



Edición 2025

Encuesta Regional sobre la Gestión de Riesgos y Analítica de Datos

**Impulsando decisiones inteligentes:
personas, procesos y tecnología hacia una
transformación financiera segura**





La Encuesta Regional sobre la Gestión de Riesgos y Analítica de Datos (2025) es una iniciativa conjunta entre PwC Interaméricas y la Federación Latinoamericana de Bancos (FELABAN) en la cual se revela que la gestión de riesgos evoluciona hacia un enfoque predictivo, integrando tecnología, cultura y vigilancia externa.

La Encuesta Regional sobre la Gestión de Riesgos y Analítica de Datos (2025) es una iniciativa conjunta entre PwC Interaméricas y la Federación Latinoamericana de Bancos (FELABAN) en la cual se revela que la gestión de riesgos evoluciona hacia un enfoque predictivo, integrando tecnología, cultura y vigilancia externa. La transparencia y participación interdisciplinaria se vuelven pilares clave, desde lo estratégico hasta lo operativo. La capacitación continua y la atención a riesgos no tradicionales fortalecen la resiliencia organizacional.

Mientras que, la adopción ética de tecnologías de vanguardia y la gestión de terceros consolidan una arquitectura robusta y adaptable con visión de futuro. Más de 95 líderes financieros de 17 países de América Latina y El Caribe aportaron sus puntos de vista en nuestro estudio realizado entre Agosto y Septiembre de 2025.



Las instituciones financieras en América Latina deben avanzar hacia modelos predictivos en gestión de riesgos, impulsados por la analítica avanzada. Este proceso exige modernización tecnológica y el desarrollo de nuevas capacidades en los equipos. Para enfrentar los retos actuales con eficacia, es crucial fortalecer la cultura interna y promover una gestión transparente con el patrocinio de la Alta Gerencia.

Bismark Rodríguez

Socio Líder Regional de Consultoría
PwC Interaméricas



Desde mi rol como Secretario General de un gremio bancario regional, resulta indispensable contar con evidencia sólida que permita comprender cómo están respondiendo los bancos de América Latina a estos desafíos. En este sentido, la Encuesta Regional sobre Gestión de Riesgos y Analítica de Datos, realizada a cerca de 100 CROs y liderada por FELABAN y PwC Interaméricas, constituye un ejercicio oportuno para recoger la visión de quienes tienen la responsabilidad de anticipar y gestionar los riesgos que definen la resiliencia del sector y traducir la incertidumbre en rentabilidad y eficiencia operativa.

En un entorno de creciente complejidad, la gestión de riesgos en la banca latinoamericana se ha consolidado como un pilar estratégico más allá del cumplimiento. Aunque existen avances, persisten brechas operativas y tecnológicas, especialmente en bancos pequeños, en un contexto regulatorio más exigente. La transformación digital amplía oportunidades y riesgos, haciendo de la ciberseguridad una prioridad. Con cooperación, liderazgo y foco en talento, tecnología y ética, la banca puede seguir siendo un factor clave de estabilidad e inclusión financiera.

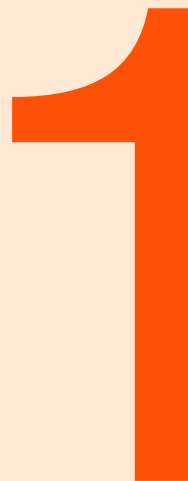
Giorgio Trettenero Castro

Secretario General

Federación Latinoamericana de Bancos (FELABAN)

Contenido

1	Resumen Ejecutivo	06
2	Introducción	08
3	Estratificación demográfica y participación	10
4	Principales prioridades	13
5	Identificación y actualización de riesgos	26
6	Gestión y priorización de riesgos	39
7	Riesgos tecnológicos y de terceros	44
8	Ruta hacia la transformación	50



Resumen ejecutivo



En el cambiante entorno económico de América Latina, los bancos enfrentan una transformación urgente en la gestión de riesgos. Esta debe pasar de ser reactiva y normativa a ser predictiva, dinámica y alineada con la estrategia organizacional. Según la **Encuesta Regional sobre la Gestión de Riesgos y Analítica de Datos de PwC Interaméricas y FELABAN (2025)**, más de 95 líderes financieros de 17 países coinciden en que la resiliencia se construye con visión, cultura y tecnología.

La analítica de datos es clave en esta evolución, permitiendo anticipar amenazas y tomar decisiones informadas. Sin embargo, plantea retos éticos que deben abordarse con responsabilidad. La cultura organizacional también es esencial: la gestión de riesgos debe ser transversal y participativa, involucrando a todos los niveles.

La capacitación continua es vital ante riesgos emergentes como sostenibilidad, reputación y conducta. Además, los bancos deben estar atentos al entorno regulatorio y a las expectativas del mercado. Los riesgos digitales y cibernéticos se vuelven centrales, exigiendo arquitecturas tecnológicas resilientes y estrategias de ciberseguridad que protejan la confianza del cliente.

La gestión de terceros requiere marcos claros para mitigar riesgos en la cadena de valor. La adopción de tecnologías como la Inteligencia Artificial (IA) debe hacerse con visión ética y políticas responsables. En este nuevo paradigma, integrar tecnología, cultura y estrategia será clave para que los bancos prosperen. La analítica de datos se convierte en un motor de transformación organizacional.

Por otro lado, en el panorama bancario latinoamericano, los informes de resultados están experimentando un cambio estructural: la atención se desplaza progresivamente de los riesgos financieros tradicionales hacia los riesgos no financieros (operacionales, tecnológicos, de cumplimiento, de ciberseguridad, de conducta, ambientales, entre otros). Esta inclinación no es casual ni superficial; responde a cambios vertiginosos en la forma en que las instituciones operan, se conectan, generan valor y enfrentan el escrutinio regulatorio. Por esta razón, el presente informe también subraya los hallazgos en los cuales la banca reconoce que los riesgos no financieros carecen de métricas estandarizadas, datos históricos robustos y modelos predictivos sólidos, lo que dificulta su evaluación sistemática.

2

Introducción

La transformación del sector financiero latinoamericano hacia prácticas sostenibles, inclusivas y resilientes enfrenta un gran obstáculo: la falta de conocimiento sistematizado sobre cómo se están adoptando estas prácticas. Esta carencia impide evaluar el progreso regional, identificar buenas prácticas y limita la competitividad frente a un contexto global donde la sostenibilidad es clave.

La ausencia de datos comparables dificulta la coordinación entre bancos, fintechs, reguladores y organismos multilaterales, lo que afecta el diseño de políticas públicas y marcos normativos adecuados. Esta barrera entre regulación y práctica ralentiza la evolución hacia estándares internacionales y limita la capacidad de anticipar riesgos y oportunidades estratégicas. Sin información confiable, se genera incertidumbre regulatoria que frena la innovación y la inversión, además de dificultar la transparencia y la rendición de cuentas.

También se obstaculiza la cooperación internacional, ya que los organismos multilaterales carecen de indicadores comunes para comparar avances y establecer metas regionales. La solución requiere una acción coordinada: recolección y análisis de datos con metodologías estandarizadas, creación de observatorios financieros, alianzas público-privadas y fortalecimiento institucional.

Cerrar esta brecha permitirá mejorar la toma de decisiones y acelerar la transformación del sector hacia un modelo más justo, transparente y alineado con las necesidades sociales. La sistematización del conocimiento es clave para liberar el potencial de innovación y desarrollo en la región.

Objetivo General	• La encuesta busca recopilar y analizar información sobre la gestión de riesgos y el uso de analítica de datos en entidades financieras públicas y privadas de América Latina. Se pretende identificar tendencias, niveles de madurez y capacidades institucionales para diseñar estrategias colaborativas, fortalecer capacidades y desarrollar políticas más efectivas.
Alcance	• Está dirigida a instituciones financieras con presencia en los 17 países miembros de FELABAN, sin importar el tamaño o alcance de sus operaciones.
Metodología	• El estudio se estructuró en cuatro fases: preparación, aplicación, interpretación y reporte. Este enfoque combinó analítica avanzada con inteligencia organizacional, convirtiendo el estudio en una herramienta estratégica para impulsar innovación y resiliencia. El levantamiento de datos se realizó del 25 de agosto al 12 de septiembre de 2025.

3

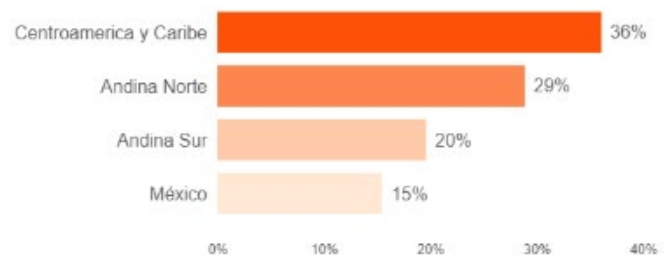
Estratificación
demográfica y
participación

El perfil institucional de la muestra revela una concentración en bancos privados (91%), lo que sugiere una visión del sector financiero dominada por lógicas de mercado y competencia. La escasa representación de entidades públicas y otras formas organizativas (9%) limita la diversidad de perspectivas en la gestión de riesgos, inclusión financiera y sostenibilidad.

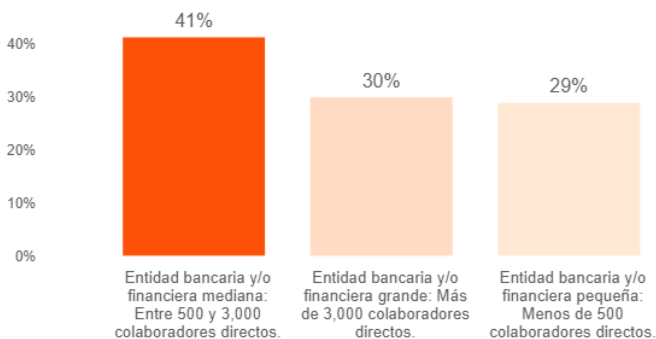
En términos de la cantidad de colaboradores, las instituciones de tamaño medio lideran con un 41%, seguidas por una distribución relativamente equilibrada entre grandes (30%) y pequeñas (29%). Esta configuración sugiere un ecosistema financiero con una base laboral significativa en estructuras intermedias, lo que puede facilitar la agilidad operativa, pero también requerir estrategias específicas de desarrollo de talento y liderazgo. La diversidad de tamaños implica necesidades diferenciadas en cuanto a gestión de riesgos, digitalización y adaptación a nuevas normativas.

Geográficamente, la mayor representación se concentra en Centroamérica y el Caribe (36%) y la región Andina Norte (29%), mientras que Andina Sur (20%) y México (15%) muestran una participación más limitada. Esta distribución evidencia una oportunidad para fortalecer la integración regional y el intercambio de buenas prácticas, especialmente en zonas con menor representación. Además, el predominio de operaciones locales (63%) frente a las regionales (21%) y globales (9%) refleja un ecosistema financiero aún centrado en dinámicas nacionales, con retos importantes en términos de internacionalización, escalabilidad y competitividad global.

Distribución por Regiones

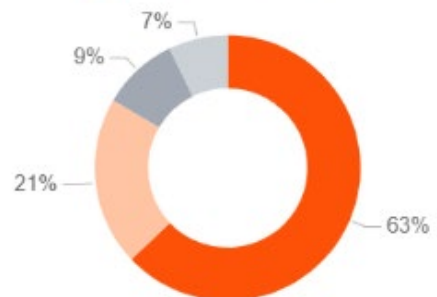


Distribución por Número de Colaboradores



Distribución por Alcance Territorial

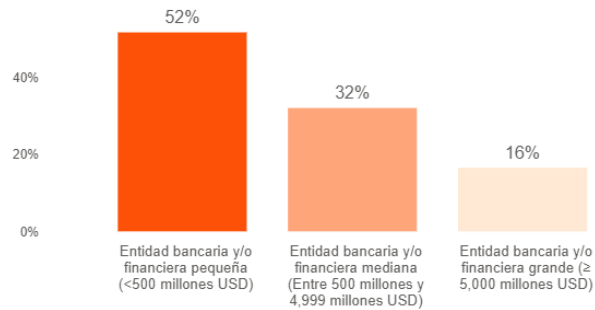
Alcance territorial ● Local ● Regional ● Global ● Latinoamericano



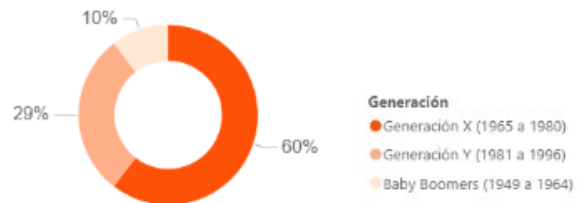
Finalmente, el perfil demográfico muestra una clara dominancia de la Generación X (60%) y una marcada concentración masculina (71% frente a 29% femenina), lo que configura un ecosistema maduro, pero con desafíos evidentes en términos de diversidad e inclusión. Esta composición plantea la necesidad de impulsar políticas activas para fomentar la equidad de género, la participación de nuevas generaciones y la renovación del liderazgo. En conjunto, estos datos configuran un panorama financiero que, si bien cuenta con fortalezas estructurales, enfrenta retos estratégicos en internacionalización, diversidad, innovación y sostenibilidad.

Además, el predominio de instituciones de menor patrimonio (52%) frente a las grandes (16%) plantea desafíos en términos de capacidad operativa, inversión tecnológica y cumplimiento regulatorio, especialmente en un entorno de riesgos emergentes y creciente complejidad.

Distribución por Patrimonio



Distribución por Generaciones



4

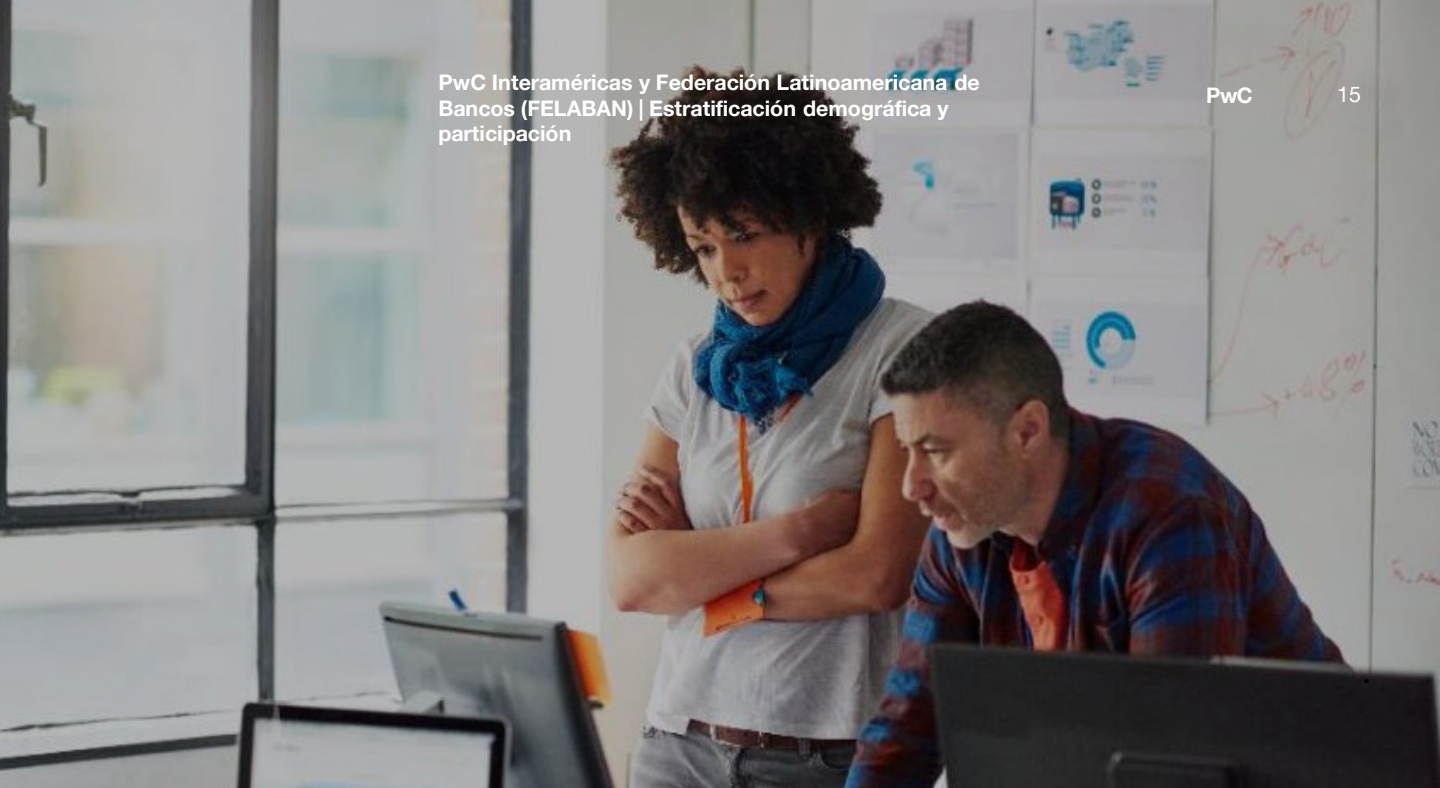
Principales
prioridades

La tecnología está reconfigurando la gestión de riesgos hacia un enfoque más estratégico y menos operativo

Principales prioridades

La tecnología está transformando la gestión de riesgos en el sector financiero, dado que no se trata solo de automatizar procesos, sino de anticipar escenarios complejos e interconectados. En este sentido, las instituciones reconocen que la gestión de riesgos debe ser un motor de ventaja competitiva y resiliencia, más allá del cumplimiento regulatorio. De acuerdo con el orden de prioridad de los riesgos que expresaron los encuestados, los riesgos tradicionales como crédito (78%) y operacional (48%) siguen siendo relevantes, pero emergen otros con mayor peso: ciberseguridad (80%), riesgos tecnológicos (77%) y privacidad (77%), impulsados por la digitalización y el uso intensivo de datos. Sin embargo, cuantificar estos riesgos no financieros es difícil: en el 80% de los casos, las metodologías actuales no capturan su complejidad.

Integrar la gestión de riesgos en una visión holística es clave: comprender la interdependencia entre factores humanos, tecnológicos, regulatorios y ambientales permite anticipar impactos sistémicos, diseñar respuestas ágiles y fortalecer la gobernanza. Así, la gestión de riesgos conecta estrategia, innovación y sostenibilidad. De acuerdo con lo inferido en las conclusiones de la encuesta, los bancos priorizan riesgos emergentes, inteligencia artificial, análisis de datos y riesgos ASG (Ambientales, Sociales y de Gobernanza), impulsados por presión regulatoria, expectativas sociales y eventos disruptivos. Integrar estos factores será determinante para la competitividad futura.



La anticipación de riesgos aún tropieza con el espejo retrovisor

Es necesario mirar hacia adelante con más ciencia y menos historia.

En IA, la preparación de las entidades bancarias en América Latina está en un momento de despegue: 62% parcialmente listo, 32% no preparado, solo 5% totalmente preparado y 1% no planea implementarla. No obstante, la inteligencia artificial (IA) y el análisis de datos fortalecen la gestión de riesgos al anticipar comportamientos, pero plantean retos éticos y de gobernanza que requieren marcos de control responsables. Los riesgos ASG son estratégicos en la banca, pues eventos climáticos, sociales o regulatorios afectan la estabilidad financiera. Integrarlos demanda nuevas fuentes de datos, indicadores y capacidades analíticas. Adicionalmente, las regulaciones exigen transparencia y resiliencia, impulsando marcos de cumplimiento y una cultura proactiva.

La colaboración entre reguladores, bancos y la tecnología, junto con un talento multidisciplinario, será clave.

Solo un enfoque retrospectivo es insuficiente; se requieren modelos predictivos basados en ciencia de datos y el uso de la IA para anticipar amenazas y pasar de una gestión reactiva a la proactiva. Esto implica modernizar procesos y fomentar una cultura que valore la anticipación. Por otra parte, la resiliencia organizacional se vuelve un activo esencial. Comprender los riesgos de manera sistémicas permite diseñar respuestas efectivas e integrar la gestión en la estrategia corporativa, convirtiendo la incertidumbre en una ventaja competitiva, reinventándose constantemente para ser resilientes y sostenibles.

Identificación y actualización de riesgos

Otro de los aspectos clave identificados fue que la gestión de riesgos de terceros se está volviendo crítica en el sector financiero, particularmente porque cerca del 40% de los bancos en la región están presentando rezagos al respecto, con marcos que aún se encuentran en desarrollo para evaluar y mitigar riesgos asociados a proveedores y plataformas externas. Aunque tecnologías como IA y ML tienen gran potencial, su adopción es limitada por falta de talento, regulación clara y preocupaciones éticas. Paralelamente, aunque hay avances en ciberseguridad con un nivel de prioridad del 80% entre las organizaciones encuestadas, riesgos emergentes como el uso de la IA generativa y ataques a la cadena digital, aún no se comprenden del todo, afectando la capacidad de respuesta de los CROs. Es urgente definir un roadmap estratégico que integre tecnología, gobernanza de datos, talento y regulación, para que la gestión de riesgos deje de ser un área aislada para convertirse en un componente transversal de la estrategia corporativa.

Gestión y priorización de riesgos

Los riesgos financieros siguen siendo centrales, pero los emergentes tales como la situación geopolítica mundial con una prioridad del 67% para los bancos, el manejo de los datos (66% de prioridad) y factores ambientales (65%) están ganando ventaja en la agenda de los directivos. Otros pilares de interés dentro los que se encuentran cambio climático, conducta corporativa, disrupción tecnológica y presión regulatoria, exigen una gestión diferenciada. Estos riesgos son complejos de cuantificar, por lo que requieren métricas nuevas y un enfoque holístico que combine datos cuantitativos y cualitativos,. Asimismo, la vulnerabilidad tecnológica y el cumplimiento normativo son críticos. La dependencia digital y las amenazas cibernéticas demandan modelos de protección ágiles y automatizados. Aunque hay avances en ciberseguridad, se debe acelerar el uso de la IA para detectar amenazas, responder a incidentes y gestionar vulnerabilidades, lo que implica inversión, talento y gobernanza ética.



Adoptar tecnologías disruptivas como el machine learning y análisis predictivos es clave para anticipar riesgos y convertirlos en oportunidades. La gestión debe evolucionar hacia una plataforma de inteligencia corporativa, con un enfoque proactivo, digitalizado y con una visión ética y global. Este cambio requiere transformación cultural: el riesgo debe ser responsabilidad de toda la organización, con líderes preparados, colaboración transversal y aprendizaje continuo. En un entorno complejo, la gestión debe ser integral, tecnológica y estratégica para asegurar excelencia y competitividad a largo plazo.

Riesgos tecnológicos y de terceros

Otro de los aspectos inferidos en este estudio es que la gestión de riesgos con terceros sigue siendo débil en muchas organizaciones, con enfoques dispares y sin marcos metodológicos sólidos; esto se deriva de que la capacidad para evaluar el riesgo de proveedores críticos es mayormente intermedia (41%), con brechas significativas: 20% inmaduro, 18% básico y apenas 4% avanzado.

Aunque la tecnología ha avanzado en el monitoreo, la adopción y el uso de la IA y ML en la gestión de riesgo de terceras partes es aún limitada y enfrenta barreras como la falta de talento, inversión e infraestructura regulatoria. La escasa trazabilidad y preparación tecnológica revelan brechas en talento, normativas y privacidad. Superarlas requiere colaboración interdisciplinaria entre diversos sectores o grupos de interés involucrados.

Es clave definir un roadmap estratégico que integre tecnología, fortalezca la gobernanza de datos y capacite al talento para su uso en pro de la gestión de riesgos tecnológicos y de terceros. Otro de los aspectos analizados es que la innovación debe verse como una oportunidad para construir sistemas resilientes y éticos. Esto implica rediseñar procesos y estructuras, integrando datos en tiempo real y garantizando decisiones automatizadas responsables. Es fundamental el liderazgo transformacional que promueva una cultura de innovación.



¿Cuáles son los Riesgos Financieros más relevantes a partir del tamaño de la entidad bancaria o financiera?

Los riesgos financieros varían significativamente según la escala operacional. Mientras que las entidades pequeñas enfrentan una elevada concentración en riesgo de crédito y vulnerabilidades operativas y de liquidez, las entidades medianas presentan un perfil más equilibrado, donde comienzan a tomar relevancia los riesgos de mercado. En complemento, las grandes entidades bancarias muestran una distribución más uniforme de riesgos gracias a una mayor diversificación, sofisticación tecnológica y capacidad de gestión, aunque mantienen exposición moderada a riesgos de mercado derivados de actividades financieras más complejas.

Tamaño de entidad	Riesgo dominante	Otros riesgos relevantes	Interpretación general
Pequeñas	Crédito (39%)	Operacional, liquidez	Altísima vulnerabilidad crediticia y operativa; limitaciones estructurales.
Medianas	Crédito (25%)	Operacional, mercado	Perfil diversificado, transición hacia mayor sofisticación financiera.
Grandes	Crédito (14%)	Mercado, operacional	Riesgos atomizados, alta capacidad de mitigación, mayor exposición financiera compleja.

El Riesgo de Crédito es la mayor amenaza que enfrentan los bancos de América. Latina y El Caribe.



¿Cuáles son los Riesgos Financieros más relevantes por cada región?

Los riesgos financieros varían significativamente según la estructura, madurez y contexto económico de cada grupo territorial. Centroamérica y Caribe presentan la mayor vulnerabilidad con una concentración crítica en riesgo de crédito y operacional. En tanto que México muestra un riesgo crediticio importante, acompañado de volatilidad operativa y de mercado. La Región Andina Sur refleja la distribución más equilibrada entre los diferentes tipos de riesgos, reportando sistemas financieros relativamente robustos. En contraste, la Región Andina Norte presenta un alto riesgo operacional y una proporción significativa de riesgos no tradicionales, reflejando condiciones estructurales y regulatorias particulares.

Región	Riesgo dominante	Interpretación general
México	Crédito (13%)	Sistema estable pero expuesto a volatilidad operativa y de mercado.
Centroamérica y Caribe	Crédito (28%)	Mayor vulnerabilidad regional con fuerte exposición crediticia y operativa.
Andina Sur	Crédito (13%) / Liquidez (10%)	Perfil más balanceado y sistemas financieros más sólidos.
Andina Norte	Operacional (12%) / Mercado y Crédito (10%)	Altos riesgos operativos y factores específicos país fuera de categorías



¿Cuáles son los Riesgos No Financieros más relevantes según el tamaño de la entidad bancaria o financiera?

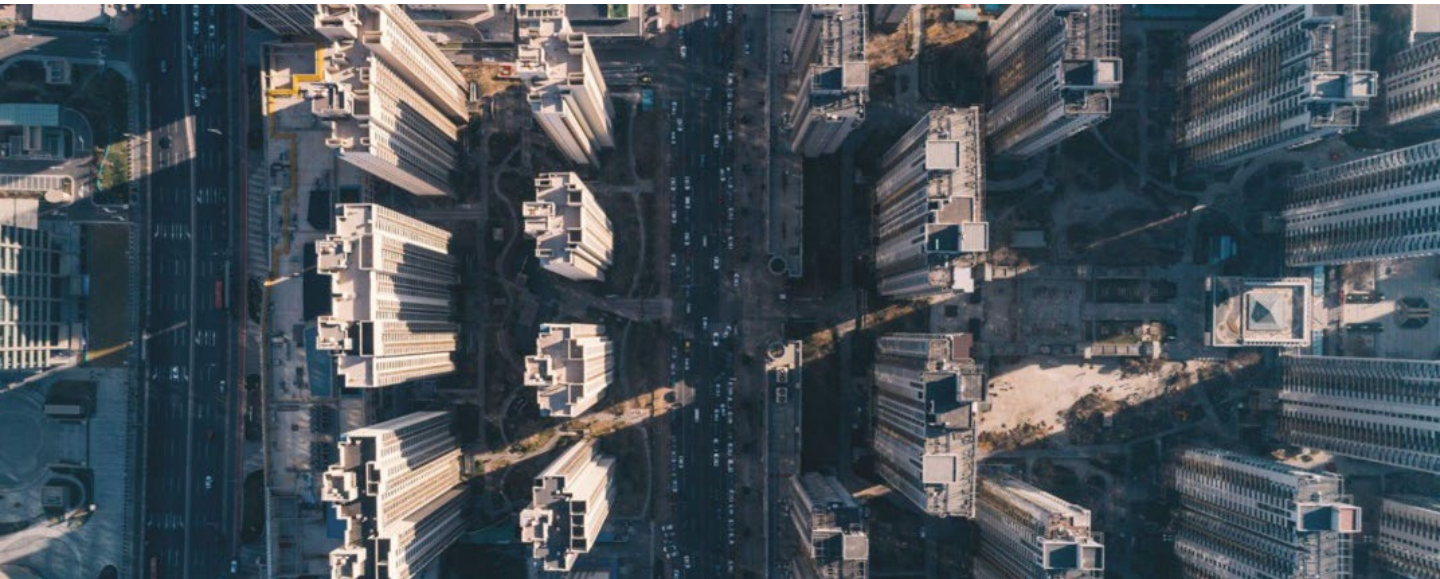
El tratamiento de riesgos no financieros varía por escala. Por una parte, las entidades pequeñas y medianas dependen fuertemente del seguimiento de métricas/umbrales y del análisis post mortem, mientras comienzan a incorporar perfiles dinámicos de riesgo. Sin embargo, las grandes muestran un repertorio más distribuido, pero reportan una brecha relevante (8%), sin método estandarizado para monitoreo no financiero. En todas las entidades, la analítica avanzada para detección de riesgos atípicos permanece subutilizada, lo que limita la identificación temprana de eventos y la anticipación a cambios en el perfil de riesgo.

Tamaño de entidad	Riesgo dominante	Riesgo latente	Interpretación general
Pequeñas	Seguimiento de métricas/umbrales (34%) y post mortem (33%), con perfiles dinámicos (28%).	Capacidad analítica limitada (10%) y gobernanza con casos sin método/planes (5% combinados) podrían ampliar el riesgo operacional y de cumplimiento.	Modelo centrado en umbrales y reacción a incidentes, con señales positivas de evolución proactiva (perfiles).
Medianas	Seguimiento de métricas/umbrales (29%) + post mortem (22%) + expertos (19%) y perfiles (19%).	La analítica sigue subutilizada (9%), lo que limita detección temprana y alertas avanzadas.	Portafolio balanceado con mejor apoyo experto.
Grandes	Cartera diversificada con métricas/umbrales (16%), post mortem (13%), expertos (13%), perfiles (11%) y analítica (7%).	8% sin método revela brechas de estandarización (frecuente en conglomerados), especialmente en riesgos emergentes o unidades periféricas.	Menor concentración en una sola práctica, lo que sugiere madurez y redundancia de controles.

¿Cuáles son los Riesgos No Financieros más relevantes con base en la región?

El Riesgo Operacional es el Riesgo No Financiero predominante en América Latina y Caribe, reflejado en el uso de indicadores o KRI, análisis post mortem y herramientas para identificar riesgos emergentes. Centroamérica y Caribe destacan por su mayor madurez preventiva, impulsada por una gestión anticipada basada en métricas. En contraste, México y Andina Sur mantienen un enfoque más reactivo, centrado en el aprendizaje tras incidentes. Andina Norte combina ambos enfoques, integrando monitoreo preventivo con análisis correctivo.

Región	Riesgo dominante	Interpretación general
México	Perfiles de riesgo para cambios inherentes/emergentes (14%)	Equilibrio entre detección temprana y análisis reactivo; oportunidad de profundizar automatización de alertas y KRIs adelantados.
Centroamérica y Caribe	Seguimiento con métricas y umbrales (31%)	Región con mayor disciplina de KRI y capacidad preventiva; espacio para ampliar analítica avanzada (detección de comportamientos atípicos).
Andina Sur	Captura y análisis de incidentes (12%) y métodos de rastreo de niveles de riesgo (12%)	Énfasis reactivo; priorizar homogeneización de umbrales y monitoreo continuo para reducir volatilidad operativa y regulatoria.
Andina Norte	Seguimiento con métricas y umbrales (23%)	Buena base preventiva vía KRI y sensibilidad a incidentes; acelerar modelos de detección temprana y respuesta coordinada ante eventos.





¿Cuál es el grado de integración del Análisis de Datos en los procesos de evaluación de riesgos según el tamaño de la entidad?

Las medianas empresas destacan con el mayor grado de integración, especialmente en niveles amplios, evidenciando una madurez analítica superior. Las pequeñas empresas presentan una adopción significativa, con mayor presencia en niveles intermedios. En contraste, las grandes empresas exhiben una integración más distribuida y menos concentrada en niveles altos, lo que sugiere heterogeneidad interna o procesos más complejos que obstaculizan su avance hacia una total integración.

Tamaño de entidad	Grado de integración	Interpretación general
Pequeñas	Muestran los porcentajes más altos en las categorías “Algo integrado” (20%) y “Amplia integración” (19%)	Tienden hacia una integración funcional pero no sofisticada. El peso fuerte en categorías medias indica que han adoptado prácticas de análisis de datos, pero aún no operan con modelos avanzados o automatización profunda.
Medianas	Porcentaje más alto en la categoría “Amplia integración” (16%)	Se posicionan como el grupo con integración más robusta y generalizada. No sólo integran el análisis de datos, sino que lo hacen con una amplitud significativa. Son el segmento donde más claramente se observa un salto entre adopción básica y consolidación operacional.
Grandes	Porcentajes distribuidos de forma más equilibrada, sin un nivel sobresaliente.	Los datos sugieren que no existe una integración sustancialmente superior respecto a los otros segmentos. Aunque sí se observa presencia en las categorías de mayor madurez

¿Cuál es el grado de integración del Análisis de Datos en los procesos de evaluación de riesgos según la región?

Avance regional significativo, aunque con brechas importantes entre los segmentos, lo que sugiere la oportunidad de desarrollar iniciativas de armonización, transferencia de mejores prácticas y fortalecimiento analítico en territorios con mayores brechas.

Región	Grado de integración	Interpretación general
México	Amplia integración (8%) y Totalmente integrado (4%) suman 12%, lo que indica que existe una cantidad relevante de bancos con uso avanzado.	Se encuentra en fase de consolidación analítica, con señales claras de adopción creciente, pero aún por debajo de los niveles más robustos observados en otras regiones.
Centroamérica y Caribe	Es el segmento mejor posicionado en análisis de datos. Amplia integración (15%) es la categoría más alta.	Lidera la adopción, mostrando una cultura más establecida de toma de decisiones basada en datos. Esto la convierte en el referente regional para prácticas maduras en evaluación de riesgos.
Andina Sur	Adopción heterogénea y más fragmentada, con porcentajes moderados que revelan un ecosistema desigual.	Estado de evolución dispar, con avances, pero mostrando la mayor necesidad de fortalecimiento en términos de estandarización y adopción de capacidades analíticas.
Andina Norte	Amplia integración (13%) es una de las cifras más altas, muestra una distribución madura con un peso claro hacia niveles altos de adopción.	Esfuerzos avanzados en la integración del análisis de datos, solo ligeramente por debajo del liderazgo actual de Centroamérica y Caribe.



Las preocupaciones de los líderes de la banca en América Latina y el Caribe sobre el contexto actual de disrupción tecnológica

En América Latina y El Caribe, la aceleración digital ha dejado de ser una aspiración estratégica para convertirse en el tejido que sostiene la competitividad del sector financiero. Los CEO's, CRO's y CTO's de entidades bancarias y financieras están operando en un entorno donde las fronteras entre lo tecnológico, lo regulatorio y lo criminal se desdibujan cada vez más.

Hoy, la pregunta ya no es cómo digitalizarse, sino cómo sobrevivir y crecer en un escenario donde cada avance tecnológico empuja simultáneamente la superficie de exposición al riesgo. La ciberseguridad y los fraudes se han posicionado como los riesgos emergentes de mayor preocupación estratégica, desplazando incluso a riesgos financieros tradicionales. El 64% de las instituciones identifica la ciberseguridad como barrera crítica para adoptar nuevas tecnologías, a la par del costo de inversión. Esa cifra no solo habla de presupuesto; habla de percepción de vulnerabilidad.

Los líderes financieros entienden que la ciberseguridad dejó de ser una disciplina técnica aislada para convertirse en un mecanismo esencial de continuidad del negocio, resiliencia reputacional y licencia operativa. Al mismo tiempo, los riesgos derivados del uso de inteligencia artificial maliciosa —como los *deepfakes* que habilitan fraudes por suplantación de ejecutivos— agregan una capa de complejidad que trasciende los controles clásicos. La digitalización masiva de los medios de pago, la interoperabilidad y las plataformas abiertas ampliaron los puntos de acceso donde los actores

criminales pueden operar con sofisticación inédita. Aunque muchos bancos han fortalecido sus sistemas antifraude, los sistemas aún no están completamente integrados entre sí, lo cual genera “puntos ciegos” que dificultan la respuesta en tiempo real.

La nube está directamente conectada con la capacidad analítica de una organización. Las plataformas cloud permiten actuar sobre datos verificables, anticipar riesgos y automatizar decisiones, pero solo si existe una gobernanza robusta del ciclo de vida del dato.

Por otra parte, la aceleración de iniciativas como Pagos Instantáneos (FPS) y Finanzas Abiertas (Open Finance) en América Latina y el Caribe no es simplemente un avance tecnológico: representa una reconfiguración profunda del entorno financiero. Estas tendencias marcan el inicio de una arquitectura más amplia y centrada en el usuario, pero también habilitan escenarios de riesgo que desafían los supuestos tradicionales de control y supervisión.

La banca latinoamericana se encuentra en un punto de inflexión histórico: el riesgo ya no es una dimensión a gestionar, sino una plataforma para competir. En esta nueva era, el liderazgo se medirá no por la capacidad de evitar amenazas, sino por la capacidad de anticiparlas, comprenderlas y convertirlas en decisiones inteligentes.

5

Identificación
y actualización
de riesgos

Perspectivas sobre la identificación de riesgos desconocidos y nuevos

En el entorno empresarial actual, caracterizado por una aceleración constante del cambio tecnológico, geopolítico y social, la identificación de riesgos emergentes se ha convertido en una prioridad estratégica. Sin embargo, esta práctica debe ir más allá de la observación pasiva del entorno competitivo. Las organizaciones líderes están integrando inteligencia sectorial con análisis contextual, permitiendo no solo identificar amenazas, sino también descubrir oportunidades ocultas en medio de la incertidumbre. Esta capacidad de leer entre líneas y conectar señales débiles con tendencias macroeconómicas es lo que diferencia a las empresas resilientes de aquellas que simplemente reaccionan.

Esta tendencia evidencia una evolución en la madurez analítica de las organizaciones, que ahora buscan comprender no solo qué podría ocurrir, sino por qué y cómo podría desarrollarse un riesgo.

Incorporar modelos de Machine Learning, simulaciones de escenarios y análisis de segmentación y comportamiento del cliente o del mercado permite construir mapas de riesgo dinámicos, que se ajustan en tiempo real a los cambios del entorno. Esta capacidad de anticipación es clave para tomar decisiones informadas, asignar recursos estratégicamente y fortalecer la gobernanza corporativa. Si bien la revisión anual es una práctica estándar, en un contexto de volatilidad creciente, podría

resultar insuficiente. Las organizaciones deben considerar esquemas de revisión continua, apoyados por comités multidisciplinarios y herramientas tecnológicas que permitan una actualización ágil del apetito de riesgo.

71%

de las entidades identifican riesgos emergentes mediante investigación de la industria.

63%

incorpora el análisis predictivo y de comportamiento.

81%

de los bancos realiza la revisión del plan de riesgos de manera anual.



Además, es fundamental que esta revisión no se limite a aspectos operativos, sino que incorpore dimensiones éticas, reputacionales y de sostenibilidad. En última instancia, la gestión de riesgos debe ser vista como un habilitador estratégico que impulsa la innovación responsable y la creación de valor a largo plazo.

En entornos corporativos complejos, donde múltiples áreas interactúan en procesos interdependientes, la falta de articulación puede generar silos informativos que dificultan la toma de decisiones oportunas. Por ello, es imperativo que las organizaciones fortalezcan sus canales de comunicación interna, promoviendo una cultura de riesgo transversal.

Herramientas como el análisis de escenarios, las pruebas de estrés, la simulación de Monte Carlo, los modelos de Valor en Riesgo (VaR) y la técnica Delphi permiten no solo modelar incertidumbres, sino también definir cursos de acción basados en criterios cuantitativos. Estas metodologías, al ser integradas en los procesos de planificación estratégica, permiten a las empresas construir resiliencia organizacional, evaluar el impacto potencial de eventos extremos y diseñar respuestas adaptativas que minimicen la exposición, a la vez que maximizan la capacidad de recuperación.

Más allá de su aplicación técnica, estas herramientas deben ser vistas como catalizadores de una transformación cultural en la gestión de riesgos.

La gestión de riesgos debe evolucionar de una función reactiva a una capacidad organizacional integrada, donde la anticipación, la comunicación efectiva y la toma de decisiones basada en datos se conviertan en pilares de la sostenibilidad empresarial.

48%

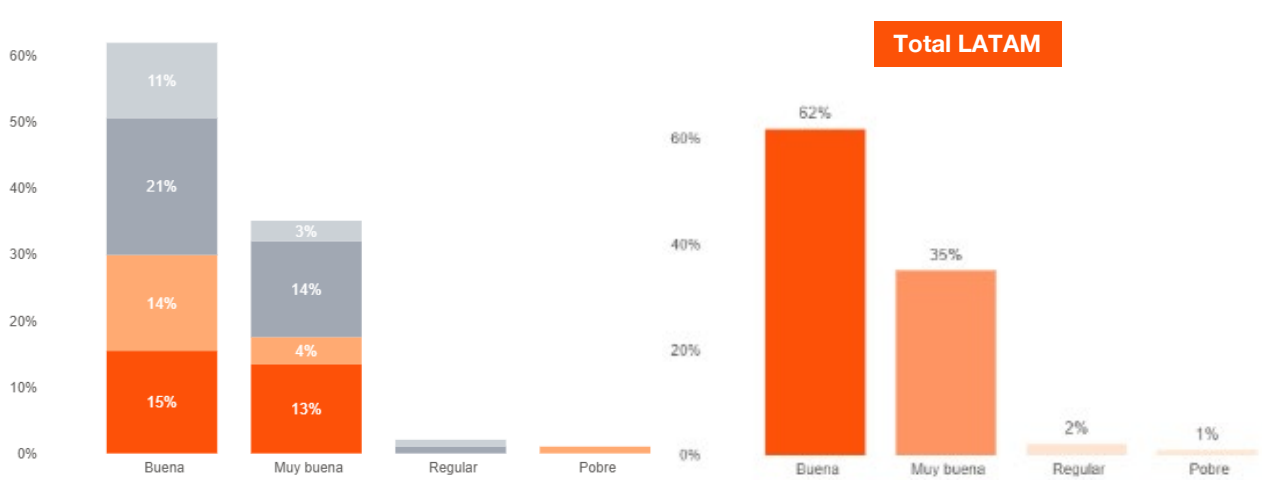
de las organizaciones considera que sus mecanismos de comunicación son muy efectivos.

9%

ha adoptado métodos avanzados para la identificación de riesgos.

La Gestión de Riesgos requiere instalar y actualizar capacidades en el personal de manera permanente

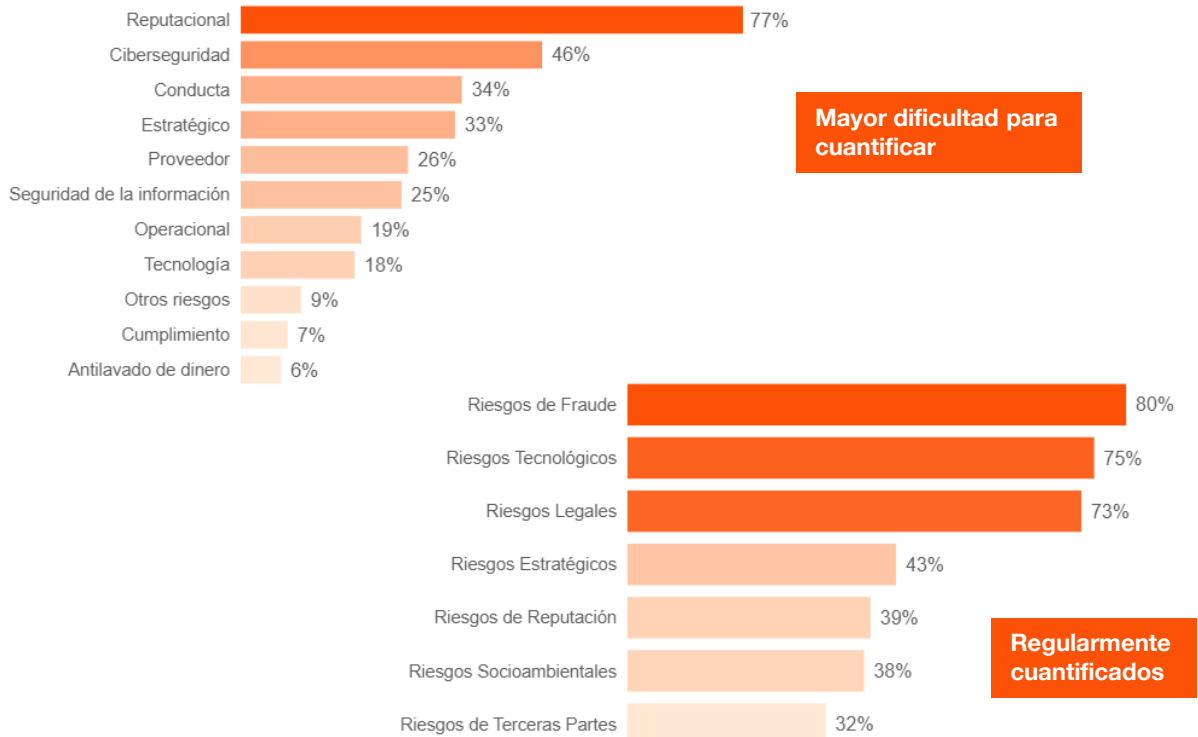
Region ● Andina Norte ● Andina Sur ● Centroamérica y Caribe ● México



La Región de Centroamérica y el Caribe muestra avances significativos en la percepción favorable de sus mecanismos de formación, lo cual representa una base sólida para fortalecer la gestión de riesgos en un entorno cada vez más digitalizado y complejo. El incremento del 40% en la inversión en programas de capacitación continua para mitigar riesgos operacionales y cibernéticos es una señal positiva, pero aún insuficiente frente a la velocidad con la que evolucionan las amenazas. En este sentido, las organizaciones deben adoptar una visión estratégica de largo plazo, donde la formación no sea vista como un gasto, sino como una inversión crítica en resiliencia organizacional. La capacitación debe estar alineada con los objetivos de negocio, ser transversal a todas las áreas y adaptarse a los distintos niveles de madurez digital de cada entidad.

A pesar de estos esfuerzos, solo el 30% de las instituciones ha avanzado en la adopción de herramientas analíticas sofisticadas, lo que evidencia una brecha entre la intención y la ejecución. La gestión de riesgos moderna exige capacidades analíticas robustas que permitan anticipar escenarios, modelar impactos y tomar decisiones basadas en datos. La baja preparación para implementar Inteligencia Artificial (IA) en estos procesos —con apenas un 15% de avance en conocimiento especializado, 8% en acceso a herramientas tecnológicas y desafíos en la calidad de los datos— revela que aún estamos en una etapa inicial. Para superar esta barrera, es necesario fomentar alianzas estratégicas con universidades, centros de innovación y proveedores tecnológicos que aceleren la transferencia de conocimiento y la adopción de soluciones avanzadas.

Riesgos no financieros más difíciles de cuantificar y regularmente cuantificados



La priorización de riesgos cuantificables como el fraude (80%), los tecnológicos (75%) y los legales (73%) refleja una tendencia natural hacia aquellos eventos que presentan impactos financieros directos y cuya trazabilidad es más clara. Sin embargo, esta focalización puede generar una visión parcial del panorama de riesgos, dejando rezagados aspectos estratégicos, reputacionales, socioambientales y de terceros, que, aunque más difíciles de medir, pueden tener consecuencias sistémicas y de largo plazo. La gestión moderna del riesgo exige una evolución desde lo cuantificable hacia lo comprensible, incorporando metodologías

que permitan capturar el valor intangible de la reputación, la sostenibilidad y las relaciones con terceros, elementos que hoy son determinantes en la percepción de valor por parte de los stakeholders.

La dificultad para cuantificar el riesgo reputacional (77%), seguido por ciberseguridad (46%) y conducta/estratégico (34–33%), contrasta con la alta medición de riesgos tecnológicos, lo que evidencia una brecha crítica entre lo que se mide con frecuencia y lo que realmente cuesta medir.

Medidas adoptadas para fortalecer la gestión de riesgos de conducta

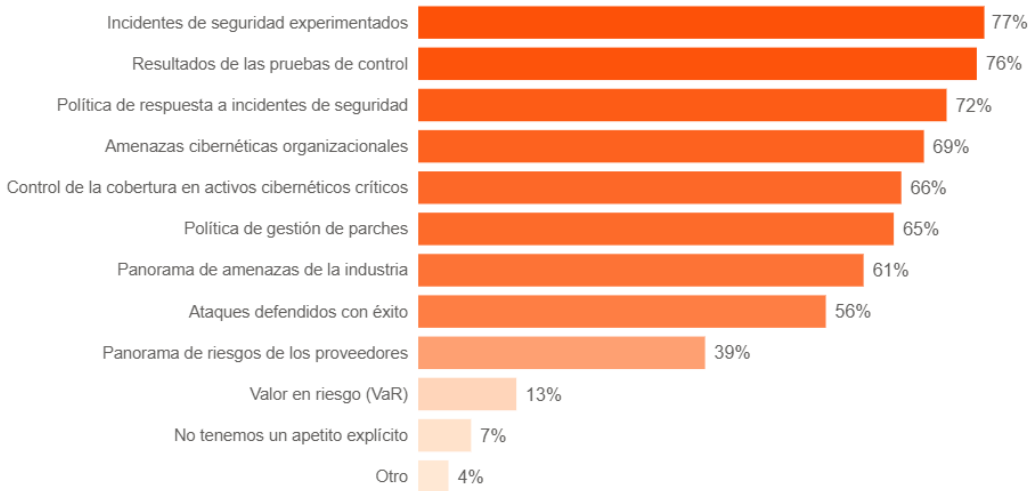


La priorización de acciones de primera línea para mitigar el riesgo de conducta —como la capacitación (66%) y el establecimiento de marcos de gestión (52%)— refleja un enfoque preventivo que busca fortalecer la cultura ética desde la base operativa. La revisión de prácticas empresariales, portafolios de productos y perfiles de clientes (42%) complementa esta estrategia, permitiendo identificar zonas de vulnerabilidad que podrían derivar en conductas inapropiadas o riesgos reputacionales. Sin embargo, para que estas acciones sean sostenibles, deben estar integradas en un sistema de gestión que combine formación continua, monitoreo activo y retroalimentación estratégica. La conducta organizacional no se transforma únicamente con políticas, sino con coherencia entre lo que se promueve, se mide y se recompensa.

El avance del cambio cultural, aunque moderado, es una señal de que las organizaciones están reconociendo la necesidad de evolucionar más allá del cumplimiento normativo. El foco en la responsabilidad de las líneas de negocio (32%) y la mejora en la medición y reportes (29%) indica que aún se percibe el riesgo de conducta como una responsabilidad operativa, más que como un desafío estratégico. Para lograr una transformación real, es necesario que el liderazgo impulse una cultura de integridad que trascienda los manuales y se refleje en las decisiones cotidianas. Esto implica redefinir indicadores de desempeño, incorporar métricas de comportamiento ético y fomentar espacios de diálogo donde los dilemas éticos puedan ser abordados con madurez y transparencia.

La seguridad y la privacidad deben ser abordadas desde el diseño, con políticas claras, controles robustos y una cultura organizacional que valore la protección de los datos.

Métricas más utilizadas en los análisis de riesgos de ciberseguridad



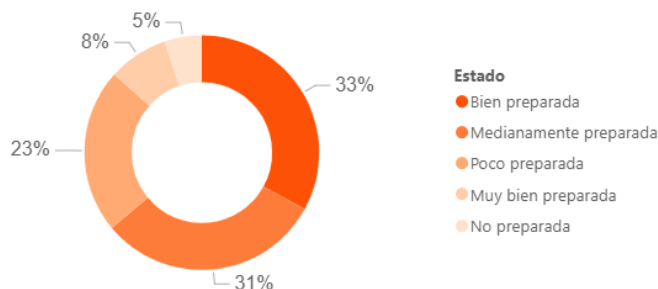
Los análisis de ciber-riesgo en las organizaciones siguen centrados en métricas operativas y de control, como incidentes experimentados (77%), resultados de pruebas (76%) y capacidad de respuesta (72%). Este enfoque, aunque útil para evaluar la madurez técnica y operativa, tiende a ser reactivo y orientado al cumplimiento, lo que restringe su capacidad para anticipar impactos estratégicos. La alta atención a amenazas internas (69%) y cobertura de activos críticos (66%) demuestra una conciencia creciente sobre la protección de infraestructura, pero también evidencia una falta de integración entre la gestión de ciber-riesgos y la creación de valor económico. Para avanzar, las organizaciones deben migrar hacia modelos que vinculen la ciberseguridad con la continuidad del negocio, la reputación corporativa y la confianza del cliente.

La baja atención al riesgo de terceros (39%) y la escasa cuantificación financiera mediante modelos como Valor en Riesgo (VaR, 13%) revelan una brecha importante en la comprensión del impacto económico de los ciber-riesgos. En un entorno digital interconectado, los proveedores, socios tecnológicos y plataformas externas representan vectores críticos de exposición. Ignorar esta dimensión puede llevar a subestimar pérdidas potenciales, especialmente en eventos que afectan la cadena de valor o comprometen datos sensibles. Además, el hecho de que un 7% de las organizaciones no declare su apetito de riesgo sugiere una falta de alineación entre la estrategia corporativa y la gestión de riesgos, lo que dificulta la toma de decisiones informadas y la asignación eficiente de recursos.

Ante este panorama, se vuelve imperativo incorporar métricas prospectivas y de impacto que permitan anticipar escenarios, modelar pérdidas potenciales y evaluar tiempos de detección y contención.

La gestión de riesgos desde la perspectiva ambiental

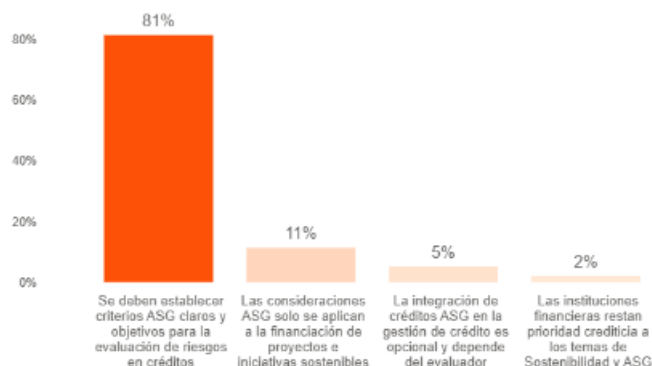
Preparación para mitigar riesgos ambientales



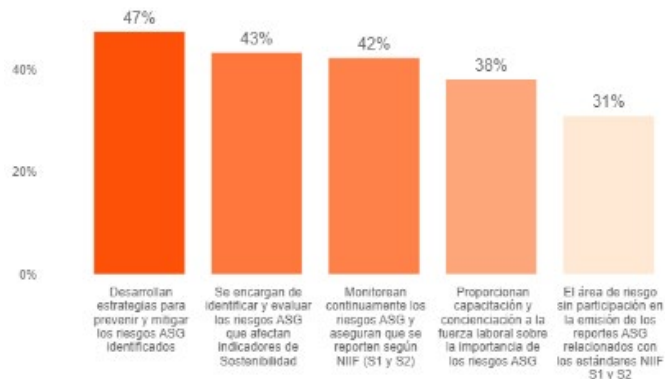
La bitácora del cambio se perfila hacia la estandarización de metodologías y el fortalecimiento de capacidades para cerrar brechas de preparación y emisión de reportes.

La evolución hacia una sostenibilidad corporativa más madura se está consolidando a través de la estandarización de metodologías y el fortalecimiento de capacidades internas. Esta “bitácora del cambio” refleja un esfuerzo por cerrar brechas en la preparación y emisión de reportes, especialmente en el marco de los estándares internacionales como NIIF S1 y S2. La estandarización no solo mejora la comparabilidad entre organizaciones, sino que también permite una gestión más rigurosa de los riesgos ASG (ambientales, sociales y de gobernanza). En este contexto, la sostenibilidad deja de ser un ejercicio de cumplimiento para convertirse en un componente estratégico que influye directamente en la toma de decisiones, la reputación corporativa y el acceso a financiamiento responsable.

Consideraciones ASG en las políticas y gestión de crédito



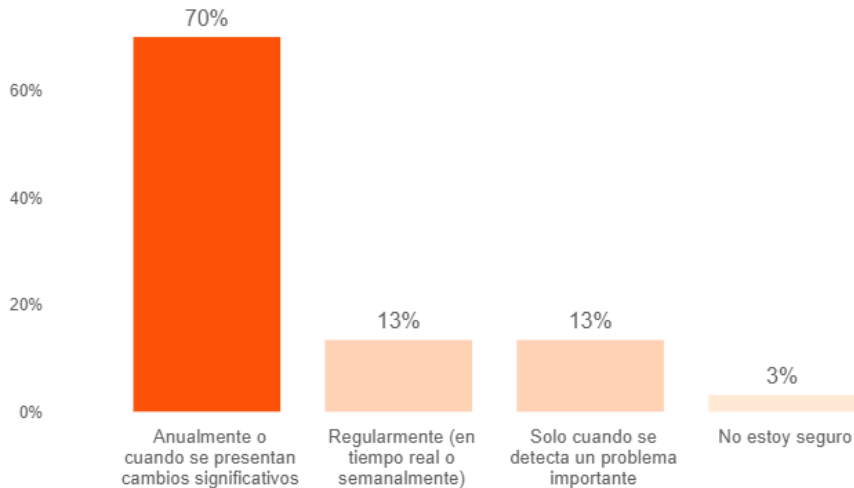
Rol de las áreas de riesgo en la emisión futura de los reportes ASG



Las áreas de riesgo han asumido un rol protagónico en la gestión ASG, con un 58% participando activamente en la gestión integral y un 74% aportando datos y herramientas para cuantificar impactos financieros.

El análisis de datos en el proceso de evaluación de riesgos

Frecuencia de actualización de modelos analíticos para la gestión de riesgos



La integración del análisis de datos en la evaluación de riesgos muestra una adopción significativa en las organizaciones, con un 42% que reporta una amplia integración y un 18% con integración total. Este avance refleja una creciente conciencia sobre el valor del dato como activo estratégico para la toma de decisiones informadas. Sin embargo, aún persiste una franja considerable (29%) con integración parcial, lo que sugiere que muchas organizaciones están en una fase de transición. Para consolidar esta evolución, es fundamental que el análisis de datos no se limite a funciones operativas, sino que se convierta en un habilitador transversal de la gestión de riesgos, capaz de conectar indicadores técnicos con impactos financieros, reputacionales y estratégicos.

El principal cuello de botella identificado —

la calidad y precisión de los datos (59%)— representa un desafío estructural que limita el potencial del análisis avanzado. Sin datos confiables, incluso los modelos más sofisticados pierden efectividad. A esto se suma la falta de herramientas adecuadas (23%) y la escasa capacitación del personal (10%), lo que evidencia una brecha entre la ambición analítica y la capacidad instalada. Para superar estos obstáculos, las organizaciones deben priorizar el fortalecimiento del gobierno de datos, implementar políticas de calidad desde el origen y fomentar una cultura de alfabetización digital. El “data quality” no es solo una cuestión técnica, sino una responsabilidad compartida que debe estar alineada con los objetivos estratégicos de la organización.



En entornos volátiles, la actualización continua de modelos es clave para mantener la relevancia de los análisis y responder con agilidad a nuevas amenazas. Además, el hecho de que otro 13% actualice únicamente ante fallas sugiere una cultura de gestión aún centrada en la corrección más que en la prevención. Migrar hacia un enfoque de monitoreo dinámico requiere no solo tecnología, sino también procesos ágiles y equipos capacitados para interpretar y actuar sobre los datos en tiempo real.

Es imperativo integrar capacidades de inteligencia artificial, automatización y visualización avanzada, pero también rediseñar los flujos de trabajo para que el análisis de datos sea parte integral de la gestión de riesgos. La transformación hacia una cultura analítica no se logra únicamente con herramientas, sino con liderazgo, visión y una estrategia clara que vincule el dato con el valor empresarial. En última instancia, el análisis de datos debe ser visto como un motor de resiliencia, innovación y ventaja competitiva.

En este contexto, las implicaciones estratégicas son claras: las organizaciones deben modernizar su stack analítico, invertir en “upskilling” del talento humano y establecer mecanismos de gobernanza que aseguren la trazabilidad, consistencia y utilidad de los datos.

70%

de las entidades actualiza sus modelos de riesgos de forma anual o ante cambios significativos.

13%

hace actualizaciones en los modelos de riesgos de manera continua, revelando una tendencia reactiva.

Desafíos para adoptar nuevas tecnologías en gestión de riesgos y perspectivas para los próximos 3 años

La evolución tecnológica en la gestión de riesgos está marcando una nueva frontera en la sofisticación operativa de las organizaciones. En el horizonte de un año, tecnologías como la inteligencia artificial (IA) y la automatización robótica de procesos (RPA) se perfilan como los frentes más maduros, con una clara orientación hacia la eficiencia, la detección temprana de anomalías y la mejora en la toma de decisiones. Chatbots y “machine Learning” (ML), aunque con una base sólida, aún se posicionan como herramientas complementarias. Blockchain, por su parte, muestra una adopción selectiva, especialmente en procesos que requieren trazabilidad y seguridad transaccional, mientras que la computación cuántica permanece en una etapa incipiente.

La falta de entendimiento sobre el impacto de estas tecnologías en la resiliencia organizacional (23%), la propiedad fragmentada de los proyectos (21%) y la resistencia del personal (20%) reflejan que la adopción tecnológica no es solo un reto técnico, sino también humano.

La adopción de estas tecnologías enfrenta barreras estructurales que deben ser abordadas con una visión integral. El costo y los riesgos de ciberseguridad (64% cada uno) se posicionan como los principales inhibidores, lo que evidencia la necesidad de construir modelos de negocio que justifiquen la inversión tecnológica desde una perspectiva de retorno estratégico. La escasez de talento especializado en TI (56%) también limita la capacidad de implementación, lo que obliga a las organizaciones a repensar sus estrategias de atracción, retención y desarrollo de capacidades. A esto se suman factores como la incertidumbre regulatoria (39%) y los desafíos de operar en múltiples jurisdicciones (30%), que requieren una gobernanza tecnológica robusta y una estrategia clara sobre cuándo construir internamente y cuándo adquirir soluciones externas.

En tres años, se espera una alta adopción de IA, ML, automatización y chatbots en gestión de riesgos. Blockchain crecerá gradualmente y la computación cuántica avanzará con aplicaciones aún en exploración.

Modelos analíticos, uso de herramientas de visualización y mitigación de riesgos con respecto a la implementación de la IA

La gestión de riesgos asociados a la inteligencia artificial (IA) se encuentra en una etapa temprana de desarrollo, donde las acciones predominantes se centran en la capacitación del personal (33%). Si bien este enfoque es fundamental para construir una base de conocimiento técnico y ético, preocupa que un 32% de las organizaciones aún no esté desplegando medidas mitigadoras.

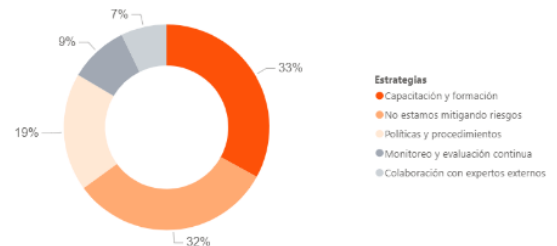
Esto evidencia una falta de urgencia estratégica frente a los riesgos emergentes de la IA, que van desde sesgos algorítmicos hasta impactos reputacionales y regulatorios. La baja implementación de políticas (19%), monitoreo (9%) y apoyo externo (7%) sugiere que muchas organizaciones aún no han incorporado la IA en sus marcos de control integral, lo que podría generar vulnerabilidades operativas y de cumplimiento en el corto plazo.

La gobernanza de IA está concentrada en Riesgos (79%), lo que limita una visión integral. Faltan responsables claros, lo que afecta trazabilidad y respuesta. Para una gestión efectiva, se deben definir roles, integrar a TI y fortalecer políticas internas con enfoque ético y estratégico.

Unidad responsable de implementar y supervisar los modelos analíticos



Estrategias de mitigación de los riesgos asociados con la implementación de soluciones IA



47%

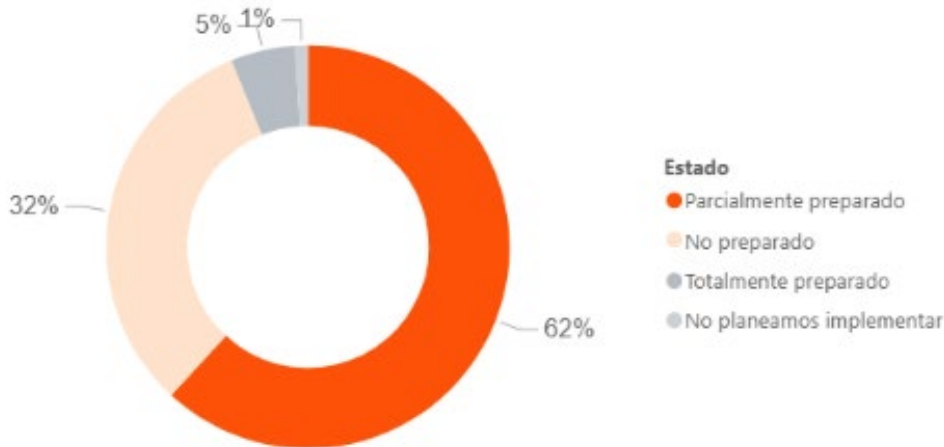
de las empresas tienen un nivel avanzado en herramientas para visualizar datos.

93%

ha logrado una adopción general en visualización de datos.

Estado actual para implementar soluciones de IA y riesgos principales que enfrentan las nuevas tecnologías

Estado actual para implementar soluciones de IA en la organización



La adopción tecnológica en las organizaciones, especialmente en el ámbito de la inteligencia artificial (IA), plantea una paradoja estratégica: mientras se reconoce su potencial transformador, los riesgos asociados —principalmente fallas de seguridad y privacidad (58%)— se convierten en factores dominantes que frenan su despliegue. A esto se suman desafíos como la dependencia excesiva de sistemas automatizados (14%), la complejidad de integración (13%) y los desajustes operacionales (12%), que evidencian una infraestructura aún en proceso de maduración. La preparación para implementar IA se encuentra en una fase inicial, con solo un 5% de las organizaciones totalmente listas y un preocupante 32% sin preparación alguna.

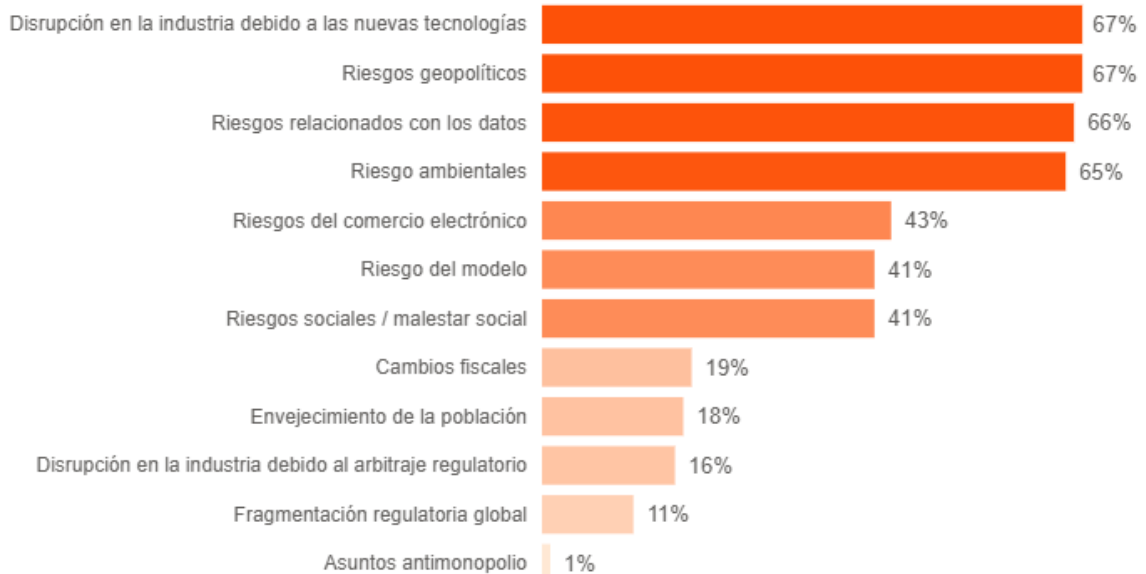
Esta combinación de alta expectativa y baja preparación anticipa una exposición significativa a incidentes de seguridad, fricciones operativas y pérdida de valor si se acelera la implementación sin una base sólida.

Es crucial fortalecer los protocolos de ciberseguridad, establecer una sólida gobernanza de datos y diseñar arquitecturas escalables. La gestión del cambio organizacional es clave, ya que la transformación tecnológica requiere una hoja de ruta que incluya desarrollo de capacidades, alineación cultural y objetivos claros. Factores como la resistencia del personal, la fragmentación de proyectos y la infraestructura limitada pueden obstaculizar el éxito.

6

Gestión y
priorización
de riesgos

Riesgos emergentes en los próximos 5 años



En los próximos cinco años, las organizaciones identifican como principales riesgos la disrupción tecnológica y los factores geopolíticos (67%), seguidos por los riesgos de datos (66%) y ambientales (65%). Esta combinación de amenazas muestra un entorno empresarial cada vez más complejo, donde factores externos e internos se entrelazan. Para enfrentarlo, las empresas deben fortalecer su resiliencia, anticiparse al cambio y adoptar modelos de gestión de riesgos con visión evolutiva.

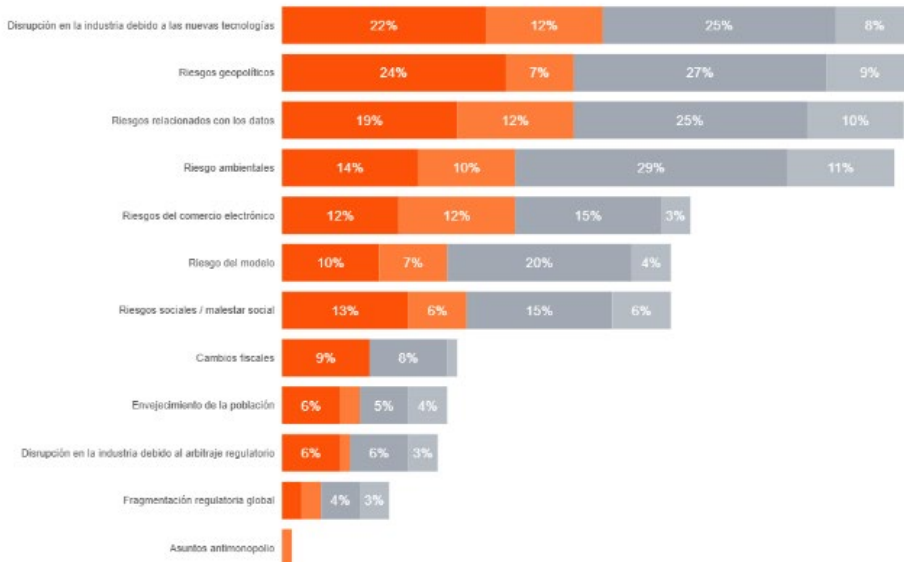
Un segundo grupo de riesgos inmediatos — como el comercio electrónico, el modelo de negocio y los riesgos sociales— puede afectar la operación y el crecimiento a corto plazo. Aunque menos estructurales, su capacidad de disrupción es alta si no se gestionan con agilidad. Por ejemplo, el comercio electrónico exige revisar canales, experiencia del cliente y ciberseguridad;

mientras que la polarización o el activismo digital pueden impactar la reputación. Las organizaciones deben equilibrar lo urgente con lo estratégico para no comprometer iniciativas futuras.

Riesgos como cambios fiscales, envejecimiento poblacional y regulación suelen ser subestimados, lo que puede generar puntos ciegos estratégicos. Es clave incluirlos en el análisis de escenarios, aunque parezcan lejanos. La gestión de riesgos debe evolucionar hacia un modelo dinámico, con monitoreo continuo, análisis predictivo y gobernanza estratégica. Adoptar una visión prospectiva permite anticiparse, fortalecer la resiliencia y detectar oportunidades. Integrar esta disciplina en el ADN corporativo mejora la adaptación, sostenibilidad e innovación en entornos inciertos.

Riesgos emergentes en los próximos 5 años

Región ● Andina Norte ● Andina Sur ● Centroamérica y Caribe ● México



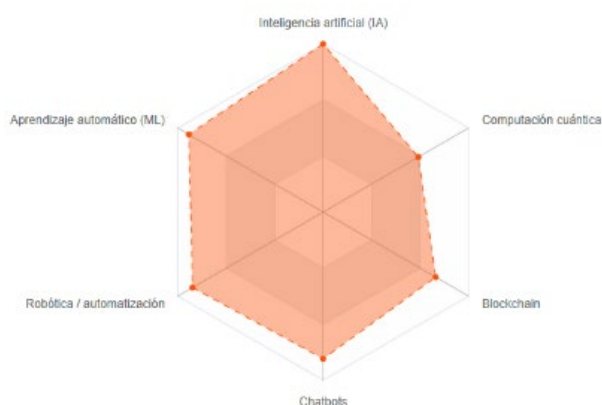
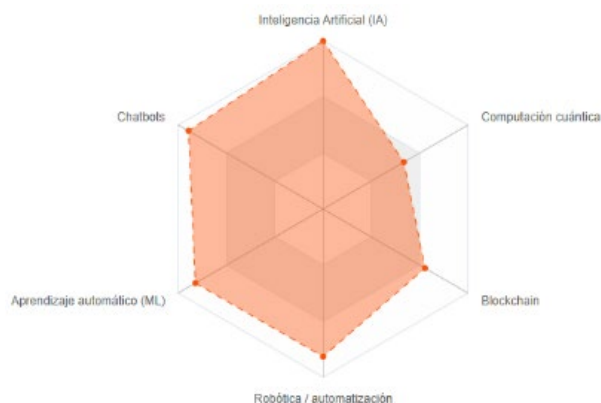
Total LATAM

La baja percepción de riesgo en temas fiscales (18–20%), demográficos (15%), y regulatorios —como el arbitraje (15–16%) y la fragmentación global (10–11%)— junto con la marginalidad de los asuntos antimonopolio (1%), revela un preocupante sesgo en la gestión de riesgos empresariales. Si bien estos factores pueden parecer menos urgentes frente a amenazas como la disrupción tecnológica o los riesgos climáticos, su potencial de impacto sistémico es alto, especialmente si se acelera la presión regulatoria o se intensifica la concentración de mercados. Las organizaciones deben evitar caer en la trampa de la inmediatez y adoptar una visión más equilibrada que incorpore estos riesgos estructurales en sus modelos de análisis prospectivo, para evitar sorpresas que comprometan la continuidad operativa o la viabilidad financiera.

Al segmentar los datos por región, se

observa que Centroamérica y el Caribe presentan los niveles más altos de preocupación en casi todas las categorías, seguidos por Andina Norte, mientras que Andina Sur y México muestran sensibilidades más bajas. Esta disparidad regional sugiere que la percepción de riesgo está influenciada por factores locales como la estabilidad política, la madurez institucional y la exposición a eventos disruptivos recientes. En consecuencia, las organizaciones deben ajustar sus estrategias de gestión de riesgos por país, reconociendo que una solución homogénea no es suficiente en un entorno tan diverso como el latinoamericano. La resiliencia empresarial exige una lectura contextualizada del entorno, que permita anticipar amenazas específicas y diseñar respuestas adaptadas a cada realidad operativa.

El ascenso de las capacidades tecnológicas en la Gestión de Riesgos



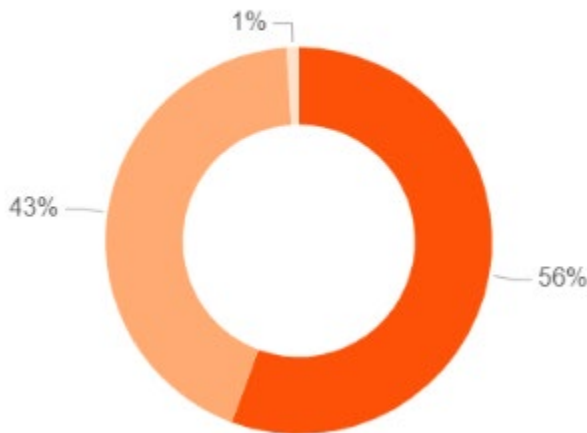
Nota: Los valores se ordenan automáticamente según la magnitud numérica de mayor a menor, por lo cual varía la posición de los ejes en ambos gráficos.

En el plazo de un año, las organizaciones apuestan por la IA, los chatbots, ML y automatización para lograr la eficiencia en sus procesos, mientras que el Blockchain y la computación cuántica siguen en fase exploratoria por madurez y regulación. La inteligencia artificial (IA) y los chatbots destacan por optimizar procesos como clasificación documental, due diligence y monitoreo de terceros, mejorando tanto tiempos como trazabilidad.

A tres años, se proyecta un desplazamiento del foco desde el front-end hacia capacidades de back-end más sofisticadas. La IA sigue siendo estratégica, pero gana protagonismo el ML y la automatización a escala (MLOps y flujos controlados), junto con mayor interés en blockchain y computación cuántica. Este panorama exige mayor integración con sistemas operativos, gobernanza más rigurosa y vuelve a los chatbots en interfaces estándar sin ventaja competitiva.

Robustez del sistema de gestión de riesgos operacionales y la inversión tecnológica para ayudar a su prevención

Estado ● Moderadamente robusto ● Muy robusto ● Poco robusto



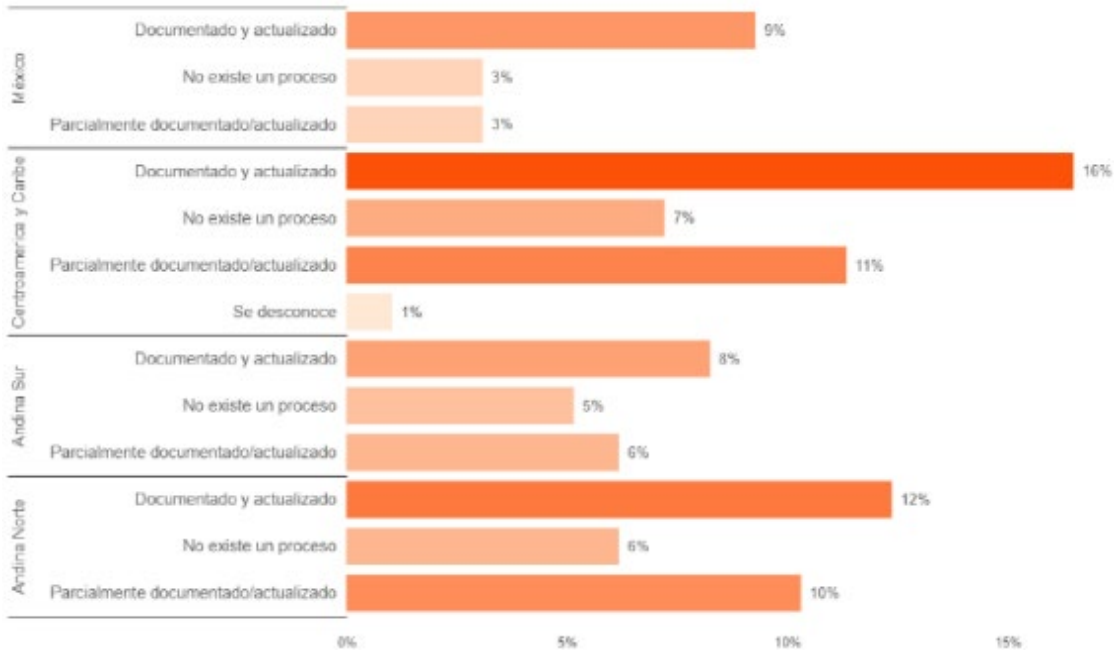
La resiliencia operativa sigue siendo una prioridad estratégica en entornos volátiles e inciertos. Disrupciones geopolíticas y ciberataques refuerzan la necesidad de estructuras sólidas para garantizar la continuidad del negocio. Los CRO la consideran el segundo tema más demandante, solo detrás de la ciberseguridad, lo que evidencia la urgencia de integrar ambos enfoques en una arquitectura de riesgos preventiva y adaptable. El sistema de gestión de riesgos muestra percepción positiva: 56% lo ve moderadamente robusto y 43% muy robusto. Sin embargo, persiste una brecha tecnológica: 37% usa sistemas avanzados, 54% básicos y 9% invierte poco o nada. Esto indica que, aunque hay control, falta escalar hacia monitoreo, automatización y protección más sofisticados.

La resiliencia debe evolucionar hacia un modelo dinámico que anticipe y se recupere de eventos adversos. Para cerrar la brecha, se requiere una estrategia que modernice sistemas con monitoreo en tiempo real, análisis predictivo y automatización. Además, fortalecer la gobernanza y alinear procesos con objetivos estratégicos. La resiliencia no depende solo de tecnología, sino también de liderazgo, cultura y visión compartida. Migrar de resiliencia media a alta exige transformación integral: capacitación, rediseño de procesos y métricas claras. Adoptar mejora continua convierte incidentes en oportunidades de aprendizaje. En un entorno interconectado y riesgoso, la resiliencia operativa es condición indispensable para la prosperidad empresarial.



Riesgos tecnológicos y de terceros

Gestión de riesgos de terceros y los retos tecnológicos que enfrenta



La madurez parcial (31%) refleja que, aunque hay prácticas, no están integradas en un ciclo completo ni se actualizan con la frecuencia necesaria ante cambios regulatorios u operativos. Esta falta de formalización aumenta el riesgo de incidentes, sobre todo con proveedores críticos en sectores sensibles. Para cerrar la brecha, se requiere un enfoque estructurado en la gestión de riesgos de terceros: documentar procesos, implementar monitoreo continuo, evaluaciones periódicas y trazabilidad. La gobernanza debe definir criterios claros de selección y supervisión, alineados con el apetito de riesgo y objetivos de sostenibilidad. Además, integrar herramientas tecnológicas para automatizar datos, generar alertas y facilitar decisiones basadas en evidencia.

22%

carece de cualquier tipo de proceso formal, revelando una brecha importante sobre la conciencia de riesgo y su gestión.

(Porcentaje total de Latam)

46%

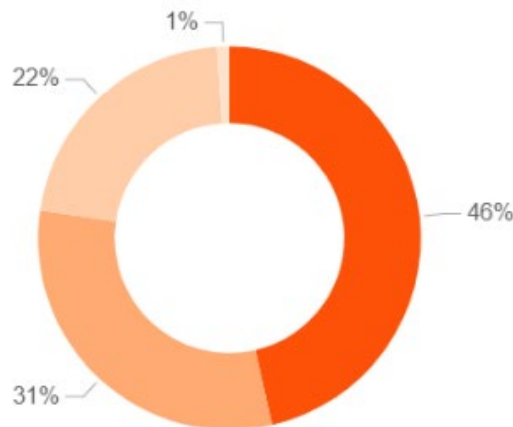
de entidades financieras cuentan con procesos documentados y actualizados.

(Porcentaje total de Latam)



Metodologías y procesos formales para reducir riesgos de terceras partes y capacidades para evaluar el riesgo de proveedores críticos

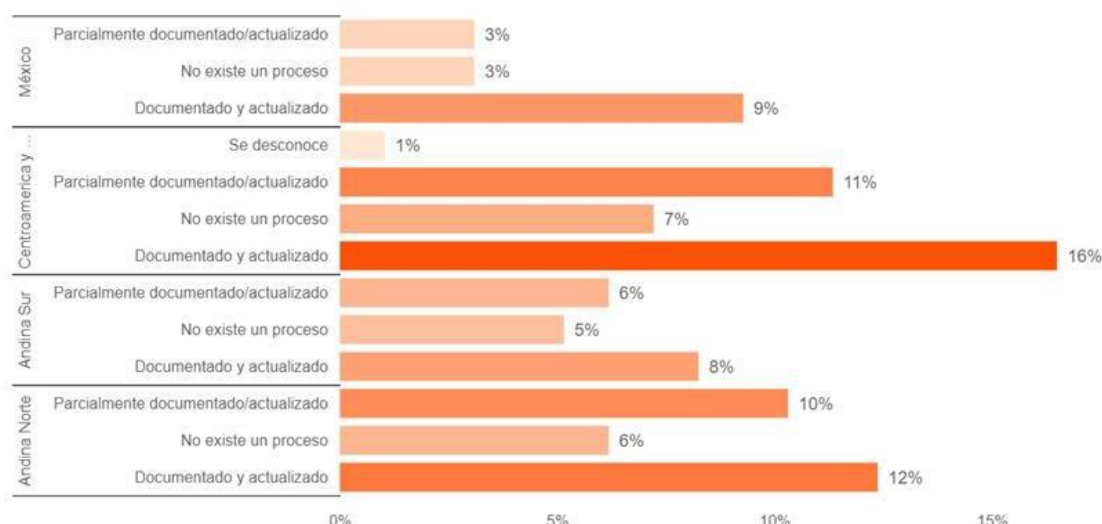
Estado ● Documentado y actualizado ● Parcialmente documentado/actualizado ● No existe un proceso ● Se desconoce



La evaluación del riesgo en proveedores críticos se encuentra en nivel intermedio (41%), lo que indica conciencia creciente pero falta de profundidad. Un 20% está inmaduro y 18% en nivel básico, aumentando la exposición en la cadena de suministro, mientras solo un 4% alcanza nivel avanzado. Esta disparidad genera vulnerabilidades operativas, regulatorias y reputacionales. Además, solo el 46% cuenta con procesos formales documentados, frente a 31%

parcialmente formalizados y 22% sin proceso, lo que refuerza la necesidad de fortalecer la gobernanza de la Gestión de Riesgos de Terceros (TPRM por sus siglas en inglés). Para cerrar la brecha, se requiere estandarizar metodologías, definir métricas, implementar monitoreo continuo y clasificar proveedores según criticidad, alineando Compras, Riesgos y TI para mejorar trazabilidad, respuesta y escalabilidad con eficiencia y resiliencia.

Nivel de madurez en la gestión de riesgos de terceros por cada región de América Latina



Centroamérica y Caribe. Presenta el mayor porcentaje de procesos “documentados y actualizados” (16%), toda vez que destaca por poseer el porcentaje más alto de procesos parcialmente documentados, lo cual revela un avance sostenido, aunque aún con espacio para formalización total. Asimismo, el porcentaje de desconocimiento es mínimo, lo cual denota consciencia generalizada sobre el estado de los procesos a nivel institucional. Los bancos de este subgrupo cuentan con una estructura más robusta de prácticas internas, lo que apunta a un recorrido de mejor gobernanza y mayor nivel de supervisión sobre terceros.

México. Muestra un bajo nivel de madurez general, pero con una ligera concentración en la categoría más alta (“documentado y actualizado”). Aunque el porcentaje es reducido,

sugiere que solo una minoría ha institucionalizado la gestión de riesgos de terceros. La igualdad entre quienes no tienen procesos establecidos y quienes lo tienen parcialmente indica que existe fragmentación y posiblemente diferencias significativas entre instituciones de dicha región. Así pues, México se ubica en una fase incipiente, con una alta dependencia de procesos no formalizados y una brecha relevante en estandarización.

Andina Sur. Muestra un equilibrio moderado entre los tres niveles de madurez, sin cifras elevadas hacia ninguno de los dos extremos. La mayor parte (8%) se sitúa en la categoría más alta, lo que sugiere progresos importantes, aunque todavía no tan avanzados como Centroamérica y Caribe. El 6% se ubica en un rango parcialmente documentado,

reflejando que la formalización está en marcha, pero no consolidada. Además, el 5% sin proceso es relativamente bajo, lo que señala cierta uniformidad inicial en la adopción. Andina Sur puede considerarse en un estado intermedio de madurez, con una tendencia positiva hacia la formalización, pero aún con brechas para garantizar consistencia y alineamiento regional.

Andina Norte. Exhibe una estructura similar a la encontrada en Andina Sur, pero con una proporción ligeramente superior en el nivel más alto, siendo que el 10% de procesos completamente documentados posiciona a esta región por encima de México y Andina Sur, pero no al nivel de Centroamérica y Caribe. La igualdad entre las categorías “sin proceso” y “parcialmente documentado” sugiere que coexisten organizaciones con prácticas muy maduras con otras totalmente rezagadas, lo cual constituye un signo de heterogeneidad para este subgrupo. En definitiva, se observa una madurez moderada–alta, con margen de mejora orientado a reducir las disparidades internas y aumentar la estandarización.

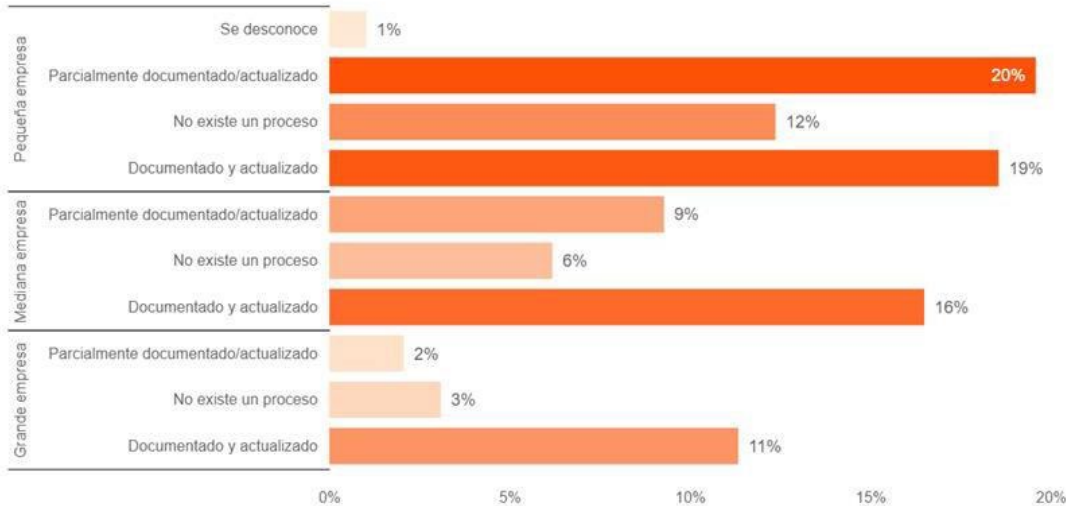
- En todas las regiones existe una combinación de organizaciones con procesos maduros y otras que todavía no disponen de ningún tipo de formalización.
- La categoría “no existe un proceso” sigue siendo visible en todas las regiones de América Latina (con un promedio entre 3% y 7%), lo que indica riesgos sistémicos y carencias de control consistentes en todos los países.
- El avance desde “parcialmente documentados” hacia “documentados y actualizados” es más notorio en Centroamérica y Caribe, apuntando a una mayor capacidad institucional y mejor gestión de riesgos.

El análisis regional evidencia una madurez heterogénea en la Gestión de Riesgos de Terceros: Centroamérica y Caribe lideran con mayor formalización, mientras México muestra rezagos importantes. Las regiones Andina Sur y Andina Norte presentan madurez intermedia, con avances en procesos, aunque aún deben fortalecer sus modelos de control para lograr mayor uniformidad.

Este contexto resalta la necesidad de impulsar la estandarización regional, robustecer el control interno y elevar la conciencia institucional sobre la relevancia del TPRM para mitigar riesgos operativos, reputacionales y regulatorios.



Nivel de madurez en la gestión de riesgos de terceros con base en el tamaño de la entidad financiera



Entidades pequeñas

Organizaciones ágiles que avanzaron en formalización (19%), pero con brechas de institucionalización: controles aún no estandarizados o no vigentes del ciclo completo de los procesos, dependencia de personas claves y heterogeneidad entre bancos.

Entidades medianas

Parecen representar el punto de mejor relación madurez–capacidad. La base “sin proceso” es baja y la transición hacia “documentado” ya está ocurriendo.

Entidades grandes

Cuentan con procesos, pero el salto a formalización “actualizada” es más costoso por complejidad (volumen de terceros, multi país, multi línea, sistemas legados, gobernanza matricial). Tienden a operar con políticas marco y controles “existentes”, pero no necesariamente uniformes ni vigentes en todo el ciclo funcional y en todas las geografías.

El nivel “documentado y actualizado” es más alto en bancos pequeños (19%) y desciende a 16% (medianos) y 11% (grandes), reflejando que la complejidad en organizaciones grandes ralentiza la actualización y homogeneización del TPRM.

La ausencia de procesos se reduce a medida que crece el tamaño (12% Pequeñas → 6% Medianas → 3% Grandes entidades), señal de que en aquellas de mayor tamaño existe TPRM, pero debe escalarse y estandarizarse.

La región debe cerrar la brecha de “parcial” a “actualizado” (especialmente en pequeñas) y estandarizar (especialmente en grandes), apoyándose en plataformas GRC/TPRM, contratación robusta y monitoreo continuo.

8

Ruta hacia la
transformación

¿Las organizaciones financieras están listas para cambiar la forma en que entienden la Gestión de Riesgos y el valor que tiene el análisis de datos?

Impulsar la transición hacia un modelo predictivo integral de identificación de riesgos representa un cambio de paradigma en la gestión empresarial. Este enfoque no solo implica el uso de análisis avanzado y herramientas de inteligencia artificial, sino también la consolidación de una cultura organizacional orientada a la anticipación. La vigilancia externa — incluyendo señales del entorno competitivo, regulatorio y social — debe integrarse como fuente clave para alimentar modelos de riesgo dinámicos. Las organizaciones que logren combinar capacidades analíticas con sensibilidad estratégica estarán mejor posicionadas para detectar amenazas emergentes, modelar escenarios complejos y tomar decisiones informadas con mayor agilidad.

Actualizar y comunicar frecuentemente las políticas y planes de riesgos es esencial para mantener la coherencia entre la estrategia corporativa y la operación diaria. La transparencia en estos procesos fortalece la confianza interna, promueve la rendición de cuentas y facilita la participación de todos los niveles organizacionales.

Desde el comité ejecutivo hasta los equipos operativos, cada actor debe comprender su rol en la gestión de riesgos. Esta alineación requiere canales de comunicación efectivos, ciclos de revisión periódicos y una gobernanza clara que permita adaptar los planes de riesgo a los cambios del entorno sin perder trazabilidad ni control.

Implementar programas robustos de capacitación multidisciplinaria es un pilar fundamental para elevar la madurez organizacional en gestión de riesgos.

Estos programas deben abordar no solo aspectos financieros y normativos, sino también dimensiones conductuales, tecnológicas y éticas. La formación continua permite que los equipos desarrollen criterio profesional, capacidad de análisis y habilidades para operar en entornos inciertos. Además, fomenta una cultura de riesgo compartida, donde el conocimiento no se concentra en áreas especializadas, sino que se distribuye estratégicamente para fortalecer la resiliencia organizacional.

Incorporar herramientas y marcos para la cuantificación y gestión de riesgos no tradicionales — como los relacionados con sostenibilidad (ASG) y conducta— es una necesidad creciente en el entorno empresarial actual. Estos riesgos, aunque menos tangibles, tienen impactos significativos en la reputación, el acceso a capital y la licencia social para operar. La gestión efectiva de riesgos ASG requiere métricas claras, modelos de evaluación integrados y una gobernanza que vincule estos factores con los objetivos estratégicos. Las organizaciones que logren integrar estos riesgos en sus sistemas de control estarán mejor preparadas para responder a las expectativas de inversionistas, reguladores y consumidores.

Fortalecer la arquitectura tecnológica para la gestión de riesgos cibernéticos y digitales es otro frente prioritario. En un entorno donde las amenazas digitales evolucionan constantemente, contar con sistemas resilientes, adaptables y alineados con las normativas vigentes es indispensable. Esto implica invertir en infraestructura segura, automatizar procesos de detección y respuesta, y establecer protocolos claros de recuperación ante incidentes. Además, la ciber gobernanza debe ser transversal, involucrando a áreas como TI, riesgos, cumplimiento y auditoría, para garantizar una protección integral de los activos digitales y la continuidad

operativa.

Definir e impulsar programas claros para el abordaje de riesgos de terceros y proveedores es clave para proteger la cadena de valor. La creciente dependencia de socios externos exige una gestión rigurosa que incluya procesos de evaluación, monitoreo y clasificación según criticidad. La alineación entre Compras, Riesgos y TI bajo responsabilidades definidas permite una supervisión más efectiva y una respuesta coordinada ante incidentes. Además, la trazabilidad de decisiones y la transparencia en la relación con terceros fortalecen la reputación corporativa y reducen la exposición a riesgos operativos, legales y reputacionales.

Finalmente, desarrollar e implementar políticas y prácticas para la adopción segura y ética de tecnologías emergentes —especialmente IA y automatización— es una responsabilidad estratégica. Estas tecnologías ofrecen enormes oportunidades, pero también plantean riesgos asociados a sesgos algorítmicos, pérdida de control y desafíos regulatorios. La adopción responsable implica establecer marcos éticos, validar modelos con intervención humana y asegurar que las decisiones automatizadas estén alineadas con los valores corporativos. En última instancia, la tecnología debe ser un habilitador de valor, no una fuente de vulnerabilidad.





¿Cuáles son las acciones claves para empezar a transitar la ruta de la transformación financiera en Gestión de Riesgos y Analítica de Datos?

Laboratorios de Riesgos Predictivos 360°

La creación de espacios colaborativos internos como laboratorios de riesgos predictivos representa una evolución en la forma en que las organizaciones abordan la anticipación estratégica. Estos entornos deben reunir equipos multidisciplinarios —riesgos, datos, tecnología, operaciones y cultura— para desarrollar habilidades de detección temprana, combinando análisis avanzado con inteligencia contextual. La clave está en integrar la vigilancia externa (tendencias, señales débiles, cambios regulatorios) con la cultura organizacional, para construir modelos de riesgo dinámicos que permitan identificar amenazas emergentes antes

de que se materialicen. Estos laboratorios no solo fortalecen la resiliencia, sino que posicionan a la organización como líder en gestión proactiva.

Programa de Cultura GRC

Insertarse con otros grupos de Gobierno, Riesgo y Cumplimiento (GRC) y establecer un programa de comunicaciones internas es esencial para democratizar el conocimiento de riesgos. Mensajes breves, visuales y accionables permiten que los colaboradores comprendan los elementos clave de control, gobernanza y cumplimiento sin saturación técnica. Este enfoque promueve una cultura de riesgo transversal, donde cada área entiende su rol en la protección del negocio. Además, al vincular la comunicación con valores

corporativos y casos reales, se refuerza el compromiso ético y se facilita la adopción de buenas prácticas en todos los niveles jerárquicos.

Academias inmersivas de riesgos y datos

Diseñar academias inmersivas que combinen simulaciones reales con retos colaborativos es una estrategia poderosa para fortalecer el aprendizaje multidisciplinario. Estas experiencias deben integrar riesgos financieros, conductuales y tecnológicos, permitiendo que los colaboradores vivan escenarios complejos y tomen decisiones bajo presión. El seguimiento de métricas de desempeño en estos entornos facilita la retroalimentación y el desarrollo de competencias críticas. Además, al fomentar la colaboración entre áreas, se rompe el paradigma de gestión aislada y se promueve una visión sistémica del riesgo, alineada con los objetivos estratégicos de la organización.

Métricas en riesgos No financieros

La implementación de talleres segmentados para líderes y staff orientados a desarrollar indicadores vivos en riesgos ASG (ambientales, sociales y de gobernanza) es clave para avanzar hacia una

gestión más responsable. Estos indicadores deben ser dinámicos, adaptables y vinculados a conductas sostenibles y decisiones éticas. La cuantificación de riesgos no financieros permite visibilizar impactos que tradicionalmente han sido subestimados, como la reputación, la inclusión o el cambio climático. Al integrar estas métricas en los tableros de control, se fortalece la toma de decisiones informada y se alinean los valores corporativos con la estrategia de negocio.

Simuladores de resiliencia cibernética

Desarrollar entornos virtuales que repliquen la arquitectura tecnológica de la organización para simular ataques y fallos es una práctica avanzada de preparación operativa. Estos simuladores permiten evaluar la capacidad de respuesta ante amenazas digitales, validar protocolos de recuperación y adaptar los sistemas a normativas emergentes. Además, fomentan la colaboración entre TI, riesgos y cumplimiento, generando una cultura de ciber resiliencia que trasciende lo técnico. La simulación periódica de escenarios críticos fortalece la confianza institucional y permite identificar vulnerabilidades antes de que se conviertan en incidentes reales.





Programas trusted chain para terceros

La creación de una certificación interna para proveedores y terceros basada en criterios de riesgo, cumplimiento y sostenibilidad es una herramienta estratégica para blindar la cadena de valor. Este programa debe incluir procesos de evaluación colaborativa, monitoreo continuo y retroalimentación transparente. Al establecer estándares claros y alineados con los valores corporativos, se promueve una relación más sólida y confiable con los socios externos. Además, se reduce la exposición a riesgos operativos, legales y reputacionales, y se fortalece la trazabilidad en toda la cadena de suministro.

Sellos de ética digital para tecnologías emergentes

Establecer un sello corporativo que valide la adopción segura y ética de tecnologías como IA y automatización es una iniciativa de vanguardia. Este sello debe evaluar riesgos de privacidad, transparencia, sesgos algorítmicos y cumplimiento normativo antes de la implementación. Al institucionalizar este proceso, la organización demuestra su compromiso con la innovación responsable y la protección de sus stakeholders. Además, este enfoque permite anticipar impactos no deseados, fortalecer la gobernanza tecnológica y posicionar a la empresa como referente en ética digital en un entorno cada vez más automatizado.



Let's talk



Bismark Rodríguez

Socio Líder Regional de Consultoría,
PwC Interaméricas
bismark.rodriguez@pwc.com



Susana Pino

Socia Líder Regional de Risk
Assurance Services (RAS),
PwC Interaméricas
pino.susana@pwc.com