Facultad de Jurisprudencia

Maestría en Derecho Corporativo

Protección de datos personales en las pymes: retos de las organizaciones en Colombia y análisis de la Legislación de Privacidad y Seguridad de la Información

Artículo de reflexión

Presentado por:
Ada Carina Ibáñez Peña
Anlly Daniela Quiroga Garzón

Director:
Bayron Prieto Castellanos

Bogotá, D.C. 3 de octubre de 2025

CONTENIDO

Resumen

Las pequeñas y medianas empresas (pymes) en Colombia atraviesan un proceso de transformación digital que implica la adopción de nuevas tecnologías y el tratamiento creciente de datos personales, proceso que plantea importantes desafíos en materia de protección y seguridad de la información; sin embargo, muchas enfrentan obstáculos significativos para cumplir con la normativa vigente de privacidad y seguridad cibernética, tales como la escasez de recursos técnicos y financieros, la falta de claridad en la regulación, y una resistencia estructural al cambio organizacional. Esta situación las expone a riesgos como ciberataques, filtraciones de información y sanciones legales, lo que a su vez puede afectar su operación y la confianza en el mercado, principalmente de clientes y aliados estratégicos. El presente estudio analiza el marco jurídico colombiano sobre privacidad y seguridad de la información, valorando su efectividad frente a los retos de las pymes en la era digital con el fin de proponer estrategias que aseguren el cumplimiento normativo y fortalezcan la competitividad empresarial mediante una gestión responsable de los datos.

Palabras claves:

Protección de datos personales; PYMES; Ciberseguridad; Legislación de privacidad; Seguridad de la información; Habeas data; Datos sensibles; Riesgos digitales; Transformación digital; Cumplimiento normativo; Autodeterminación informativa; Principios de protección de datos; Ley 1581 de 2012; Incidentes de seguridad; Evidencia digital; Respaldo y restauración de información; Cultura organizacional; Ética digital; Autorregulación; Formación empresarial; Confianza empresarial; Sanciones legales; Riesgos reputacionales; Gestión documental; Principios de legalidad y transparencia.

Abstract

Small and medium-sized enterprises (SMEs) in Colombia are undergoing a process of digital transformation that involves adopting new technologies and increasingly managing personal data. This shift brings important challenges for data protection and information security, yet many SMEs struggle to meet existing privacy and cybersecurity regulations due to limited technical and financial resources, regulatory ambiguities, and structural resistance to organizational change. As a result, they face growing risks such as cyberattacks, data breaches, and legal sanctions, which can undermine their operations and weaken market trust among clients and strategic partners. This study examines the Colombian legal framework on privacy and information security, evaluating its effectiveness in the digital era and proposing strategies that promote regulatory compliance while strengthening business competitiveness through responsible data management.

Keywords:

Personal data protection; SMEs (Small and Medium-sized Enterprises); Cybersecurity; Privacy legislation; Information security; Habeas data; Sensitive data; Digital risks; Digital transformation; Regulatory compliance; Informational self-determination; Data protection principles; Law 1581 of 2012; Security incidents; Digital evidence; Backup and data recovery; Organizational culture; Digital ethics; Compliance; Self-regulation; Business training; Business trust; Legal sanctions; Reputational risks; Document management; Principles of legality and transparency.

Introducción.

En un entorno empresarial cada vez más digitalizado, las pequeñas y medianas empresas (pymes) en Colombia enfrentan el reto de adaptarse a un ecosistema tecnológico en constante evolución. La transformación digital, impulsada por el uso intensivo de tecnologías emergentes como la inteligencia artificial y el big data, ha generado nuevas formas de gestionar la información y optimizar procesos organizacionales; no obstante, ha expuesto a las organizaciones a crecientes riesgos relacionados con la seguridad de la información y la protección legal de los datos personales, generando una preocupación importante.

La ciberseguridad se ha convertido en un pilar fundamental dentro de la gestión corporativa, especialmente en un contexto donde las amenazas digitales —como ciberataques, fugas de datos o accesos no autorizados— representan un riesgo constante para la integridad de los activos digitales de las organizaciones. Para las pymes colombianas, el desafío se agrava debido a limitaciones presupuestarias, la falta de personal especializado y una infraestructura tecnológica insuficiente. Estas condiciones no solo dificultan el cumplimiento normativo, sino que también aumentan la exposición a vulnerabilidades que pueden afectar la sostenibilidad operativa y reputacional de estas empresas.

El presente estudio se centra en el análisis del marco jurídico colombiano en materia de privacidad y seguridad de la información, evaluando su pertinencia y efectividad frente a los desafíos que enfrentan las pymes en la era digital y se abordarán los principales obstáculos para la implementación de medidas de ciberseguridad, desde una perspectiva legal, técnica y organizacional. El propósito es identificar estrategias eficaces que permitan a estas organizaciones cumplir con la normativa vigente y, al mismo tiempo, fortalecer su competitividad a través de una gestión responsable y segura de la información. De esta manera, se busca contribuir a la consolidación de un entorno empresarial más confiable, resiliente y alineado con los principios de protección de datos y seguridad cibernética que exige la economía digital actual.

Régimen jurídico de los Datos Personales en Colombia.

La protección de datos personales constituye un pilar esencial para salvaguardar la esfera íntima de los individuos, especialmente en un entorno digital donde la información es accesible de manera inmediata. Esta realidad expone a los ciudadanos al riesgo de que terceros inescrupulosos accedan, manipulen o comercialicen sus datos sin autorización, vulnerando así su derecho fundamental a la privacidad. En este sentido, la protección de datos no solo se concibe como una herramienta legal, sino como una garantía para preservar las libertades individuales frente al uso indebido de la información personal.

Uno de los objetivos fundamentales del régimen de protección de datos es asegurar que el tratamiento de la información personal se realice únicamente bajo condiciones legítimas, es decir, con el consentimiento libre, previo, informado y expreso del titular, el cual debe otorgarse de forma clara y específica para finalidades determinadas, lo que permite al titular ejercer control sobre quién accede, cómo se usa y con qué propósito se manejan sus datos, tanto en contextos internos como externos a las organizaciones.

Dado que los datos personales están ligados directamente al derecho fundamental a la privacidad, su tratamiento requiere no solo autorización, sino también el cumplimiento de principios rectores como la calidad, veracidad, actualización y pertinencia de la información. De esta manera, se garantiza que los datos tratados sean exactos, completos y estén alineados con los fines autorizados por el titular, reduciendo los riesgos asociados al uso indebido, la obsolescencia o la inexactitud de la información.

Conforme a lo anterior, es preciso señalar que el artículo 15 de la Constitución Política de Colombia (1991) consagra expresamente los derechos fundamentales a la intimidad y al buen nombre, y aunque el texto constitucional no emplea el término *habeas data*, la jurisprudencia de la Corte Constitucional ha interpretado que este se encuentra implícito en los incisos primero y segundo de la norma, en la medida en que reconocen a todas las personas el derecho a *"conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas"*, estableciendo además que *"en la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución",* y en

ese sentido, debe ser reconocido como un derecho autónomo que está estrechamente vinculado con los derechos fundamentales a la libertad y la información (Sentencia T-238/18 2018), y tiene como principal finalidad proteger una nueva dimensión de la autodeterminación personal (Sentencia T-307/99 1999), que ha adquirido especial relevancia con el auge de la era digital y la expansión de las tecnologías de la información y la comunicación.

Si bien algunos autores en materia doctrinal, e incluso la Superintendencia de Industria y Comercio (2022), han optado por referirse al derecho fundamental a la protección de datos personales, lo cierto es que para el presente caso se estudiará el derecho al *habeas data* como eje articulador del régimen de protección de datos en Colombia, en tanto constituye el mecanismo jurídico a través del cual se garantiza el control sobre la información personal. Este enfoque permite comprender la protección de datos no solo como una garantía autónoma, sino también como una expresión del derecho constitucional a la privacidad o intimidad, y desde esta perspectiva, el tratamiento de los datos personales se convierte en una actividad regulada que debe atender a principios fundamentales como la legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad, conforme lo dispone la Ley 1581 de 2012. Bajo este enfoque, se procederá a delimitar qué se entiende por datos personales, su clasificación normativa, y el potencial impacto que su uso indebido puede generar sobre los derechos fundamentales del titular.

Clasificación, Concepto y Protección Jurídica de los Datos Personales en Colombia

La doctrina ha elaborado múltiples definiciones sobre los datos personales, partiendo inicialmente del concepto de "dato" como unidad básica de información. En términos generales, un *dato* puede entenderse como la representación simbólica, numérica, alfabética o gráfica de un hecho que ha ocurrido o que se encuentra sucediendo en el momento en que es capturado o registrado (Osuna Carreño 2024). Esta representación adquiere significado en tanto puede ser interpretada y utilizada en diversos contextos informativos, jurídicos o tecnológicos; no obstante, la Ley 1581 de 2012, al definir los datos personales, no se enfoca únicamente en su estructura formal o representación simbólica, sino que subraya su dimensión jurídica y subjetiva, al establecer

que estos comprenden *"cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables";* esta definición pone en evidencia que, más allá del hecho representado, lo que convierte a un dato en personal es su capacidad de ser atribuido a un individuo específico, cuya identificación sea directa o indirectamente posible.

La Ley 1581 de 2012: Objeto y Ámbito de Aplicación

La Ley 1581 de 2012 desarrolla el derecho constitucional consagrado en el artículo 15 de la Constitución Política de Colombia -*habeas data*-, que faculta a todas las personas a conocer, actualizar y rectificar la información personal recogida sobre ellas en bases de datos o archivos. Este derecho representa una manifestación concreta de la autodeterminación informativa, al permitir que el titular ejerza control sobre su información personal frente a terceros públicos o privados (2012). Las disposiciones de esta ley se aplican al tratamiento de datos personales efectuado en territorio colombiano, o incluso fuera de él, cuando el responsable o encargado del tratamiento, no establecido en Colombia, se someta a la legislación nacional en virtud de tratados internacionales o normas con efectos extraterritoriales. Asimismo, su ámbito de aplicación comprende cualquier base de datos, pública o privada, siempre que se realice un tratamiento automatizado o manual de la información que permita su organización, acceso o consulta.

No obstante, excluye determinadas categorías de bases de datos que, por su naturaleza o finalidad, requieren un tratamiento jurídico diferenciado. Entre ellas se encuentran los archivos de uso exclusivamente personal o doméstico, los relacionados con seguridad y defensa nacional, los vinculados a actividades de prevención, detección, monitoreo y control del lavado de activos y la financiación del terrorismo, así como las bases de datos con fines periodísticos o editoriales. También se exceptúan aquellas reguladas por normativas especiales, como las bases de datos con información financiera, crediticia y comercial, que se rigen principalmente por la Ley 1266 de 2008. Este conjunto de excepciones no implica una contradicción normativa, sino que responde a un modelo regulatorio por capas, donde la ley aquí estudiada actúa como norma general y otras leyes complementan o incluso reemplazan sus disposiciones cuando se trata de sectores que exigen un mayor nivel de especialización o protección. De esta forma, se reconoce que no todos los datos personales presentan el mismo nivel de sensibilidad ni todos los nichos

enfrentan los mismos riesgos. Así, por ejemplo, el tratamiento de datos financieros tiene exigencias técnicas y legales distintas de aquellas aplicables a datos de salud o de localización geográfica.

Este marco supone un desafío especial para las pymes, que a menudo carecen de personal especializado o de estructuras legales sólidas para interpretar las diversas capas regulatorias. Por ello, es fundamental realizar un análisis jurídico integral que permita identificar el tipo de datos tratados, el sector económico al que pertenece la organización y los posibles cruces normativos. Solo con este conocimiento se podrá asegurar un cumplimiento normativo eficaz y una gestión adecuada de los riesgos legales asociados al tratamiento de datos personales (Superintendencia de Industria y Comercio 2021).

Ahora bien, la Superintendencia de Industria y Comercio -SIC- complementa la definición que resaltamos anteriormente dispuesta en la Ley, al referirse a los datos personales como toda información asociada a una persona natural que permite su identificación, directa o indirectamente. Dentro de esta categoría se incluyen elementos como el número de documento de identidad, lugar y fecha de nacimiento, estado civil, edad, residencia, así como la trayectoria académica, profesional o laboral del individuo (Superintendencia de Industria y Comercio 2021).

En este sentido, el tratamiento de datos personales debe regirse por un conjunto de principios fundamentales consagrados en la Ley 1581 de 2012, que estructuran el régimen jurídico de protección de datos en Colombia. Estos principios no solo garantizan el ejercicio del derecho al *habeas data*, sino que también establecen estándares que deben ser cumplidos por todas las personas naturales o jurídicas, públicas o privadas, que realicen tratamiento de datos personales.

- Legalidad: debe ajustarse a lo establecido por la ley.
- Finalidad: el tratamiento debe tener un propósito legítimo, claro e informado.
- Libertad: requiere consentimiento previo, expreso e informado del titular.
- Veracidad: los datos deben ser exactos y actualizados.
- Transparencia: el titular puede acceder a su información en cualquier momento.
- Acceso y circulación restringida: los datos no deben estar libremente disponibles.
- Seguridad: deben adoptarse medidas para evitar su pérdida o alteración.
- Confidencialidad: quienes traten datos están obligados a garantizar su reserva.

Estos principios son esenciales para que el tratamiento de datos personales se realice dentro del margen del respeto a los derechos fundamentales y se constituyen en ejes transversales del modelo de cumplimiento en protección de datos, caracterizado por la rápida y masiva circulación de información. Su aplicación rigurosa es especialmente crítica para las pequeñas y medianas empresas, que, aunque con menos recursos, no están exentas de las obligaciones legales y enfrentan riesgos similares a los de grandes organizaciones.

Adicionalmente, la normatividad citada, junto con el Decreto Reglamentario 1377 de 2013, establece una clasificación de los datos personales con el fin de determinar el nivel de protección y las condiciones específicas para su tratamiento, pues especifica las obligaciones que se traducen en requisitos operativos concretos, entre ellas, la necesidad de conservar prueba de la autorización, la limitación temporal del tratamiento de datos, lo que implica que la información solo puede ser recolectada, almacenada, usada o circulada durante el tiempo que sea razonable y necesario para las finalidades que justificaron el tratamiento; también se introduce el concepto legal del Registro Nacional de Bases de Datos. Esta clasificación inicial debe ser cuidadosamente considerada, ya que de ella dependen las obligaciones legales aplicables y las medidas de cumplimiento requeridas.

A. Dato Público: Ejemplos concretos incluyen el número de identificación, apellidos, lugar y fecha de expedición del documento. Su tratamiento no requiere autorización del titular, aunque debe respetar los principios de la ley.

En cuanto a los niños, niñas y adolescentes, si bien el tratamiento de datos personales de menores está prohibido, como regla general, se permite su divulgación cuando se trate de datos de naturaleza pública, de conformidad con lo establecido en el artículo 7° de la Ley 1581 de 2012. Aun así, dicho tratamiento debe responder y respetar el interés superior de los niños, niñas y adolescentes y asegurar el respeto de sus derechos fundamentales.

B. Dato Semiprivado: Son datos cuyo conocimiento interesa no solo al titular, sino a un grupo determinado, como la fecha y lugar de nacimiento o información crediticia. Aunque no son íntimos, su tratamiento sí requiere autorización previa, expresa e informada del titular, conforme a los principios de libertad y finalidad.

C. Dato Privado: Los datos privados son de naturaleza íntima o reservada, como la dirección de residencia o el número telefónico. Su tratamiento exige autorización del titular o una orden legal o judicial que lo justifique. La divulgación sin consentimiento está prohibida

D. Dato Sensible: Los datos sensibles son aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación. La Ley 1581 de 2012, en su artículo 5, proporciona una lista enunciativa de estos datos, incluyen información sobre salud, orientación política, convicciones religiosas, datos biométricos, entre otros. La Corte Constitucional (2011) ha aclarado que esta lista no es taxativa, y que la condición de víctima de violencia, por ejemplo, puede ser considerada un dato sensible si afecta la intimidad del titular y genera discriminación, postura que ha sido acompañada en múltiples ocasiones por la Superintendencia de Industria y Comercio en sus conceptos.

El tratamiento de datos sensibles está prohibido como regla general; sin embargo, el artículo 6 de la Ley 1581 de 2012 prevé excepciones bajo las cuales es viable su uso, siempre que medie una autorización expresa, ya sea por escrito o de forma verbal, aclarando que el silencio nunca podrá interpretarse como manifestación válida de voluntad. Además, se debe informar al titular que, por tratarse de datos sensibles, no está obligado a autorizar su tratamiento, y ninguna actividad podrá condicionarse a que suministre datos personales sensibles.

Es relevante observar que, si bien la Ley 1581 de 2012 establece las definiciones fundamentales para "dato personal" y "dato sensible", no define explícitamente los "datos privados" o "semiprivados". Estas definiciones han sido proporcionadas posteriormente por las entidades administrativas; tal dinámica evidencia un proceso interpretativo continuo, donde el marco legal primario establece las líneas generales, pero la aplicación práctica y la categorización detallada se refinan y aclaran a través de actos administrativos y la jurisprudencia.

Para los profesionales del derecho y los oficiales de protección de datos, o para quien cumpla dicha función en una pymes, que puede ser incluso el mismo gerente, una comprensión exhaustiva de la clasificación de datos en Colombia exige ir más allá del texto literal de la ley en estudio; requiere un seguimiento constante de las resoluciones, conceptos y circulares de la SIC, quien administra el Registro Nacional de Bases de Datos (RNBD) -*instrumento clave para el ejercicio de la función de vigilancia y control*-, ya

que estos actos administrativos proporcionan una guía esencial y, en la práctica, configuran el alcance y la aplicación precisos de las categorías de datos. Esta interpretación dinámica asegura que la ley se mantenga relevante frente a nuevos tipos de datos y contextos de procesamiento.

Se advierte que, como se analizará más adelante, la manipulación, divulgación sin autorización o uso indebido de esta información puede generar efectos que van más allá de lo patrimonial o reputacional, pues expone al titular a riesgos de discriminación, estigmatización, persecución o exclusión en los ámbitos laboral, financiero, educativo o social. Véase, por ejemplo, lo dispuesto por la Corte Constitucional, en sentencias como la T-444 de 2014, donde resaltó que los datos sensibles —como los relativos a la salud, la orientación sexual o las creencias religiosas— demandan un nivel de protección reforzado, pues su divulgación inadecuada puede derivar en estigmatización, discriminación o exclusión social, ya que la manipulación indebida de esta información no solo compromete la esfera privada, sino que puede afectar de manera directa derechos como la igualdad, el libre desarrollo de la personalidad y la dignidad humana, en tanto dichos datos suelen estar asociados a factores históricamente objeto de prejuicios y marginación. De ahí que la jurisprudencia constitucional vincule la protección de datos sensibles con la garantía de no discriminación y la necesidad de impedir que la información personal se convierta en un mecanismo de exclusión.

No obstante, resulta preocupante observar que en la práctica empresarial contemporánea —y con mayor frecuencia en los últimos años— este tipo de datos se solicitan en formularios digitales simples, como Google Forms, sin cumplir con estándares adecuados de seguridad ni con los principios de finalidad, necesidad y proporcionalidad exigidos por la Ley 1581 de 2012. En la misma línea, la Corte Suprema de Justicia, al interpretar el artículo 269F del Código Penal (Ley 1273 de 2009), ha advertido que el uso indebido, la divulgación o manipulación de datos sensibles puede configurar delitos informáticos, al afectar la confidencialidad, integridad y disponibilidad de la información (Auto Interlocutorio, 2011). Con ello se refuerza la idea de que la protección de estos datos trasciende lo patrimonial o reputacional, proyectándose hacia la defensa de derechos fundamentales frente a riesgos de discriminación y exclusión social.

Además, la pérdida de control sobre la información personal puede generar un profundo sentimiento de vulnerabilidad y desprotección, erosionando la confianza en las

instituciones públicas y privadas. Por ello, la protección efectiva de los datos personales no es solo un imperativo legal, sino una garantía indispensable para el ejercicio libre y pleno de los derechos fundamentales en el Estado Social de Derecho colombiano.

Riesgos para la protección de datos personales en PYMES colombianas.

Como se ha reiterado, la protección de los datos personales constituye un componente crítico para la sostenibilidad y la reputación empresarial en el entorno contemporáneo. En Colombia, las pequeñas y medianas empresas (pymes) representan el 99,5 % del tejido empresarial formal, aportan entre el 35 % y el 40 % del Producto Interno Bruto (PIB) y generan cerca del 79 % del empleo total (González Patiño y Llanes Valenzuela 2024), lo que las convierte en un actor fundamental para el desarrollo económico y social del país. A pesar de su relevancia, este segmento empresarial enfrenta una alta vulnerabilidad frente a los riesgos de ciberseguridad y las brechas de datos, situación que obedece, en gran medida, a la escasez de recursos, a la percepción de que las soluciones tecnológicas resultan costosas y a una preparación limitada para hacer frente a ciberataques. Esta combinación de factores, junto con la importancia estratégica del sector, configura un riesgo sistémico que trasciende lo individual y puede impactar la estabilidad económica general. Cuando la columna vertebral de la economía nacional se encuentra expuesta estructuralmente a riesgos asociados al tratamiento de la información, la resiliencia macroeconómica se ve inevitablemente comprometida.

Como se pasará a ver, la inobservancia de los principios fundamentales de la Ley 1581 de 2012 es una de las principales fuentes de riesgo legal para las pymes, dado que los datos personales deben ser recolectados para fines específicos y legítimos, y solo pueden ser tratados para esas finalidades previamente informadas al titular, tal como lo establece el artículo 4 de la Ley 1581 de 2012. Una vez cumplida la finalidad, la información debe conservarse únicamente por el tiempo razonable y necesario, siendo obligatoria su supresión o anonimización cuando deje de ser requerida (Ámbito Jurídico 2021); sin embargo, en la práctica, muchas pymes utilizan datos para fines no autorizados, como enviar mensajes comerciales a números obtenidos para una transacción puntual, o los retienen indefinidamente sin justificación, lo que configura un riesgo legal directo.

Estas falencias suelen originarse en la ausencia de políticas y procedimientos internos, obligación cuyo incumplimiento ha sido identificado reiteradamente por la Superintendencia de Industria y Comercio, según el *Estudio de Sanciones 2022* de la Escuela de Privacidad (2023). Dicho estudio reveló que el 28% de las empresas sancionadas carecían de manuales internos de políticas y procedimientos para el tratamiento de datos personales, lo que evidencia una debilidad estructural en la gestión de la protección de datos («Ciberseguridad en Colombia: Estrategias y Desafíos Actuales» 2024). Esta carencia se ve agravada por la falta de capacitación y concientización del personal, factores que incrementan la probabilidad de errores humanos, los cuales constituyen actualmente la principal causa de filtraciones de datos y de ciberataques, pues gran parte de los incidentes de seguridad se originan en fallas humanas como contraseñas débiles, phishing o descuidos operativos (Terranova Security, s. f.); en consecuencia, la ausencia de directrices claras y la falta de formación adecuada generan un efecto cascada que deriva en brechas de seguridad y, finalmente, en violaciones legales. Así, sin una política documentada o sin que esta cumpla con los requisitos legales, las pymes no están en capacidad de demostrar el cumplimiento de sus obligaciones, quedando expuestas tanto a sanciones administrativas como a la pérdida de confianza de clientes y aliados estratégicos.

Además, los responsables y encargados del tratamiento de datos personales deben cumplir los deberes consagrados en el Título IV de la misma ley, exigencias esenciales para una gestión legal y segura de las bases de datos. Uno de estos deberes es conservar la prueba de la autorización otorgada por los titulares, pues la imposibilidad de acreditarla es una causa frecuente de sanciones por parte de la Superintendencia de Industria y Comercio (SIC). Al respecto, la Sentencia C-748 de 2011 de la Corte Constitucional señala que el consentimiento debe ser previo, expreso e informado, y exige que cualquier tipo de recolección o uso de datos personales se acompañe de esta autorización clara. La falta de cumplimiento con este deber es recurrente: se estima que el 33 % de las empresas sancionadas no logran demostrar el consentimiento válido (Escuela de Privacidad 2023). Esta deficiencia es particularmente visible en prácticas comunes de las pymes, como la recolección de datos en sitios web o redes sociales - donde muchas empresas acceden a números de teléfono, direcciones de correo electrónico e incluso información personal y laboral publicada en LinkedIn—, la utilización de números de contacto obtenidos

mediante referidos para fines comerciales, o el envío de publicidad y comunicaciones sin autorización previa del titular.

Un caso reciente que ilustra la sanción por no demostrar autorización es la expuesta en la Resolución No. 60011 de 2024, en la que la SIC sancionó a un centro de idiomas por no presentar prueba de consentimiento en los términos ya descritos para enviar publicidad sobre cursos de inglés y francés, y aprobar un crédito financiero que le permitiera a la cliente acceder a lo ofrecido, utilizando datos personales sin contar con el respaldo probatorio requerido. Al ser solicitada la autorización, la empresa no aportó la evidencia correspondiente y, en consecuencia, la SIC ordenó implementar procedimientos adecuados para solicitar y conservar la autorización de los titulares, e impuso una multa equivalente a dos salarios mínimos legales mensuales vigentes para el año 2023.

Ahora bien, los responsables también deben adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y, en especial, para la atención de consultas y reclamos. La falta de una política documentada, o una que no cumpla con todos los requisitos legales, es un incumplimiento grave que impide una gestión coherente y estandarizada de los datos. Es imperativo implementar medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad y confidencialidad de la información, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, pues las brechas de seguridad por medidas inadecuadas, como la falta de antivirus o bloqueos en puertos USB, son una causa directa de incidentes y, por ende, de sanciones.

Se entienden por incidentes de seguridad las violaciones de acceso, intento de acceso, uso inadecuado, divulgación, modificación o destrucción no autorizada de información, cambios no controlados en el sistema, errores humanos, incumplimiento de las políticas de seguridad, pérdida o robo de información o recurso tecnológico, mal funcionamiento, manipulación, sabotaje, virus, códigos maliciosos, negación del servicio, violaciones de confidencialidad, entre otros.

En ese contexto, un evento de seguridad de la información corresponde a la presencia identificada de una condición en un sistema, servicio o red, que puede indicar una posible violación de la política de seguridad de la información, una falla de las salvaguardas existentes o incluso una situación desconocida que pueda resultar relevante

para la protección de los activos informáticos. Por su parte, un incidente de seguridad de la información. Hace referencia a un evento o serie de eventos no deseados o inesperados que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. (INCONTEC 2012)

Ante este panorama, resulta indispensable que las pymes implementen políticas de seguridad de la información orientadas a minimizar el riesgo de actos que puedan afectar negativamente sus procesos internos, la continuidad operativa y la imagen corporativa. Estas políticas deben complementarse con la creación de un plan formal de gestión de incidentes de seguridad, el cual permita atender oportunamente cualquier eventualidad, optimizar la respuesta institucional, minimizar los daños y garantizar la continuidad del negocio frente a las amenazas que puedan materializarse. El objetivo principal de dicho plan es garantizar una respuesta eficiente ante la ocurrencia de situaciones que afecten la prestación de los servicios, siendo necesario establecer mecanismos claros de detección, evaluación y tratamiento de incidentes, así como gestionar de manera proactiva las vulnerabilidades, con el fin de mantener los sistemas, redes y aplicaciones en un nivel adecuado de seguridad.

Para ello, resulta fundamental definir roles y responsabilidades, evaluar periódicamente riesgos y establecer procedimientos formales de reporte y escalamiento de incidentes. La gestión de todos los eventos de seguridad debe orientarse a su detección temprana y tratamiento oportuno, en este sentido, la documentación adecuada de cada caso, su evaluación y respuesta efectiva, constituyen pasos fundamentales que, además, permiten consolidar lecciones aprendidas para fortalecer la prevención de futuros incidentes.

En lo que respecta a la conservación de la información, la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) se convierte en una herramienta indispensable, ya que busca preservar la confidencialidad, integridad, disponibilidad y privacidad de la información y de los datos recolectados o generados en el desarrollo de las funciones empresariales. Para que el SGSI sea efectivo, es imprescindible que las políticas de seguridad y privacidad definidas tengan carácter obligatorio y sean ampliamente conocidas, comprendidas y aplicadas por todos los colaboradores de la organización.

Es indispensable activar un plan de seguridad, conservación y privacidad de la información, que permita planear, organizar, dirigir y controlar las actividades necesarias para resguardar la continuidad del negocio y de las comunicaciones, asegurando el uso eficiente de los activos de Tecnologías de la Información y las Comunicaciones (TIC). En este marco, se recomienda que las PYMES adopten políticas específicas orientadas a fortalecer su capacidad de prevención y respuesta frente a riesgos y amenazas, entre ellas:

Política de retención y archivo de datos

El propósito fundamental de estas medidas es conservar la integridad de los activos de información, garantizando la disponibilidad de los servicios y el tratamiento adecuado de los datos, documentos y sistemas físicos y digitales de los distintos procesos y áreas de la empresa. En ese sentido, una recomendación y posible estrategia para evitar el riesgo en estudio, consiste en implementar Tablas de Retención Documental – TRD, ya que este instrumento archivístico facilita el manejo de la información y permite determinar la ubicación de los documentos y el tiempo que deben permanecer almacenados en los archivos de gestión central o histórico (físico o electrónico). Para ello, se pueden tener en cuenta las directrices del Archivo General de la Nación, autoridad rectora de la política archivística del país. De igual manera, reglamentar e implementar políticas archivísticas que definan los parámetros para la organización en materia de conservación de la información, siendo incluso una opción, la utilización de bases de datos y sistemas de información que respalden la administración y preservación de archivos, fortaleciendo la gestión documental y contribuyendo a mitigar los riesgos asociados a la falta de registro, control y trazabilidad de los incidentes de seguridad.

Política de incidentes de seguridad de la información y manejo de incidencias

Que establece que cada equipo de trabajo debe contar con su propio plan de incidentes y protección de activos esenciales para la atención de usuarios internos y externos. Para ello, es necesario contar con listas de responsables con sus respectivas funciones, así como mecanismos claros de control, detección, acción y reporte.

Como directrices se podrían implementar las siguientes:

a) Todos los incidentes deben recibir el tratamiento adecuado y documentado, conforme al procedimiento de atención de incidentes, para determinar sus causas y responsables.

b) Al detectar un incidente, se debe actuar con precaución para no comprometer la seguridad de la evidencia y asegurar su correcta custodia.
c) Mantener la cadena de custodia de la información y establecer medidas de seguridad, roles y acciones de acceso, comunicación y salvaguarda.

Política de conservación de evidencia digital, respaldo y restauración de información

Tiene como objetivo garantizar la seguridad, integridad y confiabilidad de lo consignado en bases de datos, sistemas de información y software, mediante la implementación de mecanismos de respaldo. En ese sentido, el encargado del sistema debería asegurar la realización de copias de seguridad de la configuración de las plataformas tecnológicas y de todos los recursos tecnológicos de la entidad, como servidores, equipos de red y dispositivos inalámbricos, entre otros, siguiendo los lineamientos definidos por cada área en la empresa. Asimismo, corresponde al personal encargado definir la periodicidad de las copias, ya sea diaria, semanal o mensual, y verificar su correcto funcionamiento y el cumplimiento de los requisitos técnicos y administrativos. Conforme a ello, todos los trabajadores, contratistas y terceros tienen la responsabilidad de crear copias de seguridad de los archivos que utilizan, producen o administran, empleando exclusivamente los sistemas de salvaguarda aprobados, con el fin de asegurar la disponibilidad de la información y su recuperación en caso de incidentes.

En el caso de las pymes, la implementación de una política de conservación de evidencia digital, respaldo y restauración de la información puede verse limitada por la falta de áreas especializadas o de personal suficiente para asignar un responsable exclusivo, aun así, la medida resulta fundamental porque la seguridad e integridad de los datos son esenciales para la continuidad del negocio, en ese sentido, la responsabilidad puede recaer en la persona o equipo con contacto directo con los datos, lo que facilita adaptar la política a la realidad de la organización y asegurar que, incluso con recursos limitados, existan mecanismos básicos de respaldo y recuperación que disminuyan los riesgos asociados a la pérdida de información.

La correcta gestión de incidentes y la adecuada conservación de la información constituyen factores críticos para la seguridad, continuidad y sostenibilidad de las pymes. Implementar estas políticas de manera integral permite proteger los activos de

información, cumplir con la normativa vigente, reducir riesgos operativos y reputacionales, y fortalecer la confianza de clientes, proveedores y aliados estratégicos.

Adicionalmente, cuando las medidas de seguridad adoptadas no resultan efectivas, la Ley 1581 de 2012 impone a los encargados del tratamiento de datos el deber de *"Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares"*[1], obligación que, de acuerdo con la Circular Única de la SIC, debe cumplirse dentro de los quince días hábiles siguientes a la detección del incidente, independientemente de su complejidad, ya que la omisión en el reporte constituye por sí misma una infracción sancionable.

Las sanciones que puede imponer la SIC constituyen un riesgo significativo para las pymes, ya que pueden afectar gravemente su estabilidad financiera y operativa. Entre estas medidas se encuentran las multas de carácter personal o institucional cuyo valor puede alcanzar hasta dos mil salarios mínimos mensuales vigentes y que además pueden imponerse de manera sucesiva mientras persista la infracción[2], lo que representa una carga económica difícil de asumir para empresas con recursos limitados. A ello se suma la facultad de la autoridad de ordenar la suspensión de las actividades de tratamiento de datos por un periodo de hasta seis meses o incluso disponer el cierre temporal de las operaciones cuando no se subsanan los incumplimientos en el plazo establecido. En situaciones particularmente graves, como en los casos que comprometen el manejo de datos sensibles, la sanción puede llegar al cierre definitivo de la actividad empresarial.

---

1 Ley 1581 de 2012, "Artículo 18. Deberes de los Encargados del Tratamiento. Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad: (...) k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares"

2 Ley 1581 de 2012, "Artículo 23. Sanciones. La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:

a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;

b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;

c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;

d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles;

Parágrafo. Las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva."

Por ejemplo, en 2024 la empresa *Risks International S.A.S.* fue sancionada por infracciones a la normativa de protección de datos personales en Colombia. La investigación reveló que la compañía gestionaba una base de datos denominada *Siriest/Siscom* que contenía información sensible de titulares sin tener autorización previa, expresa e informada de datos como antecedentes judiciales, multas de tránsito, desempeño laboral, etc., y la empresa no garantizó mecanismos efectivos para que los ciudadanos ejercieran sus derechos de acceso, rectificación o supresión de la información, lo que configuró una vulneración al derecho fundamental al hábeas data (La República 2025). Como consecuencia, se impuso una multa de $190 millones (COP) y ordenó la suspensión temporal de las actividades de tratamiento de datos relacionadas con dicha base, advirtiendo que, si no se implementaban los correctivos ordenados, la sanción podía llegar al cierre definitivo de operaciones, ya que las bases de datos creadas se utilizaban como filtro para la contratación en empresas de transporte terrestre de carga bajo el argumento de cumplir con las normas de prevención del lavado de activos y financiación del terrorismo; sin embargo, dicha información solo está exceptuada de la Ley 1581 de 2012 cuando es creada y administrada por entidades públicas en el marco de sus funciones legales, por lo que los particulares no pueden generarlas con ese fin sin garantizar los derechos de los titulares, especialmente en cuanto a veracidad, calidad de la información, consentimiento previo y tratamiento de datos sensibles (Superintendencia de Industria y Comercio 2025)

El caso de *Risks International S.A.S.* evidencia cómo la ausencia de autorización clara y de procedimientos internos para garantizar el ejercicio de derechos puede derivar en consecuencias económicas y reputacionales significativas para las empresas, lo que constituye un ejemplo de la importancia de implementar mecanismos de consentimiento documentado, canales efectivos de atención a los titulares y controles de seguridad adecuados en las bases de datos, a fin de mitigar riesgos legales y proteger la confianza de clientes y aliados estratégicos, pues más allá de las sanciones económicas y operacionales directas, la afectación con la relación con clientes, proveedores, financistas y socios comerciales lleva a la pérdida de oportunidades de negocio y de confianza.

Este "costo oculto" puede ser mucho más perjudicial, dado que a menudo las pymes dependen en gran medida de su reputación local y la confianza de su comunidad para su supervivencia y crecimiento. La pérdida de confianza puede ser irreparable,

llevando a una disminución de clientes y una afectación duradera en el posicionamiento empresarial.

Además, los titulares afectados por incidentes de seguridad, como fugas de información derivadas de ciberataques, pueden reclamar indemnización por daños patrimoniales y extrapatrimoniales, siempre que acrediten el perjuicio sufrido. La jurisprudencia civil colombiana ha desarrollado subcategorías de perjuicios extrapatrimoniales, destacando los vinculados a la vulneración de derechos fundamentales como el buen nombre, la imagen, la privacidad y la dignidad, los cuales cuentan con especial protección constitucional (Castillo Díaz 2020), por ejemplo, la Corte Suprema de Justicia, en sentencia SC10297-2014, precisó que estos daños pueden manifestarse como daño moral, daño a la vida de relación o afectación a derechos fundamentales.

Véase también que en Colombia, la responsabilidad penal por la violación de datos personales se encuentra regulada principalmente por la Ley 1273 de 2009, que tipifica los ciberdelitos desde diversas perspectivas, incluyendo el acceso abusivo a sistemas informáticos, la obstaculización ilegítima de datos, la interceptación de información, la generación de daños a sistemas, la creación y distribución de software malicioso, así como la violación, suplantación, hurto y transferencia ilícita de datos personales. Quien incurra en estos actos se expone a penas privativas de la libertad y multas, reflejando la gravedad con la que el ordenamiento jurídico colombiano protege la información personal y corporativa frente a amenazas digitales. Esta regulación destaca la necesidad de abordar los ciberdelitos de manera integral, no solo desde la perspectiva del atacante, sino también considerando la protección preventiva dentro de las organizaciones.

En este contexto, resulta fundamental que las empresas, en especial las pymes, implementen estrategias de prevención orientadas al factor humano, fomentando dentro de su cultura organizacional hábitos que minimicen vulnerabilidades como descuidos o prácticas inseguras en la gestión de la información digital. Entre estas medidas se incluyen la limitación del acceso a información sensible, el uso de herramientas de protección como redes privadas virtuales (VPN) que cifran la conexión y mejoran la seguridad, así como la formación continua de los colaboradores sobre buenas prácticas digitales. Sin embargo, estas soluciones también presentan riesgos, dado que los atacantes pueden utilizar VPN para ocultar su ubicación y dificultar la identificación del origen del ataque

(Prieto Castellanos 2019), lo que puede complicar la presentación de denuncias o la instauración de acciones penales.

La ciberseguridad en Colombia: más allá del cumplimiento, una necesidad empresarial frente a los riesgos del entorno digital.

Los sistemas de información al tener importancia y dependencia con las empresas en la actualidad ponen en riesgo la seguridad de la información de todos los individuos que la utilizan, ya que los grandes datos pueden ser vulnerados por delincuentes informáticos que buscan capturar la información de manera ilegal, por esta razón se necesita de un sistema de defensa que proteja los datos personales que se localizan en el ciberespacio, este sistema se denomina la ciberseguridad.

La ciberseguridad se configura como una estrategia fundamental para gestionar el ciberriesgo, entendida como el conjunto de técnicas, prácticas y procesos orientados a proteger la información vinculada con los usuarios de las cibertecnologías, lo que implica no solo la vigilancia sobre los datos en sí mismos, sino también sobre los sistemas, infraestructuras y componentes asociados a su administración. En este sentido, su objetivo esencial es resguardar todos aquellos recursos o activos que resultan valiosos para una persona, una empresa o una organización.

Uno de los principales desafíos que enfrentan las empresas en Colombia es la adopción de sistemas de ciberseguridad. En el caso de las pequeñas y medianas organizaciones, estas herramientas no suelen considerarse elementos fundamentales dentro de su estructura operativa, por el contrario, suelen percibirse como un gasto prescindible y no como una inversión estratégica, pese a los altos riesgos asociados a su no implementación, como podrían ser: la pérdida de la información, deterioro de la imagen corporativa e ingresos futuros dejados de percibir. Por consiguiente, es fundamental generar conciencia sobre la relevancia de implementar un sistema robusto de protección de datos, que brinde seguridad a las operaciones empresariales y fortalezca la confianza, y tranquilidad, tanto interna como externa.

De acuerdo con el Ministerio de Tecnologías de la Información y las Comunicaciones (Ministerio de Tecnologías de la Información y las Comunicaciones 2023), la Estrategia Nacional de Ciberseguridad busca consolidar un modelo de

protección integral que beneficie tanto a usuarios finales como a servidores públicos, empresas y ciudadanía en general; no obstante, como se mencionó, muchas pymes continúan percibiendo estas iniciativas como cargas económicas, lo que dificulta la adopción de medidas eficaces para resguardar sus activos digitales. En consecuencia, tanto las personas como las empresas deben, según su área de especialización y negocio, confiar en expertos que crean herramientas y desarrollan soluciones orientadas a la protección de dichos recursos. Esta delegación de confianza, sin embargo, debe estar sustentada por un conjunto de mecanismos que sean fáciles de usar, accesibles, funcionales y claros para quienes emplean cibertecnologías y que generen la tranquilidad o aporten la estabilidad necesaria para el entorno corporativo y para los particulares.

Según el último informe del Centro Cibernético de la Policía Nacional, al cierre de 2024, Colombia reportó un aumento en denuncias de cibercrimen en un 23% pasando de 63.249 en 2023 a 77.666 en 2024, donde las acciones delictivas más frecuentes son hurto por medios informáticos con 37.409 casos, acceso abusivo a sistema informático con 16.955 y la violación de datos personales con 11.954. Las ciudades con mayor número de casos son Bogotá (23.490), Medellín (6.533) y Cali (4.969) liderando las estadísticas como las más afectadas. Las principales amenazas detectadas son mediante un software malicioso que advierte virus en las computadoras a través de ventanas emergentes, invitando a descargar archivos fraudulentos, esta modalidad se denominada Scareware, también se utilizan eventos falsos, que contienen enlaces maliciosos mediante la modalidad Phishing en Google Calendar y Google Drawings y por último la extorsión por Ransomware, se trata de contactar a las empresas afectadas para negociar la recuperación de la información. (Cámara colombiana de Informática y Telecomunicaciones 2025).

Las cifras anteriores evidencian un incremento exponencial en los ciberataques, lo que sugiere que solo un reducido porcentaje de los usuarios con acceso a Internet es consciente de las amenazas derivadas de la ausencia de control o protección sobre los datos que suministran en distintas plataformas, así como de la falta de verificación frente a la autenticidad de enlaces que se reciben por medio de ventanas emergentes. Esto nos da una idea y evidencia el creciente auge de los delitos informáticos, que pueden suponer que los usuarios entran en contacto con diferentes ataques, especialmente cuando los actores maliciosos conocen que la identifican debilidades o ausencia de medidas de

seguridad, ya que la mayoría de los individuos pueden caer en instalar accesos en su computadora que facilitan el robo de la información.

La mayoría de los informes de seguridad reportan un aumento sostenido en el número de agentes peligrosos, entendidos como aquellas entidades que, sean humanas o automatizadas, aprovechan vulnerabilidades específicas para ejecutar sus ataques. Las razones que se analizan giran, esencialmente, en torno a la facilidad con la que se intercambian herramientas tecnológicas entre los atacantes, lo que evidencia un alto grado de cooperación en la ejecución de actividades maliciosas y plantea un escenario cada vez más complejo para la prevención de delitos informáticos, siendo la preocupación más apremiante los fraudes que permiten el acceso no autorizado a entidades bancarias, el robo de información a través de tarjetas y la eventual suplantación de identidad con fines delictivos más amplios.

En esta guerra contra la amenaza de la seguridad cibernética, es importante enfatizar en la existencia de la gestión básica de la ciberseguridad, las estructuras normativas nacionales e internacionales y controles en la red.

La legislación colombiana, a través de la Ley 1273 de 2009, incorporó al Código Penal una nueva estructura normativa para abordar los delitos informáticos, creando el Título VII BIS bajo la denominación "*De la Protección de la información y de los datos*", dentro del cual se establecen dos capítulos diferenciados, el primero referente a los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, y el segundo dedicado a los atentados informáticos y otras infracciones, previendo penas que pueden alcanzar los 120 meses de prisión y multas de hasta 1.500 salarios mínimos legales mensuales vigentes.

La expedición de esta ley representa una herramienta importante para condenar actividades criminales que afectan especialmente a las pequeñas y medianas empresas, al tipificar una serie de conductas que están en contravía del tratamiento correcto de la información. Esta regulación no solo permite identificar el tipo penal aplicable, sino que también ha contribuido al aumento de las denuncias, en la medida en que se conocen las sanciones previstas. Además, facilita la comprensión del *modus operandi* de los atacantes y resalta la necesidad de implementar mecanismos de control más rigurosos, orientados a garantizar el uso legítimo de los datos y prevenir que tanto organizaciones como individuos incurran en prácticas ilícitas.

Adaptación de medidas de ciberseguridad y protección de datos en las PYMES: Hacia una gestión integral de la información.

La necesidad de que las pymes adopten estrategias sólidas de ciberseguridad, frente a los desafíos previamente expuestos, ha impulsado el desarrollo de diversas herramientas y aplicaciones orientadas a fortalecer la protección de la información. Entre estas soluciones se destacan aquellas que ofrecen funciones específicas para preservar la privacidad y seguridad de los usuarios, como los navegadores con modo anónimo, sistemas de cifrado y plataformas diseñadas para evitar el monitoreo no autorizado; sin embargo, en algunos casos, no puede asumirse que estas herramientas garanticen plenamente el servicio para el cual fueron adquiridas.

Para las pymes, confiar en soluciones tecnológicas que posiblemente no satisfagan los estándares de seguridad exigidos constituye un riesgo relevante. Esta aparente sensación de protección genera vulnerabilidades que pueden conducir a la pérdida o exposición indebida de datos personales, lo cual compromete no solo la privacidad de los titulares, sino también la calidad y continuidad de los servicios ofrecidos. En el ámbito corporativo, este tipo de incidentes se traduce en afectaciones reputacionales y perjuicios económicos significativos, que impactan directamente la sostenibilidad del negocio.

Las características que los usuarios deben evaluar para el proceso de selección de un servicio que garantice y cubra aquellos aspectos importantes como lo son las aplicaciones o herramientas de seguridad y privacidad, deben responder a requisitos básicos como la madurez y estabilidad, así como la implementación de políticas de privacidad claras y fáciles de usar. Por madurez y estabilidad hacemos referencia al cómo reacciona la herramienta ante problemas de seguridad actuales y novedosos, y cómo su comportamiento o desarrollo a lo largo del tiempo para satisfacer las necesidades de seguridad y privacidad, lo que incluye por ejemplo la frecuencia de sus actualizaciones, la rapidez con que se corrigen fallos y la capacidad del proveedor para adaptarse a los cambios en el entorno digital. Adicionalmente, es importante considerar otros dos parámetros al momento de seleccionar este tipo de herramientas. El primero es el nivel de apoyo y respaldo que recibe la herramienta por parte de la comunidad de usuarios (lo que en ocasiones se puede medir mediante el número de descargas). El segundo

corresponde a las auditorías y revisiones realizadas por organismos especializados, firmas reconocidas del sector tecnológico o medios de comunicación especializados en ciberseguridad, así como a las certificaciones, acreditaciones o reconocimientos que haya recibido el software. (Arroyo Guardeño, Gayoso Martínez, y Hernández Encinas 2020).

Es fundamental que las políticas de tratamiento de datos personales implementadas por los desarrolladores y distribuidores de las herramientas sean claras, accesibles y transparentes. Los usuarios deben contar con información suficiente que les permita conocer con precisión qué tipo de datos personales serán recolectados o procesados por la aplicación, con qué frecuencia se realizará dicho acceso y cuál es la finalidad específica que justifica ese tratamiento.

Por otro lado, si los datos del usuario se envían al servidor, es importante saber quién recibirá los datos, el propósito y el contenido de esta transferencia o transmisión de datos y los derechos que el usuario ha eliminado y/o reparado, sobre aquellos datos que se han transferidos. Es indispensable que la política de privacidad de los programadores y distribuidores de software esté completamente recopilada por escrito y posiblemente pueda ser inspeccionada por el usuario. Lo mismo es que los usuarios sean notificados de cualquier cambio en las políticas de privacidad mientras usan la aplicación.

En la etapa de uso de herramientas, resulta esencial evaluar el nivel de complejidad que presentan, es decir, si su manejo está orientado a un público general o, por el contrario, requiere conocimientos técnicos avanzados. La usabilidad se convierte así en un criterio determinante, ya que define en qué medida los usuarios pueden utilizar la herramienta de forma efectiva y satisfactoria. Esta evaluación debe considerar aspectos como la facilidad de instalación, uso cotidiano, configuración y eliminación del software, así como la disponibilidad de información clara y accesible que oriente al usuario en cada uno de estos procesos. La simplicidad y claridad en la experiencia de uso no solo facilitan su adopción, sino que también reducen los riesgos asociados a configuraciones inadecuadas que puedan comprometer la seguridad de los datos personales.

Como herramientas indiscutibles para salvaguardar la privacidad, destacamos las copias de seguridad. Frente a ataques como el ransomware estas permiten recuperar la información comprometida, ya que los datos encriptados ser sustituidos por versiones previamente respaldadas. Este reemplazo o proceso de restauración debe hacerse sin conectarse a Internet para evitar que el respaldo también sea cifrada por el atacante.

Gracias a ello se neutraliza la amenaza de extorsión y el usuario puede iniciar la recuperación de la información sin ceder ante las exigencias del ciberdelincuente. Para garantizar la efectividad de este mecanismo, las copias de seguridad deben realizarse con una frecuencia adecuada, la cual varía según el tipo de usuario. No es lo mismo el volumen de información que generan las pequeñas y medianas empresas, en comparación con el de un usuario particular. Asimismo, teniendo en cuenta la relevancia de los datos y las necesidades específicas de cada caso, resulta recomendable implementar tanto copias locales como remotas. Esta combinación resulta pertinente, ya que los dispositivos físicos son susceptibles a fallos, pérdidas o robos, riesgos que pueden mitigarse mediante servicios de respaldo en la nube o almacenamiento externo seguro.

Actualmente, la mayoría de los sistemas operativos de computadoras y teléfonos móviles pueden masivamente generar las actualizaciones de seguridad de los usuarios y de las funciones, realizan estas tareas muy a menudo. Además, si hay un sistema operativo sin el servicio que proporcione actualizaciones regulares y efectivas, tenemos que descartar su implementación.

Al mismo tiempo, no basta con mantener actualizados los sistemas y corregir errores de seguridad; las pymes deben procurar que estas medidas sean sostenibles y válidas en el largo plazo. Sin embargo, estas acciones, por sí solas, no garantizan completamente la confiabilidad de un sistema frente a ataques cibernéticos, una problemática que, como se ha evidenciado, presenta un crecimiento sostenido en el número de denuncias en Colombia. Esta situación aplica tanto a las herramientas de seguridad (como antivirus, firewalls y sistemas de detección de malware) como al resto de las aplicaciones utilizadas por la organización, ya que cualquier vulnerabilidad en el software puede convertirse en una puerta de entrada para los ciberdelincuentes. Por esta razón, es fundamental implementar sistemas robustos de detección y prevención de amenazas, acompañados de un proceso constante de actualización y revisión del entorno digital.

Propuestas y estrategias para el cumplimiento efectivo del régimen de protección de datos en las PYMES colombianas.

El cumplimiento del régimen de protección de datos en Colombia representa un desafío particular para las PYMES, que suelen operar con recursos limitados y estructuras administrativas reducidas. No obstante, su responsabilidad legal es equivalente a la de grandes empresas, por lo que se hace indispensable adoptar estrategias realistas, escalables y legalmente sólidas. A continuación, se presentan una serie de propuestas orientadas a fortalecer las capacidades internas de estas organizaciones, garantizar el respeto de los derechos de los titulares y reducir los riesgos derivados del tratamiento inadecuado de la información personal.

Diseño e Implementación de Políticas y Procedimientos Internos

La documentación interna constituye el pilar fundamental para un cumplimiento legal efectivo. En este sentido, las PYMES deben formular y divulgar una Política de Tratamiento de Datos Personales (PTDP) que especifique con claridad los tipos de datos recolectados, las finalidades del tratamiento, los derechos de los titulares y los mecanismos para su ejercicio. Además, debe incluir la identificación del responsable del tratamiento y el período de vigencia de las bases de datos (Superintendencia de Sociedades 2023), Esta política debe ser pertinente, eficaz, comprensible, actualizada, operativa y verificable, en armonía con las disposiciones legales vigentes en Colombia.

Resulta fundamental que las empresas también implementen un manual interno de políticas y procedimientos para la recolección, almacenamiento, uso, circulación y supresión de datos personales, así como un manual de seguridad de la información, ya que, como la ha identificado la SIC, la ausencia de estos documentos no solo debilita la gestión interna sino que además constituye una de las causas más frecuentes de sanciones por parte de las autoridades de control (Superintendencia de Industria y Comercio 2021b); y si bien la implementación, no garantiza por sí sola el cumplimiento absoluto del régimen de protección de datos, sí representa una estrategia fundamental dentro del marco del gobierno corporativo. Estos documentos permiten establecer una estructura organizacional clara, con lineamientos precisos y protocolos para la gestión de riesgos y respuesta ante incidentes de seguridad. Como mecanismos de gobierno corporativo, los manuales no solo promueven la transparencia y la rendición de cuentas, sino que también fortalecen la cultura de cumplimiento al interior de la empresa, al facilitar la capacitación del personal, asignar responsabilidades y estandarizar procesos. En el contexto de las

pymes, contar con estas herramientas proporciona una base sólida para la toma de decisiones informadas, mejora la capacidad de respuesta frente a requerimientos regulatorios y contribuye a la sostenibilidad jurídica y reputacional de la organización.

Además, las empresas con activos totales superiores a 100.000 UVT están obligadas a registrar sus bases de datos en el Registro Nacional de Bases de Datos (Decreto 90 de 2018), una herramienta administrada por la Superintendencia de Industria y Comercio que funciona como directorio público y mecanismo de vigilancia institucional, promoviendo la transparencia en el tratamiento de la información personal. Este registro debe mantenerse actualizado anualmente durante el periodo comprendido entre el 2 de enero y el 31 de marzo, y también debe reflejar mensualmente cualquier modificación significativa que ocurra en las bases de datos existentes. En el caso de la creación de nuevas bases de datos, la inscripción debe realizarse dentro de los dos meses siguientes a su conformación, lo que implica que el cumplimiento no solo es una obligación puntual, sino también una tarea continua que exige seguimiento y gestión constante por parte de las organizaciones (Superintendencia de Industria y Comercio, s.f.) Y aunque las microempresas podrían no estar dentro del rango de obligatoriedad por criterios del valor total de activos totales (Bancóldex 2025) muchas pequeñas empresas del sector servicios y comercio sí lo están, lo cual hace aún más relevante que este requisito sea considerado desde una perspectiva estratégica y no meramente formal.

Rol del compliance, la autorregulación y la formación empresarial.

En un contexto empresarial dominada por cambios digitales, globalización y desarrollo sostenible, las pequeñas y medianas empresas (pymes) enfrentan retos constantes es por ello por lo que el rol del compliance, la autorregulación y la formación empresarial abarca grandes aspectos como lo es: la incorporación de procedimientos que asegure el cumplimiento normativo aplicable al sector de cada negocio y sus actividades.

Ante el problema de los ciberataques, incluida la práctica responsable en la gestión de los datos personales de los clientes, el personal y los aliados estratégicos, la implementación de las estrategias que crean valor no debe limitarse en los aspectos productivos o comerciales, sino que también incluye elementos invisibles como la confianza, la reputación y la ética empresarial.

En este sentido, el cumplimiento de los sistemas de protección de datos no solo se considera como una obligación legal, sino también la capacidad de crear un valor

sostenible y de generar una responsabilidad empresarial. Fortalecer la cultura de protección de datos en el sector de las pymes requiere una estrategia integral que articule la conciencia organizacional, el cumplimiento normativo y la eficiencia operativa.

Por ello, se propone un conjunto de estrategias legales y técnicas adaptadas a la realidad. Las pequeñas y medianas empresas (pymes) deben comenzar a identificar flujos de información importantes en sus procesos y evaluar las capacidades de sus colaboradores, su tecnología y la regulación de la protección de datos.

Después de este diagnóstico, pueden fortalecer su infraestructura a través de soluciones disponibles para la seguridad de la red, creando políticas internas en el alcance del procesamiento de datos personales que orienten la recolección, almacenamiento, uso y eliminación de la información, y que sean comunicadas de manera efectiva a clientes, proveedores y empleados.

Otro paso esencial es identificar y clasificar los datos personales administrados, lo que permite implementar medidas de seguridad como el cifrado de archivos, autenticación multifactorial, actualizaciones de software y respaldo de información.

Además, la potencialización de los talentos humanos es la clave, mediante la capacitación del personal, ya que es una buena estrategia de seguridad practicar la conciencia digital, aumenta la cultura organizacional y minimiza los riesgos operativos, asegurando que todos los colaboradores desde la alta dirección hasta los operativos comprendan el valor estratégico y legal de los datos personales y las consecuencias de su mal manejo. Por tal razón las pymes deben designar un responsable de protección de datos, interno o externo, que coordine las acciones de cumplimiento, asesore a la empresa y actúe como enlace ante las autoridades competentes.

De igual forma, es necesario gestionar adecuadamente el consentimiento informado de los titulares, garantizando que toda recolección y tratamiento de datos se realice conforme a los principios de legalidad y transparencia, en concordancia con la norma como la Ley 1581 de 2012 en Colombia.

Las pymes también deben establecer protocolos de respuesta ante incidentes de seguridad, con mecanismos para notificar y mitigar daños en caso de filtraciones o accesos no autorizados. Igualmente, se recomienda integrar la protección de datos en toda la cadena de valor, exigiendo a proveedores tecnológicos y socios contractuales estándares similares de cumplimiento, mediante cláusulas contractuales y evaluaciones

periódicas. Para asegurar la mejora continua, es clave realizar auditorías internas y evaluaciones de riesgo, que identifiquen vulnerabilidades y permitan ajustar las prácticas a los cambios regulatorios y tecnológicos.

Por otro lado, la cooperación con entidades externas es muy importante para el desarrollo de la empresa a través de asesores legales y proveedores de tecnología, que pueden convertirse en alianzas estratégicas que aumentan la capacidad de cumplir con los requisitos e introducir a las pequeñas y medianas empresas sobre el valor de la innovación y los costos de desarrollo tecnológico.

Articular estas acciones dentro de la cadena de valor permite a las pymes optimizar recursos, establecer alianzas estratégicas y posicionarse como actores confiables en sus respectivos sectores, mejorar el cumplimiento normativo en protección de datos no debe verse como un costo adicional, sino como una inversión estratégica que potencia la sostenibilidad, la eficiencia operativa y la resiliencia de las pymes en el nuevo ecosistema empresarial digital.

Finalmente, es necesario mejorar la cultura organizacional basada en la ética digital y la responsabilidad, donde la protección de los datos personales sea percibida no solo como una obligación legal, sino como un compromiso con la confianza del cliente y la sostenibilidad del negocio.

Conclusiones

La protección de datos personales en las pymes colombianas no puede entenderse únicamente como un imperativo legal derivado de la Ley 1581 de 2012 y normas complementarias, sino como un componente estratégico de la gestión empresarial en la era digital. Este estudio permite concluir que la normativa vigente, si bien ofrece un marco robusto de garantías en torno al derecho al habeas data, enfrenta serios desafíos de aplicabilidad en organizaciones con recursos limitados, que en muchos casos carecen de infraestructura tecnológica, capacitación especializada y cultura de cumplimiento. Esta brecha entre norma y práctica se traduce en un escenario de riesgo jurídico, operativo y reputacional que compromete no solo la sostenibilidad de las pymes, sino también la confianza en el ecosistema digital colombiano.

Los riesgos analizados evidencian que la ausencia de políticas internas de protección de datos, la deficiente gestión del consentimiento, la falta de planes de

respuesta a incidentes y la carencia de medidas mínimas de seguridad tecnológica constituyen las principales fuentes de vulnerabilidad. Frente a ello, resulta indispensable que las pymes asuman la ciberseguridad no como un gasto accesorio, sino como una inversión esencial para la continuidad del negocio, pues la gestión responsable de la información exige pasar de un modelo reactivo, centrado en el cumplimiento formal de la ley, hacia un enfoque preventivo y estratégico, en el cual la protección de datos se articule con la planeación corporativa, la innovación tecnológica y la resiliencia empresarial. Su implementación debe estar acompañada de programas de formación y concienciación en todos los niveles jerárquicos, pues el factor humano continúa siendo el eslabón más vulnerable en materia de ciberseguridad.

El análisis realizado demuestra que fortalecer la gobernanza corporativa en torno a la protección de datos no solo mitiga sanciones y responsabilidades legales, sino que constituye un factor de competitividad y sostenibilidad en el mercado. La protección de la información debe ser vista como un activo intangible que genera valor, incrementa la confianza de clientes y aliados estratégicos, y posiciona a las pymes como actores confiables en la economía digital, de esta manera, la normativa en materia de privacidad y seguridad de la información se convierte en una herramienta no restrictiva, sino habilitante, que impulsa a las organizaciones hacia prácticas más responsables, transparentes y sostenibles.

En conclusión, el reto para las pymes en Colombia consiste en superar la visión reduccionista del cumplimiento normativo como carga administrativa y transitar hacia un modelo de gestión integral de la información, en el que legislación, políticas internas, ciberseguridad y compliance se articulen de manera coherente. Solo así podrán garantizar el respeto de los derechos fundamentales de los titulares, responder eficazmente a los riesgos del entorno digital y consolidar su papel como motor del desarrollo económico y social en un escenario cada vez más interconectado y globalizado.

Bibliografía

Aguilar Antonio, Juan Manuel. 2021. «Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior». *Estudios internacionales: Revista del Instituto de Estudios Internacionales de la Universidad de Chile*, 2021.

Alayón Rodríguez, Edgar Eduardo. 2021. «Tecnologías disruptivas en la transformación digital de las organizaciones en la industria 4.0. ». https://doi.org/10.29394/Scientific.issn.2542-2987.2021.6.21.14.267-281.

Ámbito Jurídico. 2021. «Una vez cumplida la finalidad, responsable y/o encargado del tratamiento de datos personales deberá suprimirlos». Legis, febrero 16. https://www.ambitojuridico.com/noticias/constitucional/una-vez-cumplida-la-finalidad-responsable-yo-encargado-del-tratamiento-de.

Arroyo Guardeño, David, Víctor Gayoso Martínez, y Luis Hernández Encinas. 2020. *Ciberseguridad*. CSIC.

Auto Interlocutorio, M.P. Fernando Alberto Castro Caballero, Nº 37145 (Corte Suprema de Justicia - Sala de Casación Penal 13 de septiembre de 2011). https://vlex.com.co/vid/auto-interlocutorio-corte-suprema-874032789.

Bancoldex. 2025. «Clasificación de Empresas en Colombia». https://www.bancoldex.com/es/sobre-bancoldex/quienes-somos/clasificacion-de-empresas-en-colombia.

Cabrera Peña, Karen Isabel, y Yamile Andrea Montenegro Jaramillo. 2022. «Protección de Datos Personales en el Marco de la COVID-19: el Caso de CoronApp en Colombia». *The Law, State and Telecommunications Review*, 2022. https://www.researchgate.net/publication/361265804 Protección de.

Cámara Colombiana de Informática y Telecomunicaciones. 2025a. «Balance de Ciberseguridad 2024: Desafíos y prevención para un entorno digital seguro». marzo 28. https://www.ccit.org.co/noticias/balance-de-ciberseguridad-2024-desafios-y-prevencion-para-un-entorno-digital-seguro.

———. 2025b. «Estado de la ciberseguridad y la Inteligencia Artificial en Colombia». https://www.ccit.org.co/estudios/estado-de-la-ciberseguridad-y-la-inteligencia-artificial-en-colombia/.

Cámara de Comercio de Bogotá. 2024. «Evolución de las empresas activas entre 2023 y 2024 por tamaño». https://www.ccb.org.co/informacion-especializada/observatorio/dinamica-empresarial/empresas-activas/tamano.

Castillo Díaz, Felipe Andrés. 2020. «Contrato de seguro para riesgos cibernéticos: análisis de la cobertura de responsabilidad civil por violación de datos personales». Proyecto de grado, Universidad Externado de Colombia. https://bdigital.uexternado.edu.co/server/api/core/bitstreams/4d280fac-a565-45ff-9c57-e6c806305890/content.

Constitución Política de Colombia (1991). http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html.

Decreto 90 de 2018, Diario Oficial No. 50.480 (2018). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=85039.

Decreto 1377 de 2013, Diario Oficial 48834 (2013). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646.

Editorial La República S.A.S. 2025. «La SIC sancionó a Risks International por infracción de protección de datos personales». Diario La República, agosto 6. https://www.larepublica.co/empresas/la-sic-sanciono-a-risks-international-por-infraccion-de-proteccion-de-datos-personales-4197313.

Escuela de Privacidad. 2023. «¿Por qué motivos sancionan a las empresas en materia de protección de datos personales?» https://escueladeprivacidad.co/wp-content/uploads/2023/08/Estudio-Sanciones-2022-EP-VF.pdf.

Flórez Rojas, María Lorena, y Angélica María Camelo Pimienta. 2023. «Tecnologías de reconocimiento facial en Colombia: Análisis comparativo en relación con la protección de datos». *Iux et Praxis*, 2023. https://dialnet-unirioja-es.ez.urosario.edu.co/servlet/articulo?codigo=8975285.

Gabriunas, Iliana Páez, Mauricio Sanabria Rangel, Valérie Gauthier Umaña, Rafael Alberto Méndez Romero, y Liliana Rivera Virgüez. 2022. *Transformación digital en las organizaciones*. Universidad del Rosario. https://dialnet.unirioja.es/servlet/libro?codigo=900317.

González Patiño, Juan Sebastián, y María Claudia Llanes Valenzuela. 2024. «Una mirada a las mipymes en Colombia ». BBVA Research. https://www.bbvaresearch.com/wp-content/uploads/2024/02/202401_MiPymes_Colombia-1.pdf.

Impacto TIC. 2024. *Ciberseguridad en Colombia: Estrategias y Desafíos Actuales*. 3 de junio de 2024. https://impactotic.co/ciber-seguridad/ciberseguridad-en-colombia-riesgos-a-los-que-se-enfrenta-el-pais/.

Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). 2012. «Guía Técnica GTC-ISO/IEC colombiana 27035». diciembre 21.

Jiménez Almeira, Gabriel Andrés, y David Enrique López. 2023. «Ciberseguridad y Seguridad Integral: un análisis reflexivo sobre el avance normativo en Colombia». *RISTI: Revista Ibérica de Sistemas e Tecnologias de Informação,* 2023. https://dialnet-unirioja-es.ez.urosario.edu.co/servlet/articulo?codigo=10050181.

Ley 1266 de 2008, Diario Oficial No. 47.220 (2008). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488.

Ley 1273 de 2009, Diario Oficial 47.223 (2009). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492.

Ley 1581 de 2012, Diario Oficial No. 48.587 (2012). http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html.

Ministerio de Tecnologías de la Información y las Comunicaciones. 2023. «Ministro TIC presenta la estrategia de cuatro puntos para hacer de Colombia una potencia en Ciberseguridad - Ministro TIC presenta la estrategia de cuatro puntos para hacer de Colombia una potencia en Ciberseguridad». julio 19. https://www.mintic.gov.co/portal/715/w3-article-276939.html.

Osuna Carreño, Alejandro José. 2024. *El derecho fundamental a la protección de datos personales en Colombia*. Bogotá, Colombia: Grupo Editorial Ibañez.

Prieto Castellanos, Bayron. 2019. «Ciberdelito: Buscando rastros digitales.» En *Ciberespacio, ciberseguridad y ciberjusticia en la era digital. El futuro de la abogacía.* , 179-210. Bogotá: Grupo Editorial Ibañez.

Ramírez Pascual, Basilio. 2023. *La ciberseguridad en la era de la Inteligencia Artificial: dilemas y retos empresariales*. La Ley Soluciones Legales S.A.

Sentencia C-748/11, M.P. Jorge Ignacio Pretelt Chaljub, Expediente PE-032 (Corte Constitucional 10 de junio de 2011). https://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm.

Sentencia SC10297-2014, M.P. Ariel Salazar Ramírez (Corte Suprema de Justicia - Sala de Casación Civil 6 de marzo de 2014).

Sentencia T-238/18. M.P. Gloria Stella Ortiz Delgado, Expediente T-6.467.142 (Corte Constitucional 26 de junio de 2018). https://www.corteconstitucional.gov.co/relatoria/2018/t-238-18.htm.

Sentencia T-307/99. M.P. Eduardo Cifuentes Muñoz, Expediente T-187958 (Corte Constitucional 5 de mayo de 1999). https://www.corteconstitucional.gov.co/relatoria/1999/t-307-99.htm.

Sentencia T-444/14, M.P. María Victoria Calle Correa, Expediente T-4236830 (Corte Constitucional 7 de abril de 2014). https://www.corteconstitucional.gov.co/relatoria/2014/t-444-14.htm.

Superintendencia de Industria y Comercio. 2014. «Concepto 18039 de 2014». https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=57327&dt=S.

———. 2021a. «Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability). ». https://issuu.com/quioscosic/docs/guia_accountability_26_p__g.

———. 2021b. «Sanciones por incumplimiento del régimen de protección de datos personales». https://www.sic.gov.co/sanciones-proteccion-datos-personales-2021.

———. 2022. «Circular Externa No. 006 del 2022 | Sede Electronica». https://sedeelectronica.sic.gov.co/transparencia/normativa/circular-externa-no-006-del-2022.

———. 2025. «La Superintendencia de Industria y Comercio confirmó sanción a Risk International S.A.S. por infracción al régimen de protección de datos personales.» junio 8. https://sedeelectronica.sic.gov.co/comunicado/la-superintendencia-de-industria-y-comercio-confirmo-sancion-risks-international-sas-por-infraccion-al-regimen-de-proteccion-de-datos .

———. s. f. «Preguntas frecuentes RNBD». https://www.sic.gov.co/preguntas-frecuentes-rnbd.

Superintendencia de Sociedades. 2023. «Manual Interno de Políticas y Procedimientos para el Tratamiento y Protección de los Datos Personales». septiembre 20. https://www.supersociedades.gov.co/documents/107391/3463418/GC-M-003_ManualTratamientoDatosPersonales.pdf.

Terranova Security. s. f. «130 Cybersecurity Statistics: 2024 Trends and Data». Human Risk Management. https://www.terranovasecurity.com/blog/cyber-security-statistics.