección desde el diseño y por defecto y el análisis de riesgos (arts. 10 lits. j y k, 37, 39, 41 y 47 nums. 2 y 7 LOPDP); que documente sistemáticamente sus actividades de tratamiento mediante el Registro Nacional de Protección de Datos Personales, el cual debe ser reportado y mantenido actualizado ante la Autoridad (arts. 47 num. 12 y 51 LOPDP); y que esté en condiciones de gestionar vulneraciones de seguridad y responder al ejercicio de los derechos de información, acceso, rectificación, eliminación y oposición del titular conforme a los plazos y requisitos fijados por la propia

ley (arts. 6, 12 a 16, 37, 40 a 43 y 46 LOPDP).

En el caso de actividades como las telecomunicaciones, la videovigilancia, la geolocalización y el tratamiento de datos biométricos, el propio reglamento y la normativa de la autoridad de control consideran que el riesgo se incrementa y, por eso, exigen obligaciones reforzadas, entre ellas la designación de un delegado de protección de datos personales y la implementación de esquemas de cumplimiento más robustos, independientemente del tamaño de la empresa.

La relevancia de la aplicación efectiva de estas obligaciones para las empresas analizadas no es únicamente formal o sancionatoria; desde la óptica de los derechos fundamentales, el incumplimiento se traduce en una afectación directa de garantías básicas como la privacidad, la autodeterminación informativa y la seguridad de las personas cuyos datos se tratan, porque sin información clara, sin control sobre quién accede a sus datos ni mecanismos para exigir correcciones o supresiones, los titulares quedan en la práctica desprotegidos frente a decisiones empresariales opacas, tal como se desprende de los artículos 66 numerales 19 y 20 y 92 de la Constitución de la República del Ecuador (2008), que reconocen el derecho a la protección de datos personales, a la intimidad y al hábeas data, así como de los artículos 1 y 10 literal k de la Ley Orgánica de Protección de Datos Personales (2021), que establecen que las obligaciones de información, control y seguridad del responsable existen precisamente para garantizar el ejercicio efectivo de esas garantías y cuya inobservancia implica su vulneración.

Desde la perspectiva de la responsabilidad empresarial, la carencia de medidas adecuadas expone a las PYMES a procedimientos administrativos, multas y eventuales responsabilidades penales o civiles si el manejo indebido de datos deriva en daños concretos, lo que vincula de manera directa este problema con la literatura de derecho penal económico y de compliance, que entiende los programas de cumplimiento como verdaderos mecanismos de prevención y gestión de riesgos jurídicos dentro de la organización, tal como establecen los artículos 62 a 64 y 65 a 72 de la Ley Orgánica de Protección de Datos Personales (2021), que regulan el reclamo y el procedimiento administrativo ante la Autoridad de Protección de Datos Personales, así como el régimen de medidas correctivas, infracciones y sanciones administrativas, incluidas multas sobre el volumen de negocios del responsable, sin perjuicio de las acciones civiles, penales o constitucionales que el titular puede ejercer frente a los daños ocasionados por un

tratamiento indebido de sus datos.

En ese marco, el aporte del compliance en protección de datos no consiste en crear una "capa extra" ornamental sobre la empresa, sino en traducir las obligaciones legales en estructuras internas de decisión, control y rendición de cuentas. Para sectores como el tecnológico y la videovigilancia, donde el servicio se construye precisamente a partir del tratamiento intensivo de datos personales y, en el segundo caso, de datos biométricos y de geolocalización, la existencia de un programa de cumplimiento deja de ser una opción conveniente para convertirse en un presupuesto mínimo de licitud de la actividad.

El estudio de las dos PYMES muestra que ambas se ubican de lleno en estas categorías de alto riesgo, pero operan sin delegado registrado, sin registros de actividades de tratamiento, sin evaluaciones de impacto y sin protocolos claros para incidentes, lo que revela no solo desconocimiento, sino una distancia estructural entre el estándar normativo de diligencia exigible y la forma en que la gestión de datos está organizada al interior de las empresas.

A partir de estas premisas jurídicas es que los resultados empíricos cobran sentido: las prácticas descritas por los directivos permiten ver cómo, detrás de medidas técnicas puntuales y de una preocupación genérica por "cuidar la información", subsiste un incumplimiento objetivo de obligaciones que la ley califica como esenciales para responsables que tratan datos sensibles o de alto volumen. Precisamente por ello, la discusión no se limita a narrar lo que hacen o dejan de hacer las PYMES, sino que propone un modelo de cumplimiento progresivo en tres niveles que intenta acercar su realidad actual al estándar exigido por la LOPDP, sin perder de vista las restricciones de recursos y capacidades que caracterizan a este tipo de empresas, para de esta manera incluir el compliance dentro de la cultura empresarial.

Los hallazgos del estudio se conectan de forma directa con lo que viene diciendo la literatura sobre protección de datos personales en la era digital, que no es un tema puramente técnico ni algo que se resuelva instalando un programa informático, sino un desafío de gobernanza y de responsabilidad empresarial que atraviesa toda la organización, desde quien toma las decisiones hasta la última persona que tiene acceso a un archivo o a un sistema (Barzola & Núñez, 2025), en las dos PYMES analizadas se confirma que las pequeñas empresas manejan información tan delicada como las grandes y, en algunos casos, incluso más sensible cuando se trata de datos biométricos o de

seguridad, pero lo hacen sobre la base de un conjunto de prácticas fragmentadas, intuitivas, que todavía no alcanzan la estructura que exige la LOPDP, algo muy cercano a esa "brecha de implementación" que otros autores ya habían descrito entre normas modernas y realidades organizacionales frágiles.

Si se mira la situación con la lente de la responsabilidad social corporativa, lo que aparece es una responsabilidad asumida a medias, porque hay una convicción genuina de que la información de clientes y trabajadores debe cuidarse y se asocia ese cuidado con la confianza y con la reputación, pero esa convicción no termina de convertirse en políticas claras, procesos definidos y rendición de cuentas interna, como plantean los enfoques que entienden la RSC como un proceso de normalización del deber ético dentro de la gestión diaria de la empresa, en las entrevistas se nota que se quiere "hacer lo correcto", que se corrigen errores cuando estallan, pero mientras no existan herramientas adaptadas a su escala las PYMES tienden a ir apagando incendios y no a prevenirlos, lo que las mantiene lejos de una responsabilidad planificada y estable.

Desde el derecho económico y el compliance también se ha insistido en que los programas de cumplimiento no son un manual bonito guardado en un cajón ni un PDF que se enseña al juez cuando hay problemas, sino un sistema vivo de gestión de riesgos con mínimos claros de identificación, control, seguimiento y mejora, a la luz de ese estándar, las PYMES del estudio están en una especie de zona intermedia, ya no hay caos absoluto porque usan contraseñas, restringen ciertos accesos, hacen copias de seguridad y han aprendido de errores pasados; sin embargo, todavía no traducen las obligaciones de la LOPDP en decisiones sistemáticas, medibles y trazables, la ausencia de registros de actividades, de protocolos escritos para incidentes y de capacitaciones mínimas marca que el cumplimiento descansa más en intuiciones y en buena voluntad que en criterios jurídicos y técnicos consolidados.

Si se incorpora el marco de la Agenda 2030, esta situación toca de lleno el Objetivo 16, que reclama instituciones eficaces, transparentes y responsables, porque hoy las empresas, incluso las PYMES (Programa de las Naciones Unidas Para el Desarrollo, 2023), forman parte de ese tejido ampliado de instituciones que pueden aportar a la paz social o, al contrario, generar desconfianza y conflicto si gestionan mal la información, las propias personas entrevistadas reconocen que un incidente con datos puede significar pérdida de clientes, ruptura de contratos, quejas formales y tensiones internas con su propio

personal, de modo que la protección de datos funciona también como un mecanismo preventivo de conflictos y se relaciona con la idea de cultura de paz, entendida como una manera de organizar las relaciones basada en el respeto, la previsión del daño y la transparencia antes de que estalle el problema (CEPAL, 2018).

En coherencia con la literatura de compliance que entiende estos programas como sistemas de gestión de riesgos que deben ser proporcionales al tamaño de la organización y al nivel de exposición, y no como modelos rígidos copiados de las grandes corporaciones (Nieto et al., 2025), y a partir del análisis conjunto del marco normativo de la LOPDP y de las prácticas observadas en las dos PYMES estudiadas, se propone un modelo de cumplimiento progresivo en tres niveles, pensado específicamente para pequeñas y medianas empresas.

La lógica escalonada del modelo recoge, por un lado, el principio de responsabilidad proactiva y de enfoque basado en el riesgo que subyace a la regulación de protección de datos, y por otro, las necesidades concretas que los propios directivos identificaron en las entrevistas cuando describieron qué les haría posible empezar a cumplir sin desbordar sus capacidades.

En ese marco, un primer nivel básico se entiende como el piso mínimo irrenunciable para cualquier empresa que trate datos personales y supone que la PYME identifique de manera ordenada qué datos recoge, de quién, con qué finalidades, sobre qué base jurídica los trata, quiénes acceden a ellos dentro y fuera de la organización y durante cuánto tiempo los conserva.

Este nivel incluye además la adopción de un aviso de privacidad claro para clientes y trabajadores y de una política interna breve que fije reglas esenciales de confidencialidad y manejo de información, de manera que las obligaciones generales de licitud, transparencia y seguridad previstas en la LOPDP (2021), , conforme a los artículos 6 y 10 literales j y k, que consagran los principios de licitud, transparencia y seguridad y obligan al responsable a implementar medidas técnicas y organizativas acordes con dichos principios se traduzcan en decisiones comprensibles y aplicables en la vida diaria de la empresa.

Sobre ese piso se propone un segundo nivel intermedio que no exige grandes estructuras, pero sí un paso adelante en formalización, aquí el modelo incorpora la elaboración de un registro sencillo de actividades de tratamiento donde se ordenen flujos

de datos y bases legales, la designación formal de una persona de referencia en protección de datos, aunque no tenga dedicación exclusiva, la inclusión de cláusulas específicas sobre datos personales en los contratos con clientes y proveedores y la adopción de un protocolo básico para responder ante incidentes y solicitudes de ejercicio de derechos, de conformidad con los artículos 35 y 47 numeral 10 de la Ley Orgánica de Protección de Datos Personales (2021), que exigen regular mediante contrato el acceso a los datos por parte de terceros y suscribir acuerdos de confidencialidad y manejo adecuado de la información, así como con los artículos 12 a 16, 43 y 46 de la misma Ley y los artículos 24 a 28 y 41 del Reglamento General (2023), que obligan al responsable a disponer de procedimientos claros para tramitar los derechos de los titulares y notificar las vulneraciones de seguridad.

Finalmente se plantea un nivel avanzado reservado para aquellas PYMES que, una vez consolidados los pasos anteriores, estén en condiciones de integrar la protección de datos en su estrategia de negocio y en su sistema de gobierno corporativo, en este escalón entrarían medidas como realizar evaluaciones de impacto en protección de datos cuando se pongan en marcha proyectos de alto riesgo, diseñar esquemas de auditoría interna o externa, implementar programas periódicos de formación diferenciada según perfiles de la organización y establecer mecanismos de monitoreo continuo del cumplimiento, en sectores como la videovigilancia o el uso intensivo de biometría, llegar a este nivel implicaría revisar de manera regular la seguridad de los dispositivos, justificar y documentar plazos de conservación de imágenes, registros y mantener un diálogo más estrecho con la autoridad de control, de forma parecida a lo que ya se ha visto en programas de compliance ambiental o anticorrupción donde la prevención termina siendo parte de la identidad de la empresa y no solo un escudo defensivo.

De esa manera, mantener un diálogo más estrecho con la autoridad de control, de forma parecida a lo que ya se ha visto en programas de compliance ambiental o anticorrupción donde la prevención termina siendo parte de la identidad de la empresa y no solo un escudo defensivo, en coherencia con los artículos 39 y 41 de la Ley Orgánica de Protección de Datos Personales (2021), que obligan a realizar evaluaciones de impacto cuando el tratamiento entrañe un alto riesgo para los derechos de los titulares y a revisar periódicamente la eficacia de las medidas técnicas y organizativas, así como con los artículos 37, 39, 41 y 47 numeral 7 de la misma Ley, que imponen la adopción de medidas

de seguridad, la formación del personal y mecanismos de supervisión continua del cumplimiento, especialmente en tratamientos de alto riesgo como la videovigilancia y el uso de datos biométricos.

Este modelo escalonado responde a una preocupación muy clara que expresaron las empresas entrevistadas, la sensación de que la LOPDP (2021) ha sido escrita pensando en estructuras grandes y que trasladar ese estándar sin matices puede volverse inviable para una PYME, al ofrecer niveles diferenciados y acumulativos el cumplimiento deja de verse como un "todo o nada" inalcanzable y se convierte en un camino donde cada organización puede ubicarse según sus capacidades, sin renunciar al núcleo mínimo de protección que corresponde a cualquier tratamiento de datos personales, desde la perspectiva de la cultura de paz esto significa también que la empresa puede ir transformando, paso a paso, la forma en que se relaciona con clientes, trabajadores y terceros, reduciendo espacios de opacidad y arbitrariedad, y fortaleciendo la confianza como un activo que se protege a diario a través de decisiones concretas sobre cómo se trata la información de las personas.

Conclusiones

Del análisis de las dos PYMES se desprende que estas organizaciones trabajan todos los días con datos personales sensibles de clientes, trabajadores y terceros, incluyendo información biométrica y vinculada a la seguridad, pero los mecanismos que utilizan para protegerlos siguen siendo parciales, apoyados más en hábitos internos, en la idea general de "cuidar la información" y en ciertas medidas técnicas puntuales que en un sistema ordenado, de modo que el cumplimiento de la LOPDP y su Reglamento aparece incompleto y disperso, más cercano a una actuación de buena fe que a un programa de compliance diseñado y gestionado de forma sistemática.

Al poner en relación las exigencias del marco normativo con lo que realmente se hace en estas PYMES, se observa una distancia evidente que no solo tiene que ver con el desconocimiento de la ley, sino también con la falta de tiempo, de recursos y de herramientas pensadas para este tipo de empresas, lo que termina reflejándose en la ausencia de registros de tratamiento, en la falta de protocolos frente a incidentes, en una capacitación muy limitada y en una respuesta más bien reactiva cuando surgen problemas, aun cuando los directivos admiten que un manejo inadecuado de los datos podría afectar la confianza, la reputación e incluso generar conflictos con clientes y con el

propio personal.

Ante este panorama, el modelo de cumplimiento progresivo en tres niveles planteado en el artículo se ofrece como un camino posible para acercar la práctica cotidiana de las PYMES al estándar de la LOPDP, comenzando por un nivel básico centrado en identificar los datos que se tratan, sus finalidades y unas reglas mínimas de confidencialidad, pasando luego a un nivel intermedio en el que se formalizan registros, cláusulas y protocolos, hasta llegar a un nivel avanzado en el que la protección de datos se incorpora a la estrategia y a la cultura organizacional, de manera que el compliance deja de entenderse solo como defensa frente a sanciones y pasa a ser también una herramienta para fortalecer la responsabilidad social y aportar a una cultura de paz en las relaciones empresariales.

Como corresponde a un estudio basado en casos, la investigación tiene límites definidos, pues se apoya en la experiencia de dos PYMES y no permite extraer conclusiones generalizables en términos estadísticos, sin embargo, los patrones observados pueden servir de guía para futuros trabajos con muestras más amplias y ofrecer insumos para que autoridades, gremios y universidades elaboren orientaciones y apoyos específicos para PYMES, de tal forma que la protección de datos personales se convierta en un derecho que se ejerce de manera real en el día a día y no solo en un mandato legal difícil de aplicar en la práctica.

Bibliografía

Alcivar, E. (2024). Responsabilidad Social Corporativa como Estrategia para Mejorar el Rendimiento Empresarial. *Revista Científica Zambos, 3*(2), 31-47. https://doi.org/10.69484/rcz/v3/n2/16

Asamblea Nacional del Ecuador. (2021, mayo 26). Ley Orgánica de Protección de Datos Personales. Quito, Ecuador: Registro Oficial Suplemento 459. Retrieved from https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Asqui, A., García, H., & Sandoya, Á. (2024). Análisis y consecuencias del uso de datos personales en el sistema SATJE. *Dominio De Las Ciencias, 10*(4), 1353–1367. https://doi.org/10.23857/dc.v10i4.4157

Barzola, Y., & Núñez, R. (2025). Desafíos legales en la protección de datos personales en la era digital. *3*(1). Obtenido de https://mcjournal.editorialdoso.com/index.php/home/article/download/

Cabrera, K., & Zamora, A. (2024). The constitutional principle of celerity and its non-compliance in the administration of justice in the province of Cañar in the year 2022. *Resistances. Journal of the Philosophy of History, 5*(10), 1-21. https://doi.org/10.46652/resistances.v5i10.150

CEPAL. (2018). *La Agenda 2030 y los Objetivos de Desarrollo Sostenible Una oportunidad para América Latina y el Caribe.* Naciones Unidas. Retrieved from https://repositorio.cepal.org/server/api/core/bitstreams/cb30a4de-7d87-4e79-8e7a-ad5279038718/content

Cevallos, L., & Delgado, J. (2023). *Ley de Protección de Datos Personales: Impacto en la promoción del ODS 16 en el Ecuador* (Vol. 2). https://doi.org/https://www.researchgate.net/deref/https%3A%2F%2Fdoi.org%2F10.59282%2Freincisol.v2%284%29271-?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19

et Silva, J. (2024). *Responsabilidad penal de las empresas y compliance program.* Ediciones Olejnik. Retrieved from https://www.google.com.ec/books/edition/Responsabilidad_penal_de_las_empresas_y/k8ADEQAAQBAJ?hl=es-419&gbpv=0

Ferré, J. (2021). El Objetivo de un Desarrollo Económico Sostenible en la Amazonía: El Criminal Compliance Medioambiental. In I. Gómez de la Torre, *La Protección del Mediambiente y las Políticas de Desarrollo en la Amazonía Brasileña* (pp. 279-300). Grupo Editorial Salamanca. https://doi.org/10.14201/0BR008

Guerrero, E. (2020). Acoso cibernético: perspectivas post covid-19 desde el derecho a la protección de datos personales y la libertad de expresión. *Revista Enfoques de la Comunicación*(4), 42-66. https://doi.org/10.1000/rec.vi4.10

Gutiérrez, N., & Uchuari, J. (2020). Gestión documental del proceso de digitalización en la empresa pública municipañ registro de la propiedad Manta. *Revista Científica de Informática ENCRIPTAR, 3*, 1-10. Retrieved from https://publicacionescd.uleam.edu.ec/index.php/encriptar/article/download/81/169/

Morán, R. (2012). La Normalización de la Responsabilidad Social Empresarial. *Polémika, 3*(9), 38-45. Retrieved from https://revistas.usfq.edu.ec/index.php/polemika/article/view/426

Moreano, C., Escobar, T., Haro, E., & Villagomez, P. (2024). Redes Sociales y su Impacto en el Entorno Digital de las Empresas. *Ciencia Latina Revista Científica Multidisciplinar, 8*(2), 831-857. https://doi.org/10.37811/cl_rcm.v8i2.10531

Nieto, A., de la Mata, N., & Gómez, D. (2025). *Derecho penal económico y de la empresa.* Dykinson. Retrieved from https://editorial.tirant.com/es/libro/derecho-penal-economico-y-de-la-empresa-9788410706163

Presidencia de la República. (2023). Reglamento General de la Ley Orgánica de Protección de Datos Personales. Quito: Registro Oficial Suplemento 435. Retrieved from https://www.cosede.gob.ec/wp-content/uploads/2023/12/REGLAMENTO-GENERAL-A-LA-LEY-ORG%C3%81NICA-DE-PROTECCION-DE-DATOS-PERSONALES_compressed-1.pdf

Programa de las Naciones Unidas Para el Desarrollo. (2023). *¿Qué son los Objetivos de Desarrollo Sostenible?* Retrieved from https://www.undp.org/es/sustainable-development-goals#:~:text=Los%20Objetivos%20de%20Desarrollo%20Sostenible%20(ODS)%2C%20tambi%C3%A9n%20conocidos%20como,disfruten%20de%20paz%20y%20prosperidad.

Ramírez, P. (2021). La Corrupción en el ámbito ambiental y la importancia del compliance en la Amazonía. In I. Gómez de la Torre, *La protección del medioambiente y las políticas de desarrollo en la Amazonia brasileña* (pp. 301-318). Grupo Editorial Salamanca. https://doi.org/10.14201/0BR008

Ramírez, P., & Ferré, J. (2021). *Compliance, Derecho Penal Corporativo y Buena Gobernanza Empresarial.* Bogotá: tirant lo blanch. Retrieved from https://editorial.tirant.com/co/ebook/compliance-derecho-penal-y-corporativo-y-buena-gobernanza-empresarial-2-edicion-paula-andrea-ramirez-barbosa-9788413557274

Superintendencia de Proteccion de Datos Personales. (2025, julio 30). Resolución Nº SPDP-SPD-2025-0028-R. Quito, Ecuador. Retrieved from https://spdp.gob.ec/wp-content/uploads/2025/07/028-R.pdf