S+S INSIGHTS

Santamarina + Steta

PROTECCIÓN DE DATOS PERSONALES Y CIBERSEGURIDAD EN LA MIGRACIÓN DIGITAL EMPRESARIAL

La ciberseguridad no debe verse como un gasto, sino como una inversión estratégica que protege los activos digitales, la reputación empresarial y la confianza de clientes y socios.

"Existe un marco normativo bastante robusto. Cualquier empresa que maneje datos personales —y hoy prácticamente todas lo hacen— debe implementar medidas de seguridad físicas, administrativas y técnicas adecuadas. No hacerlo, incluso por desconocimiento, puede acarrear consecuencias legales y reputacionales muy graves"

La transformación digital ha dejado de ser una tendencia para convertirse en una necesidad estructural en la operación de las empresas mexicanas. Tras la pandemia, miles de organizaciones aceleraron su paso al comercio electrónico, plataformas en la nube y modelos de negocio híbridos. Esta evolución ha traído eficiencia, nuevos canales de venta y expansión internacional. Sin embargo, también ha generado desafíos significativos: entre ellos, la urgente necesidad de garantizar la protección de los datos personales y la implementación de mecanismos efectivos de ciberseguridad.

En un contexto donde la información es uno de los activos más valiosos —tanto para las empresas como para los consumidores—, protegerla no solo es una obligación legal, sino una estrategia empresarial crítica. Según Cybersecurity Ventures, para 2025 el costo del ciberdelito a nivel mundial alcanzará los 10.5 billones de dólares anuales, una cifra alarmante si se compara con los 3 billones que representaba en 2015. Estos datos confirman que los riesgos digitales crecen a un ritmo vertiginoso y que ninguna organización está exenta de sufrir una filtración o ataque cibernético.

El costo del ciberdelito en México es cada vez más alarmante y representa una amenaza tangible para empresas, gobiernos y ciudadanos. Según el más reciente informe de la firma Statista Market Insights, el costo estimado del ciberdelito en México alcanzó los 9 mil millones de dólares en 2024, ubicando al país entre los más afectados de América Latina.

Paola Morales, Socia responsable de las áreas de telecomunicaciones, medios y tecnología (TMT), comercio electrónico, privacidad y protección de datos, de Santamarina + Steta, destacó que aún persiste entre muchas empresas la percepción errónea de que el entorno digital está poco regulado o que las normativas en materia de ciberseguridad no son vinculantes en México. "Existe un marco normativo bastante robusto. Cualquier empresa que maneje datos personales —y hoy prácticamente todas lo hacen— debe implementar medidas de seguridad físicas, administrativas y técnicas adecuadas. No hacerlo, incluso por desconocimiento, puede acarrear consecuencias legales y reputacionales muy graves", explicó.

Y es que, en México, la Ley Federal de Protección de Datos Personales en Posesión

de los Particulares (LFPDPPP) establece lineamientos claros para el tratamiento, resguardo y transferencia de datos personales. A esto se suma la Ley de Firma Electrónica Avanzada, la cual refuerza la validez y seguridad de los procesos digitales. Además, existen normas técnicas y criterios emitidos por autoridades como el extinto INAI, ahora sustituido por la Secretaría de Anticorrupción y Buen Gobierno, que a partir de 2025 se convierte en la nueva entidad encargada de la supervisión y sanción en materia de protección de datos personales.

Esta Secretaría tendrá un papel clave, como lo es: vigilar el cumplimiento de la legislación, recibir quejas y denuncias, e imponer sanciones cuando se detecten omisiones, negligencias o vulneraciones a los derechos de los titulares de datos.

RETOS Y ERRORES COMUNES EN EL ENTORNO EMPRESARIAL

La socia indicó que una de las principales barreras que enfrentan las empresas al migrar al entorno digital es el desconocimiento de sus obligaciones legales. Muchos empresarios aún consideran que en internet o en el comercio electrónico no hay reglas claras, lo cual es incorrecto. "Las leyes aplican tanto en el mundo físico como en el digital. No es que sea tierra de nadie. Las empresas deben cumplir con avisos de privacidad, políticas de tratamiento de datos personales, medidas de seguridad informática y restricciones sectoriales cuando corresponda", agregó Morales.

De hecho, resaltó como la norma mexicana en materia de comercio electrónico, aunque no es oficial, ha sido considerada obligatoria por la Procuraduría Federal del Consumidor (Profeco), lo que amplía aún más el espectro normativo para quienes venden o prestan servicios a través de plataformas digitales. Por ejemplo, se establece que para el tratamiento de datos personales de los usuarios y consumidores en la generación de perfiles, el análisis de comportamiento en línea, fines mercadotécnicos, publicitarios o de prospección comercial, se deberá contar con el consentimiento del usuario o consumidor, para lo cual se deberá poner a su disposición un mecanismo que permita solicitarlo previo al uso de los datos personales con esos fines independientemente de la puesta a disposición del Aviso de Privacidad correspondiente.

Además, sectores estratégicos como el financiero, farmacéutico, hospitalario o asegurador, que manejan datos personales financieros y/ o sensibles, enfrentan exigencias aún mayores. Deben implementar estándares internacionales, como las certificaciones ISO en ciberseguridad, y contar con controles internos mucho más estrictos para proteger la integridad, confidencialidad y disponibilidad de la información.

VULNERACIONES Y SUS CONSECUENCIAS

Las filtraciones de datos ya no son eventos aislados. Empresas públicas y privadas en México y el mundo han enfrentado incidentes que han puesto en evidencia la fragilidad de sus sistemas. Las consecuencias pueden ir desde sanciones económicas hasta la pérdida de la confianza de los usuarios y clientes, lo que a la larga puede costar más que cualquier multa.

"Muchas organizaciones creen que no son responsables si fueron atacadas por terceros, pero la ley es clara: si no se adoptaron medidas adecuadas de prevención, existe responsabilidad legal", indicó Morales. Y esas medidas no solo incluyen tener un antivirus actualizado o usar contraseñas fuertes, sino también una segmentación adecuada del acceso a los datos, auditorías internas, políticas de respuesta ante incidentes y capacitación continua del personal.

En ese sentido, las multas por incumplimiento de la LFPDPPP pueden alcanzar hasta 36 millones de pesos, dependiendo del tipo de infracción. Pero más allá del aspecto económico, el impacto reputacional puede ser irreversible. "Hoy en día, el usuario promedio valora más la privacidad de su información. Un escándalo por mal manejo de datos puede hundir una operación comercial, reducir el valor de marca o incluso cancelar oportunidades de inversión", sostuvo Morales.

INTELIGENCIA ARTIFICIAL Y NUEVAS TECNOLOGÍAS ¿SIN REGULACIÓN?

Asimismo, con el auge de la inteligencia artificial (IA) se ha introducido una nueva capa de complejidad legal. Si bien en México aún no existe una ley específica que regule esta tecnología, ya hay iniciativas en discusión en el Congreso y se anticipa que en los próximos años se adopte un modelo similar al europeo: una regulación basada en el nivel de riesgo que representa la IA para los derechos de las personas.

Por ahora, las empresas que utilizan algoritmos, procesamiento automatizado de datos o asistentes virtuales deben seguir rigiéndose por las leyes de propiedad intelectual, derechos de autor, protección de datos y protección al consumidor. "El hecho de que una tecnología sea nueva no la exime de regulación. Las leyes actuales siguen aplicando y deben ser observadas con el mismo rigor", puntualizó la experta.

Esto implica, por ejemplo, que si una herramienta de IA trata datos personales, debe respetar los principios de legalidad, consentimiento, finalidad, proporcionalidad y seguridad. También se debe garantizar la transparencia en los procesos automatizados y ofrecer mecanismos para que los usuarios puedan ejercer sus derechos.

DE LA CULTURA DE PREVENCIÓN A LA RESPONSABILIDAD COMPARTIDA

Uno de los mensajes más importantes que subrayó Morales es la necesidad de cambiar la mentalidad reactiva por una cultura de prevención y cumplimiento proactivo. En otras palabras, no basta con reaccionar ante un incidente de ciberseguridad; es indispensable anticiparse a los riesgos. Para ello, recomienda que las empresas construyan un plan de trabajo jurídico y tecnológico, con el acompañamiento de especialistas en derecho digital, desde la concepción misma del proyecto o plataforma tecnológica.

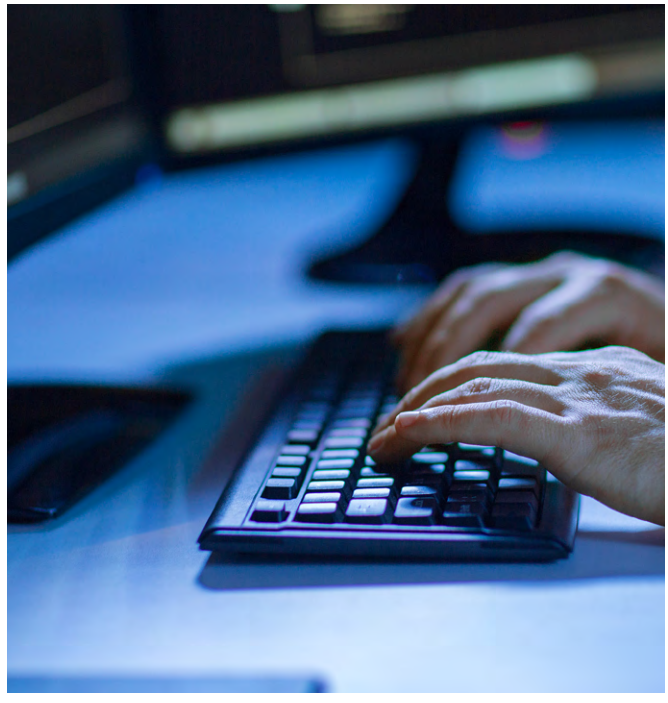
Parte de este enfoque preventivo implica implementar políticas internas claras, segmentar el acceso a la información según funciones específicas, establecer protocolos de seguridad y realizar auditorías periódicas. Por ejemplo, no todo el personal debe tener acceso a todos los datos. Recursos humanos requiere información médica o personal, pero no necesariamente el área comercial o financiera. La segmentación y el principio de mínima intervención deben regir la operación digital.

Además, la ley exige que el personal reciba capacitación continua en protección de datos y ciberseguridad, ya que solo con conocimiento actualizado es posible cumplir eficazmente con la normativa y adaptarse a los constantes cambios en el entorno digital. Esta obligación no debe verse únicamente como un requisito legal, sino como una inversión estratégica que fortalece la cultura organizacional en torno a la seguridad de la información. El personal capacitado puede identificar riesgos con mayor rapidez, responder adecuadamente ante incidentes y prevenir vulnerabilidades que podrían poner en peligro datos personales, incluyendo los sensibles. En un contexto donde las amenazas cibernéticas evolucionan de manera vertiginosa y donde los marcos regulatorios se actualizan para hacer frente a nuevos desafíos, la formación continua se vuelve un elemento clave para garantizar el cumplimiento normativo y la protección de los activos digitales. Además, promueve la confianza tanto de clientes como de socios comerciales, que valoran el compromiso real con la seguridad.

¿HACIA DÓNDE VAMOS?

Ante todo este panorama, la Socia de Santamariana + Steta destacó como la reforma de 2025 ha dejado claro que la dirección que toma el país en materia de protección de datos personales es hacia una mayor rigurosidad normativa y una vigilancia más estricta. Se espera que en un futuro cercano se emitan nuevas disposiciones reglamentarias que muy probablemente detallarán las medidas de seguridad que deben adoptar las organizaciones, además de actualizar las existentes.

También se anticipa que surjan nuevos actores en el ecosistema, como asegurado-



ras especializadas en ciberseguridad, las cuales exigirán que las empresas cuenten con marcos de gobernanza internos sólidos para poder acceder a coberturas viables. De lo contrario, los costos de aseguramiento podrían volverse prohibitivos.

Desde la óptica legal y estratégica, la migración digital empresarial ya no puede desligarse de la responsabilidad legal y ética. La protección de datos y la ciberseguridad son hoy factores fundamentales para la sostenibilidad y competitividad en el mercado.

"La ciberseguridad no debe verse como un gasto, sino como una inversión que protege el negocio, la reputación y la confianza del cliente", concluyó Paola Morales.

En la economía digital del siglo XXI, los datos se han convertido en uno de los activos más valiosos para las empresas, comparables incluso con bienes tangibles como infraestructura o capital financiero. La información personal, financiera y operativa que circula en los entornos digitales representa un recurso estratégico que puede impulsar el crecimiento, la innovación y la competitividad. Sin embargo, ignorar las obligaciones legales y éticas en torno a su recolección, almacenamiento, uso y en general, a su tratamiento, puede derivar en consecuencias graves; desde sanciones económicas y pérdida de reputación hasta la desconfianza de los consumidores. En este contexto, integrar desde el inicio la ciberseguridad y la protección de datos personales como pilares fundamentales de la estrategia empresarial no es una opción, sino una necesidad.

"LA CIBERSEGURIDAD
NO DEBE VERSE COMO UN GASTO,
SINO COMO UNA INVERSIÓN
QUE PROTEGE EL NEGOCIO,
LA REPUTACIÓN Y
LA CONFIANZA DEL CLIENTE"

Paola Morales V.
Socia
pmorales@s-s.mx