ESTUDIO

Gestión de Riesgos en Latinoamérica 2025

pirani

ÍNDICE

INTRODUCCIÓN

La gestión de riesgos se ha convertido en un área transversal para cualquier empresa, sin importar su tamaño o el sector al que pertenezca. Más allá de cumplir con las normativas correspondientes, las organizaciones han comprendido que identificar y gestionar sus riesgos es importante para proteger su operación, fortalecer su relación con los grupos de interés y asegurar su sostenibilidad a largo plazo. Esto no sólo las ayuda a mantener el rumbo frente a desafíos, sino que también les permite generar valor y aprovechar oportunidades para su crecimiento.

El concepto de riesgos ha evolucionado significativamente. Ya no se limita a eventos aislados que puedan afectar la continuidad operativa de una organización, sino que abarca un espectro más amplio, que incluye factores internos y externos con el potencial de impactar todas las áreas del negocio. Esto ha llevado a que la gestión de riesgos no sólo sea una obligación regulatoria, sino también una estrategia clave para anticiparse a escenarios adversos, proteger los activos críticos y, en última instancia, construir una ventaja competitiva sostenible.

Comprender los riesgos implica reconocer su naturaleza cambiante y multifacética. No todos los riesgos son iguales; algunos son los conocidos pueden ser gestionados de manera estructurada, mientras que otros emergen con poca advertencia y traen consigo una complejidad inédita. Esta clasificación es importante para desarrollar estrategias efectivas de prevención y mitigación.

En cuanto a los tipos de riesgos, estos pueden dividirse en dos grandes categorías. Por un lado, están los **riesgos tradicionales**, aquellos que la mayoría de empresas conoce y gestiona de manera frecuente. Este grupo incluye riesgos financieros, riesgos operativos relacionados con el cumplimiento normativo y los cambios regulatorios.

Por otro lado, están los **riesgos emergentes**, que son menos predecibles y más difíciles de cuantificar tanto en impacto como en probabilidad de ocurrencia. Dentro de esta categoría encontramos los riesgos asociados al cambio climático, que pueden ser físicos o de transición, así como los riesgos sociales. También destacan los riesgos de ciberseguridad, que, aunque no son completamente nuevos, han evolucionado significativamente con el avance de las tecnologías, presentando desafíos cada vez más complejos y difíciles de anticipar.

Por quinto año consecutivo en Pirani, quisimos conocer y entender cuáles son los riesgos actuales más importantes a los que se enfrentan las organizaciones en Latinoamérica, además de esto, el propósito de nuestro **Estudio de Gestión de Riesgos 2025**, es compartir conocimiento y brindar herramientas que ayuden a los profesionales de riesgos a enfrentar y gestionarlos de una mejor manera, teniendo en cuenta que, los riesgos son dinámicos y están en constante evolución.

Por eso, es importante mantenerse **actualizados en tendencias y buenas prácticas** para estar preparados ante los diferentes escenarios de riesgos que se pueden presentar.

Las empresas en 2025 se enfrentarán a grandes desafíos como la inteligencia artificial, la automatización y el cambio climático

Para el 2025, inteligencia artificial, automatización, cambio climático y cambios regulatorios son las principales dificultades a las que se enfrentan las empresas según los participantes y expertos entrevistados para este estudio.

La falta de cultura de riesgos, ciberseguridad, protección de datos, fraude, corrupción y delitos financieros; y cambio regulatorio, cumplimiento normativo y la incertidumbre macroeconómica y geopolitica lideran la lista de los retos más grandes, estos también serán importantes para las organizaciones de la región en este 2025.

En esta edición del **Estudio de Gestión de Riesgos en Latinoamérica**, conocerás información relevante sobre los principales riesgos a gestionar y recomendaciones de expertos para **fortalecer la cultura de riesgos**, una de las molestias principales de nuestros encuestados. Esta falta de cultura de riesgos, una vez más prevalece como el principal reto de las áreas de gestión de riesgos.

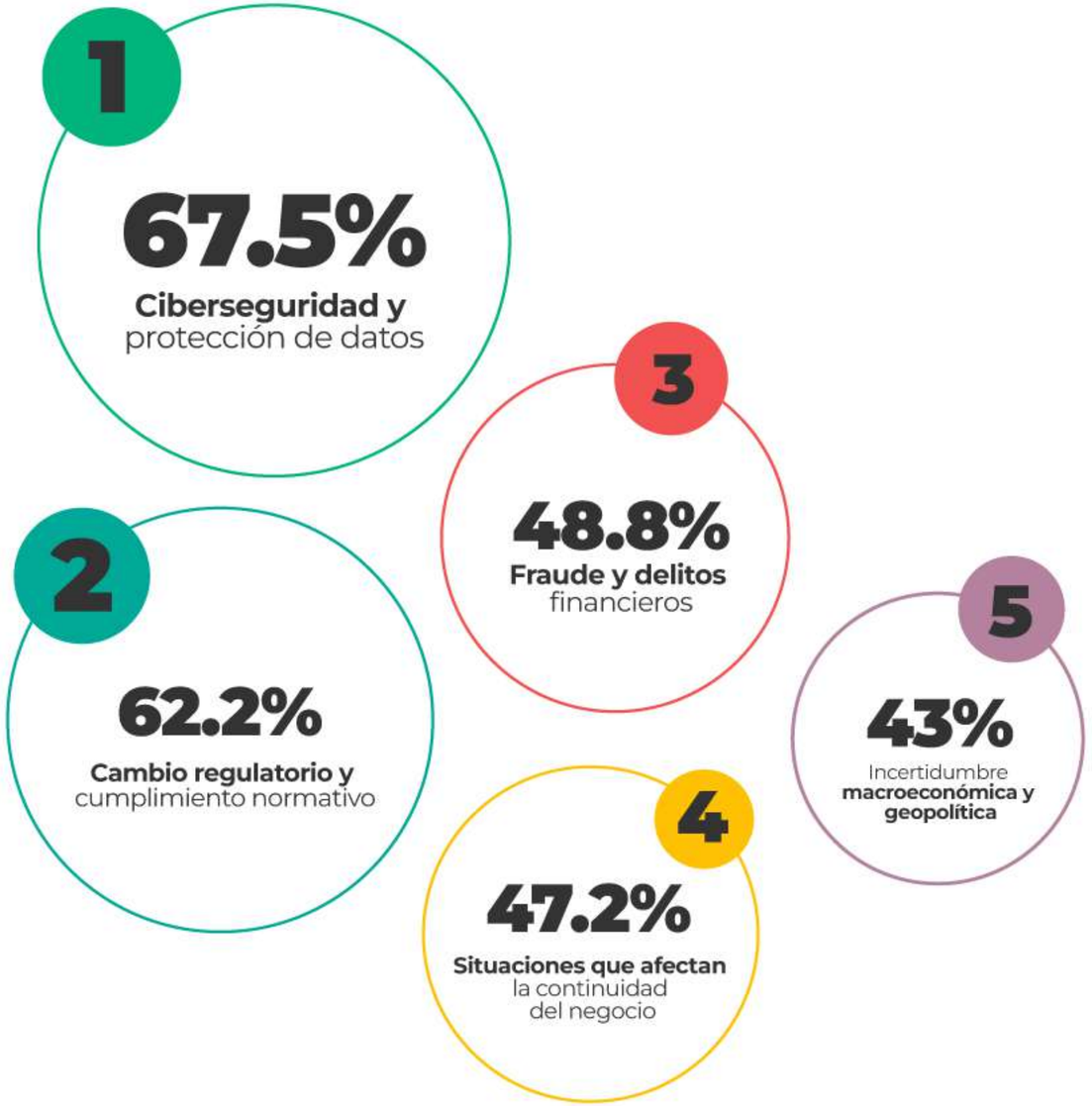
Por último, como novedad de este año, en nuestro **Estudio de Gestión de Riesgos** incluimos los principales riesgos relacionados con **Inteligencia Artificial (IA)** que será de mucha utilidad para estar preparados, antes, durante y después de todos los procesos en los que se requiera el uso de estas nuevas herramientas tecnológicas.

RESULTADOS DEL ESTUDIO 2025

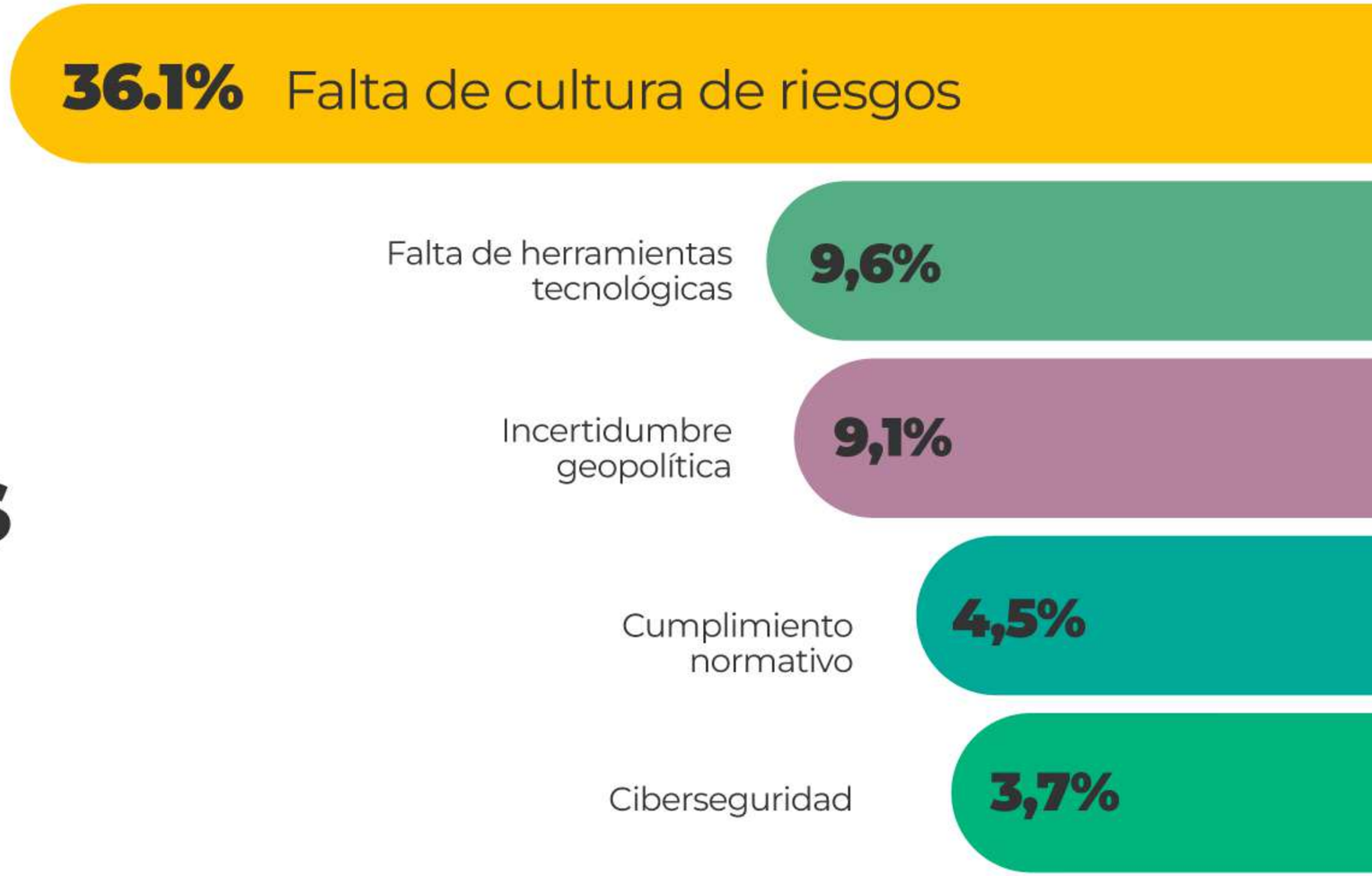
En esta quinta edición del **Estudio de Gestión de Riesgos en Latinoamérica,** que realizamos en Pirani, participaron 530 personas de más de 15 países de la región de diferentes industrias.

A través de una encuesta virtual que respondieron, pudimos conocer entre otros datos, los riesgos más importantes que tienen en gestión de riesgos.

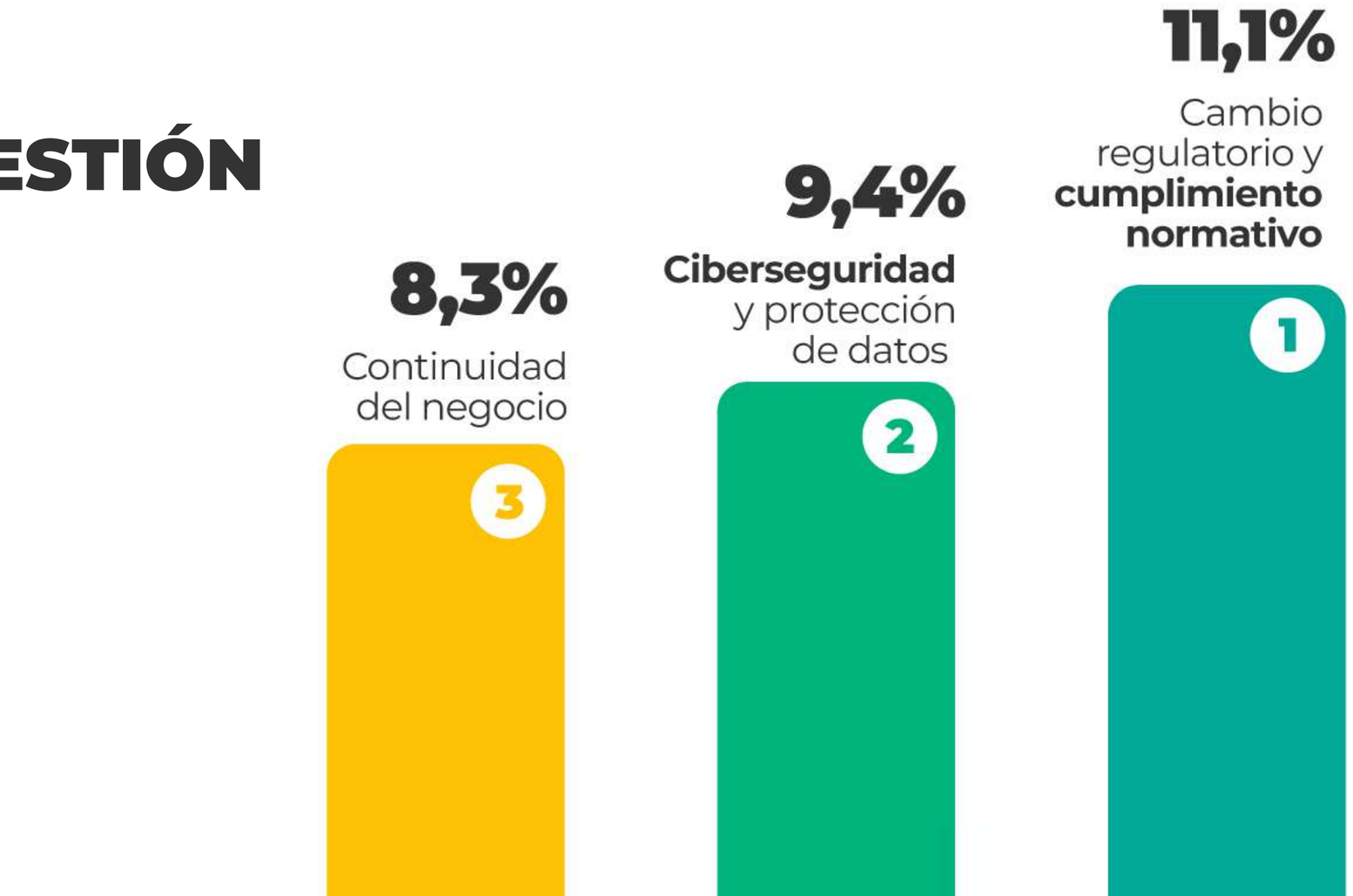
TOP 5 RIESGOS PARA EL 2025



TOP 5 DIFICULTADES ACTUALES



TOP 3
RETOS EN GESTIÓN DE RIESGOS
PARA EL 2025



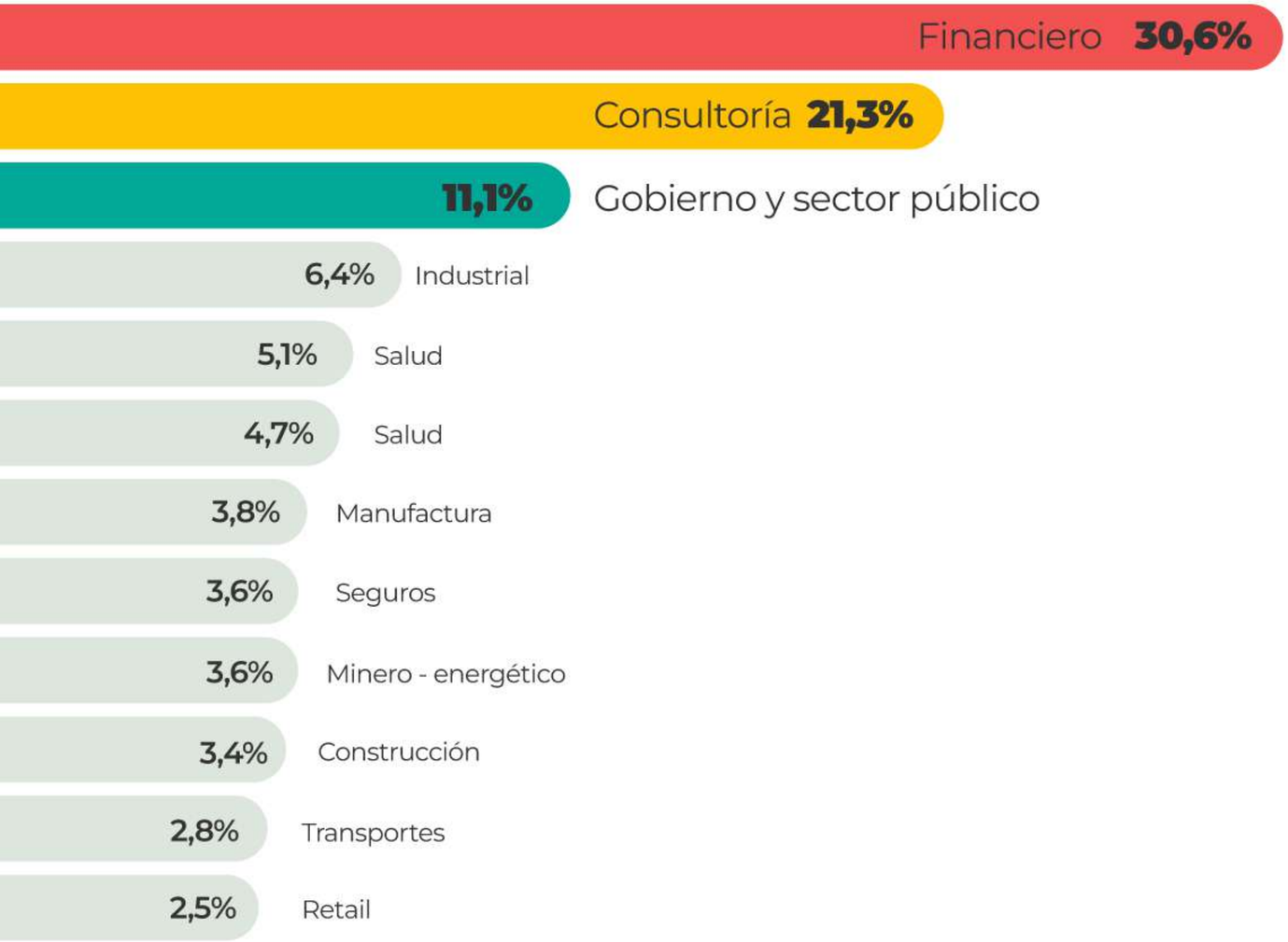
METODOLOGÍA

SOBRE LOS PARTICIPANTES Y LAS ORGANIZACIONES

a. País de los participantes

Los 530 participantes que respondieron la encuesta virtual del **Estudio de Gestión de Riesgos en Latinoamérica 2025**

COLOMBIA, MÉXICO Y PERÚ FUERON LOS PAÍSES CON MÁS **NÚMERO DE PARTICIPANTES**



GRÁFICA: ¿A qué sector pertenece tu empresa?

b. Sector industrial

El sector financiero (30,6%) es el principal sector industrial al que pertenecen las organizaciones donde trabajan los participantes de este estudio.

OTROS SECTORES DESTACADOS FUERON: CONSULTORÍA, GOBIERNO Y SECTOR PÚBLICO E INDUSTRIAL.

c. Importancia de la gestión de riesgos

48,1%

Muy importante en sus organizaciones

El 48,1% de los participantes asegura que **la gestión de riesgos es muy importante en sus organizaciones**, consideran que es un área estratégica para el logro de los objetivos organizacionales y la continuidad de los negocios.

42,1%

Importante en sus organizaciones

El 42,1% de los encuestados dice que **la gestión de riesgos es importante,** sin embargo, consideran que en sus organizaciones hace falta mayor compromiso por parte de todos los colaboradores.

8,7%

Área poco importante

Finalmente, el 8,7% manifiesta que **la gestión de riesgos en sus organizaciones es un área poco importante** y que la mayoría de empleados ni la comprende ni le da el valor que tiene.

RIESGOS MÁS IMPORTANTES PARA LAS ORGANIZACIONES EN LATINOAMÉRICA

RECUENTO DE LOS RIESGOS MÁS IMPORTANTES

Por tercer año consecutivo, **ciberseguridad y protección de datos es el riesgo más importante** para las organizaciones latinoamericanas

El riesgo de fraude, corrupción y otros delitos financieros está en el segundo lugar, cambio regulatorio y cumplimiento normativo es el tercer riesgo este año, le siguen continuidad de negocio y riesgos financieros, según los participantes de este **Estudio de Gestión de Riesgos en Latinoamérica 2025**

1. Ciberseguridad y protección de datos

67,5%

DE LAS RESPUESTAS, SIGUE SIENDO EL PRINCIPAL RIESGO PARA LAS ORGANIZACIONES.

Con el 67,5% de las respuestas, se mantiene en el primer lugar de los riesgos más importantes para las organizaciones. Según los expertos, este riesgo seguirá creciendo por mucho más tiempo, sobre todo en un contexto en el que la Inteligencia Artificial (IA) está tan implementada en las labores cotidianas de las empresas, pero para lograr un equilibrio, los usuarios deben tener un conocimiento sobre las buenas prácticas al usar esta herramienta. Según Jean Paul Heymans, consultor en ciberseguridad:

“La gente, en la mayoría de las organizaciones ya ha estado expuesta a algún tipo de simulación de phishing, y al entrenamiento de buenas prácticas, pero muchas veces la barrera para llevar esos conocimientos a la práctica es no verlo como un escenario real. Entender que todos estamos expuestos a ser víctimas y el impacto de algo tan sencillo como hacer un clic malicioso puede ser gigantesco en la empresa”

Otro factor importante para que la ciberseguridad, se mantenga como uno de los principales riesgos, es como lo explica Esperanza Hernandez, representante legal de HC Gestión: “El robo de datos es algo muy frecuente y las interrupciones en los sistemas a causa de esto” es por esa razón que las organizaciones deben seguir implementando y actualizando sus controles para evitar estos riesgos.

La ciberseguridad, es el principal riesgo a nivel mundial, te presentamos diferentes situaciones que pueden ayudar a entender el por qué:

- **Fortalecimiento de la ciberseguridad**
- **Ataques más profesionales, complejos y sofisticados**
- **Falta de conocimiento y concientización del personal**
- **Nuevos retos: regulación y privacidad de datos**

Fortalecimiento de la ciberseguridad

Estamos en un contexto en el que las empresas están migrando su información a servicios en la nube, esto, aunado a la transformación digital ha redefinido el perímetro digital de las organizaciones, generando nuevos desafíos para proteger los activos digitales. Según Jean Paul Heymans, consultor en sistemas de gestión de seguridad de la información (ISMS) “el cambio hacia modelos de servicio en la nube requiere controles más orientados a la gestión de identidades y configuraciones, debido a que los controles tradicionales pierden efectividad en estos entornos ampliados” Este cambio no sólo implica una adaptación tecnológica, sino también la implementación de esquemas de responsabilidad compartida, especialmente importantes en un terreno donde “los datos empresariales muchas veces se alojan en servicios cuyos términos de uso y medidas de seguridad son opacos para los equipos internos” asegura Heymans.

Por su parte, Carlos Clavel, experto en ciberseguridad, advierte que la migración masiva a la nube también trae riesgos asociados a la tercerización. “Es fundamental revisar los contratos y exigir reportes de cumplimiento como SOC 2 para asegurarnos de que los proveedores cuenten con medidas de seguridad internas sólidas”. Este contexto refleja cómo las organizaciones deben evolucionar sus estrategias de gestión de riesgos para adaptarse a un perímetro cada vez más complejo y menos definido.

Ataques más profesionales, complejos y sofisticados

La ciberdelincuencia evoluciona a una velocidad alarmante, con estrategias cada vez más avanzadas. Heymans destaca como la inteligencia artificial se ha convertido en un arma de doble filo: “Mientras enriquece las capacidades de los analistas, también permite a los atacantes crear campañas más complejas que explotan las vulnerabilidades en modelos de decisión”. Por ejemplo, los ataques de inyección de prompts en sistemas de IA muestran cómo estas tecnologías pueden ser manipuladas para realizar acciones no deseadas.

Carlos Clavel añade que la creciente dependencia de modelos como SaaS e IaaS introduce nuevas amenazas: “La tercerización de servicios incrementa los riesgos si no sabemos dónde están nuestros datos ni cómo los protegen los proveedores”. Este panorama subraya la importancia de implementar controles adaptativos que mitiguen riesgos en entornos híbridos y distribuidos.

Falta de conocimiento y concientización del personal

La concientización del personal sigue siendo el eslabón más débil en la cadena de seguridad. Según Heymans, es crucial que los empleados dejen de subestimar las amenazas: “Muchas organizaciones aún operan bajo la creencia de ‘A nosotros eso no nos va pasar’. Cambiar esta mentalidad es clave para reducir errores humanos”. Por su parte, Clavel enfatiza que el análisis de riesgos debe ser preventivo y no reactivo: “Si no sabes qué tienes ni hacia dónde vas, ninguna estrategia de capacitación funcionará”. Este enfoque proactivo requiere simulaciones realistas, entrenamientos continuos y políticas claras que permeen a todos los niveles organizativos.

Nuevos retos: regulación y privacidad de datos

Un punto crítico adicional es la creciente regulación en torno a la privacidad de los datos. Heymans menciona que “La regulación emergente, similar a la GDPR en Europa, está marcando el camino para una mayor protección de la información personal y corporativa”: Esto, combinado con la falta de visibilidad sobre cómo se manejan los datos en la nube, incrementa los riesgos de incumplimiento y exposición.

Clavel sugiere que las empresas deben anticiparse a estas normativas fortaleciendo sus análisis de riesgo: “Los controles deben ser lo suficientemente flexibles para adaptarse a cambios regulatorios mientras garantiza la continuidad operativa”.

¿Cómo prevenir este riesgo?

El panorama de ciberseguridad para 2025 estará definido por la transformación digital, la migración masiva a la nube, la evolución de los ciberataques y la creciente presión regulatoria. Tanto Heymans como Clavel coinciden en que la preparación y la planificación estratégica son las mejores herramientas para enfrentar estos desafíos. Esto implica:

1. Promover una cultura de ciberseguridad

Capacitar continuamente a todos los colaboradores es esencial para reducir el riesgo de errores humanos, responsables de la mayoría de las brechas de seguridad. La concienciación constante ayuda a prevenir incidentes, especialmente en entornos donde las amenazas evolucionan rápidamente.

2. Asignar responsabilidades claras

Designar un encargado de seguridad de la información, ya sea un equipo dedicado o una persona capacitada, asegura una respuesta coordinada ante riesgos. Este rol debe contar con el respaldo de la alta dirección para establecer políticas claras y fomentar la seguridad como prioridad organizacional.

3. Adaptar estándares internacionales

Guiarse por normas reconocidas, como ISO 27001 o el marco NIST, garantiza un enfoque estructurado y alineado con las mejores prácticas globales. Implementar esas políticas asegura una gestión adecuada de activos de información y controles efectivos.

4. Evaluar y gestionar los riesgos regularmente

El análisis periódico de los activos digitales y los posibles riesgos asociados permite priorizar acciones de mitigación. Además, contar con un plan de continuidad y recuperación asegura que las operaciones críticas puedan restablecerse rápidamente tras un ataque. Según “Cyber Risk Management” de Ariel Evans [1], un enfoque basado en riesgos es esencial para tomar decisiones estratégicas informadas.

5. Realizar pruebas de vulnerabilidad

Incluir evaluaciones como hacking ético o pruebas de penetración ayuda a identificar puntos débiles en sistemas, redes y aplicaciones. Esto permite corregir fallas antes de que puedan ser explotadas por actores maliciosos.

6. Mantener los sistemas actualizados

Actualizar regularmente software y hardware es importante para cerrar vulnerabilidades conocidas. Según “Practical Cybersecurity Architecture” de Ed Moyle y Diana Kelley [2], los ataques suelen aprovechar fallas en sistemas desactualizados, por lo que la actualización continua es un pilar básico de la prevención.

La ciberseguridad no es sólo una cuestión técnica; es un compromiso organizacional que, como señala Heymans, requiere “un enfoque integral y adaptativo que combina tecnología, procesos y persianas”.

1.Routledge. *Managing Cyber Risk, Ariel Evans*

2. Packt Publishing. *Practical Cybersecutiry Architecture, Ed Moyley, Diana KelleyLa ciberseguridad*

“La preparación es clave para reaccionar mejor ante incidentes. Inicia con pasos simples, como definir un equipo de respuesta y establecer quién dará la voz de alarma en los procesos de wardroom.” **Jean Paul Heymans**

2. Cambio regulatorio y cumplimiento normativo

62,2%

DE LOS ENCUESTADOS CONSIDERA QUE ESTE RIESGO ES UNO DE LOS MÁS IMPORTANTES PARA **ENFRENTAR EN EL 2025.**

Según Mariano López, jefe de cumplimiento y gestión integrada en la fundación ArgenINTA, “En latinoamérica, el principal riesgo está relacionado con las modificaciones en las reglas y legislaciones generadas por los cambios de gobiernos y autoridades, que pueden llevar a afectar los bienes y servicios que ofrecen las organizaciones y cómo los comercializan”

Sumado a esto la constante evolución de las normativas y el aumento de regulaciones complejas han convertido el cumplimiento normativo en un desafío crucial para las organizaciones. Además de las posibles sanciones legales y económicas, el incumplimiento puede impactar negativamente en la reputación y continuidad operativa.

¿Cómo prevenir este riesgo?

1. **Monitorear proactivamente el entorno regulatorio**
2. **Fortalecer la cultura organizacional de cumplimiento**
3. **Adoptar tecnología para automatizar el cumplimiento**
4. **Realizar análisis de contextos internos y externos**
5. **Capacitar a los equipos en temas de cumplimiento**
6. **Gestionar los riesgos regulatorios con una visión integral**
7. **Diversificar proveedores y clientes**

¿Cómo prevenir este riesgo?

1 Monitorear proactivamente el entorno regulatorio

La vigilancia continua de los cambios normativos es fundamental. Pablo Camacho destaca que “las regulaciones están en constante evolución y su incumplimiento puede ser costoso y complejo para las entidades”. Las organizaciones deben anticiparse a estas modificaciones con un monitoreo activo y contar con equipos especializados en compliance que analicen el impacto de cada regulación en todas las áreas. seguridad como prioridad organizacional.

2 Fortalecer la cultura organizacional de cumplimiento

Más allá de cumplir con normativas, las empresas deben desarrollar una cultura sólida basada en ética y responsabilidad. Según Mariano López, es importante integrar criterios ASG (ambientales, sociales y de gobernanza) en las estrategias de riesgos, ya que esto no sólo mitiga riesgos regulatorios, sino que también mejora la reputación ante stakeholders y fomenta la sostenibilidad operativa.

3 Adoptar tecnología para automatizar el cumplimiento

Implementar soluciones tecnológicas, como un software de gestión de riesgos que ayude a manejar grandes volúmenes de datos y a cumplir con normativas complejas de manera eficiente. Camacho resalta que “la automatización puede aliviar la carga operativa, pero siempre debe complementarse con supervisión humana”.

4 Realizar análisis de contextos internos y externos

López subraya que “analizar los cambios en los contextos internos y externos permite tomar medidas preventivas y mantener la continuidad del negocio”. Este enfoque holístico ayuda a las organizaciones a prepararse frente a factores como cambios políticos, económicos o climáticos, que afectan directa e indirectamente el cumplimiento normativa.

5 Capacitar a los equipos en temas de cumplimiento

La formación continua en normativas y buenas prácticas permite que los colaboradores apliquen principios de compliance en sus tareas diarias. Camacho recomienda integrar simulaciones y casos prácticos para que el aprendizaje sea aplicado y efectivo.

6 Gestionar los riesgos regulatorios con una visión integral

Para López, “la gestión de riesgos debe incluir planificación de escenarios y medidas preventivas”. Esto implica priorizar sectores clave como tecnología, finanzas y energía, que enfrentan una mayor presión normativa, y trabajar en estrategias que combinen resiliencia operativa con cumplimiento normativo.

7 Diversificar proveedores y clientes

Evitar dependencias excesivas reduce riesgos asociados a la cadena de suministro, como destaca Camacho: “las empresas deben buscar diversificación para mitigar interrupciones en sus operaciones causadas por eventos externos, como desastres naturales o conflictos políticos”.

El cambio regulatorio y el cumplimiento normativo son riesgos que requieren una gestión proactiva y multidisciplinaria. Adoptar estas estrategias no sólo garantiza el cumplimiento legal, sino que también refuerza la reputación y sostenibilidad de las organizaciones en un entorno dinámico.

> ***“Las empresas deben buscar diversificación para mitigar interrupciones en sus operaciones causadas por eventos externos, como desastres naturales o conflictos políticos”***
> **Mariano López**

3. Fraude y delitos financieros

48,8%

DE LOS ENCUESTADOS, LO UBICAN COMO UNO DE LOS RIESGOS A LOS QUE SE LES DEBERÍA PRESTAR ATENCIÓN POR LAS **EMPRESAS DE LATINOAMÉRICA EN EL 2025**

El fraude, tanto interno como externo, sigue siendo uno de los mayores riesgos operativos para las organizaciones, con graves impactos financieros y reputacionales. Este riesgo, exacerbado por la creciente digitalización y la hiperconectividad, requiere una gestión proactiva e integral que involucre tecnología avanzada controles robustos y un entendimiento profundo del comportamiento humano,

El fraude no sólo representa una amenaza económica, sino que también pone en riesgo la confianza que stakeholders, clientes y empleados depositan en las organizaciones. En un entorno donde la digitalización y la hiperconectividad aumentan las oportunidades para actividades fraudulentas, resulta esencial abordar este desafío con estrategias modernas que combinan tecnología avanzada y una gestión humana eficaz.

Además, el panorama regulatorio y la rápida evolución de las herramientas tecnológicas obligan a las empresas a adaptarse continuamente para mitigar este riesgo. Implementar controles efectivos y fomentar una cultura organizacional basada en la ética no sólo reduce la incidencia de fraudes, sino que refuerza la sostenibilidad operativa en el largo plazo.

¿Cómo prevenir este riesgo?

1 Fortalecer la cultura organizacional

El fraude no es solo un fenómeno económico; tiene raíces comportamentales: Marta Cadavid, reconocida experta en AML enfatiza que “el fraude surge desde el ser”, lo que subraya la importancia de cultivar una cultura ética en las organizaciones. Esto incluye políticas de cero tolerancia frente a actos antieméticos, programas de capacitación que lleguen a todos los niveles, desde la alta dirección hasta los empleados operativos y campañas de comunicación dirigidas a clientes y proveedores para alinear valores y expectativas.

2 Implementar tecnología avanzada para la prevención

La inteligencia artificial (IA) se ha convertido en una herramienta esencial para prevenir y detectar el fraude. Según Juan Carlos Medina, consultor y conferencista experto en riesgos, “los modelos de aprendizaje no supervisado pueden identificar operaciones inusuales y segmentar clientes de forma más precisa, ayudando a detectar patrones de fraude en etapas tempranas”. Estas tecnologías permiten analizar grandes volúmenes de datos en tiempo real, ofreciendo predicciones y detección temprana que mitigan riesgos antes de que se materialicen.

3 Adoptar una gestión de riesgos holística

Marta Cadavid señala que “las matrices de riesgos tradicionales a menudo no incorporan a las personas”, lo que limita su efectividad. Para superar esto, las organizaciones deben integrar perspectivas multidisciplinarias, involucrando expertos en psicología, sociología y comportamiento organizacional. Esto ayuda a comprender las normativas humanas detrás del fraude y a diseñar controles más efectivos.

4 Realizar auditorías regulares y controles internos sólidos

Auditar constantemente los procesos financieros es una práctica indispensable. Como recomienda Medina, “la evaluación recurrente de los modelos de identificación de riesgos asegura que los controles se mantengan actualizados y eficaces”. Además, es fundamental establecer sistemas de control interno que permiten identificar desviaciones o inconsistencias rápidamente.

5 Capacitar a los empleados y concientizar a los stakeholders

La capacitación no debe limitarse al personal interno. Cadavid sugiere involucrar también a proveedores y clientes en estrategias antifraude mediante campañas educativas y acuerdos contractuales que refuercen el compromiso con la ética. Esto crea un ecosistema donde todos los actores entienden su papel en la prevención del fraude.

6 Promover la transparencia y la comunicación interna

La transparencia fortalece la confianza y minimiza la percepción de opacidad que puede alimentar el fraude. Según “Fraud Risk Management: A Guide to Good Practice” de CIMA [3], las empresas que comunican abiertamente sus políticas y procedimientos logran mejores resultados en la prevención de fraudes. Las plataformas digitales y las reuniones internas regulares son ideales para compartir estas políticas.

3. Chartered Institute of Management Accountants. *Fraud Risk Management: A guide to good practice*

7 Adaptarse al entorno tecnológico y regulatorio

Los cambios normativos y tecnológicos requieren una adaptación constante. Medina resalta que la "identidad digital y las aplicaciones de IA serán clave en la debida diligencia y el control de riesgos". Estar al día con las regulaciones locales e internacionales, además de incorporar tecnologías avanzadas, asegura que las organizaciones puedan mitigar riesgos emergentes de manera efectiva.

El fraude es un riesgo multifacético que demanda una respuesta igualmente compleja y proactiva. Adoptar tecnologías como la IA, fortalecer la cultura organizacional y establecer controles robustos permite a las empresas, prevenir el fraude y proteger su reputación y garantizar la continuidad del negocio en un entorno cada vez más exigente.

> ***"El tejido social de una organización, desde el tono de la cabeza hasta el zumbido en el piso, define su capacidad para enfrentar este desafío".*** Marta Cadavid

4. Situaciones que afectan la continuidad del negocio

47,2%

DE LOS ENCUESTADOS SEÑALA LA CONTINUIDAD DEL NEGOCIO COMO UNO DE LOS PRINCIPALES RIESGOS EN SUS EMPRESAS.

Es importante poder garantizar la continuidad en medio de situaciones adversas, crisis o sorpresas inesperadas en las actividades diarias de cualquier organización, por eso, para el 47,2% de los encuestados, uno de los principales riesgos en sus empresas están relacionados con la continuidad del negocio.

En un entorno donde las crisis inesperadas son cada vez más frecuentes, las organizaciones deben estar preparadas para afrontar riesgos que amenacen su continuidad operativa. Desde ciberataques y desastres naturales hasta fallos en la cadena de suministro y cambios regulatorios, los desafíos son amplios y complejos.

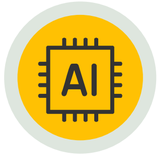
Por ello la gestión de riesgos no sólo debe ser reactiva, sino también estratégica y proactiva, como lo enfatiza Jorge Pinzón: “La gestión de riesgos típica ya no cumple los objetivos; debemos buscar cómo realmente aportar valor a la toma de decisiones del negocio”

Para enfrentar estos riesgos, resulta esencial adoptar estrategias que no se limiten a metodologías estándar, sino que se enfoquen en agregar valor organizacional. Esto incluye **fortalecer la cultura de riesgos** para que sea intrínseca en todos los niveles de la organización y aprovechar tecnologías avanzadas, como inteligencia artificial y la analítica de datos. Estas herramientas permiten modelar escenarios futuros, identificar patrones anómalos y optimizar la toma de decisiones antes de que un riesgo se materialice, ayudando a proteger los activos críticos y la reputación empresarial.

¿Cómo prevenir este riesgo?

1. Integrar análisis de entorno estratégico

Es crucial no sólo evaluar los riesgos internos, sino también explorar las “aguas turbulentas” externas, como lo describe Pinzón, que podrían impactar a las organización. Esto implica incluir tendencias globales, cambios regulatorios y factores macroeconómicos en la planificación estratégica.



2. Adoptar tecnologías emergentes

La inteligencia artificial permite automatizar tareas repetitivas y realizar análisis predictivos para identificar riesgos antes de que ocurran. Como afirma Pinzón, “estas tecnologías liberan a los profesionales para enfocarse en decisiones estratégicas, mientras detectan anomalías en tiempo real”.

3. Fortalecer los planes de continuidad

El business Impact Analysis (BIA) debe actualizarse regularmente para reflejar la realidad operativa y los cambios en el entorno. Además, el Plan de Continuidad del Negocio debe probarse en escenarios reales y controlados para garantizar su efectividad.

4. Promover una cultura de gestión de riesgos

Más allá de imponer obligaciones, es vital inspirar a los empleados a “amar los riesgos”, como señala Pinzón. Esto requiere campañas educativas prácticas que destaquen cómo la gestión de riesgos protege a las personas y asegura la sostenibilidad organizacional.

Garantizar la continuidad del negocio en un entorno incierto requiere un enfoque integral, donde la gestión de riesgos está alineada con los objetivos estratégicos de la organización. Incorporar tecnologías avanzadas, fortalecer los planes operativos y fomentar una cultura de prevención son pasos esenciales para navegar con éxito las adversidades y asegurar el futuro empresarial.

"Es necesario que la gestión de riesgos deje de ser solo un requisito y se convierta en un verdadero motor de valor para el negocio". **Jorge Pinzón**

5. Incertidumbre macroeconómica y geopolítica

43%

DE LAS ORGANIZACIONES IDENTIFICA LA INESTABILIDAD POLÍTICA, ECONÓMICA Y LA CRISIS MIGRATORIA COMO EL QUINTO MAYOR RIESGO PARA 2025

En el 2024, la región fue testigo de las elecciones presidenciales de **Estados Unidos**, unas de las más importantes y representativas para el comercio internacional. Según Pablo Camacho, experto en auditoría y compliance “Con la llegada de Trump al poder, vamos a ver un proteccionismo, esto puede generar tensiones comerciales que pueden afectar los mercados emergentes”

En un panorama global marcado por la inflación, la inestabilidad política, los cambios de gobierno y los conflictos internacionales, las empresas de Latinoamérica enfrentan desafíos significativos que amenazan su sostenibilidad. La volatilidad económica y los conflictos como la guerra de Ucrania afectan directamente las cadenas de suministro y los costos de producción, mientras que la tensión entre China y Estados Unidos amplifica la incertidumbre en los mercados emergentes.

Además, factores internos como el cambio de gobiernos y la crisis migratoria agravan las dificultades para mantener la estabilidad operativa, siendo éste riesgo el quinto del 2025 con un 43% de los votos según la encuesta.

Pablo Camacho señala que “las fluctuaciones en los mercados globales y las políticas monetarias de los principales bancos centrales impactan las carteras de empresas públicas y privadas, aumentando la exposición a riesgos de crédito”. Este efecto, sumada a la desaceleración de la inversión extranjera, exige que las organizaciones adapten sus estrategias para navegar en un entorno dinámico e incertidumbre.

¿Cómo prevenir este riesgo?

1

Monitorear el entorno global y local

La capacidad de adaptarse rápidamente a los cambios depende del monitoreo constante de los factores macroeconómicos y políticas. Según el informe “World Economic Outlook” del FMI [4], la proyección de crecimiento global para 2025 es de 3.3% lo que subraya la necesidad de que las empresas evalúen sus riesgos en función de tendencias globales y regionales.

2

Diversificar mercados y proveedores

Esperanza Hernández destaca que “la guerra en Ucrania y la crisis en China han afectado significativamente las cadenas de suministro”. Diversificar mercados y proveedores ayuda a reducir la dependencia de zonas de conflicto y a mitigar los impactos en los costos de producción.

3

Innovar para encontrar oportunidades en la crisis

En toda crisis hay oportunidades. Esto incluye identificar sectores emergentes que atraigan a los inversionistas, especialmente aquellos alineados con tendencias de sostenibilidad, como energías renovables o tecnología, tal como podría incentivarse.

4

Apostar por la resiliencia financiera

Camacho señala que la volatilidad de las divisas y la alta morosidad son desafíos críticos. Las empresas deben reforzar su estructura financiera mediante reservas estratégicas y planes que aseguren la liquidez frente a fluctuaciones en tasas de cambio o incrementos en los costos operativos.

4. World Economic Outlook, October 2024: *Policy Pivot, Rising Threats*

5 Innovar para encontrar oportunidades en la crisis

En toda crisis hay oportunidades. Esto incluye identificar sectores emergentes que atraigan a los inversionistas, especialmente aquellos alineados con tendencias de sostenibilidad, como energías renovables o tecnología, tal como podría incentivarse en un posible gobierno enfocado en ESG.

6 Mejorar la digitalización y ciberseguridad

Hernandez advierte que, aunque la digitalización ha avanzado en la región, aún existen brechas de conectividad y seguridad, Invertir en infraestructura tecnológica y medidas de ciberseguridad es esencial para proteger datos y operaciones ante posibles interrupciones y ataques.

La incertidumbre macroeconómica y geopolítica es un desafío complejo, pero también una oportunidad para fortalecer la resiliencia y adaptabilidad de las organizaciones. Desde la diversificación de riesgos hasta la implementación de estrategias ESG y la inversión en tecnología, las empresas deben adoptar enfoques integrales que les permitan sobrevivir y prosperar en un entorno en constante cambio.

> ***"Las organizaciones deben dejar de ver los riesgos como problemas aislados y empezar a entenderlos de manera holística, incluyendo el comportamiento humano y las dinámicas globales que impactan directamente su operación."***
>
> **Jorge Pinzón**

6. Otros riesgos

APARTE DE LOS RIESGOS MENCIONADOS ANTERIORMENTE, LOS PARTICIPANTES DE NUESTRO ESTUDIO TAMBIÉN CONSIDERAN PARA ESTE **2025** **RIESGOS COMO:**

6.1 Daños reputacionales

6.2 **Riesgos ASG** (Ambientales, Sociales y de Gobernanza)

6.3 Riesgos emergentes

6.4 Gestión del talento humano

6.1 Daños reputacionales

"Las decisiones que tomamos hoy impactan directamente en la percepción pública de mañana; manejarlas con cuidado es esencial para la supervivencia empresarial." **Pablo Camacho**

El riesgo reputacional también se encuentra entre los desafíos más críticos para las organizaciones. Una **crisis reputacional** puede surgir de factores como malas prácticas comerciales, falta de transparencia, daños ambientales o sociales y errores en la gestión de datos, afectando la confianza de los stakeholders y comprometiendo la sostenibilidad del negocio. Como advierte Pablo Camacho "Toma 20 años construir una imagen, pero sólo 5 minutos destruirla": lo que subraya la importancia de una gestión proactiva.

La gobernanza corporativa y los principios éticos son la base de una buena reputación. Según Estefania Rubio "La corrupción y la falta de transparencia no sólo afectan la imagen, sino que también limitan el acceso a financiamiento". Implementar códigos de buen gobierno y conducta, respaldados por políticas claras de prevención de malas prácticas, es esencial para mitigar este riesgo. Además, la comunicación estratégica, tanto interna como externa, juega un papel clave en la construcción de confianza y prevención de crisis.

La interacción con los stakeholders es otro pilar fundamental. Esperanza Hernández destaca que "conocer a fondo a los grupos de interés y entender sus expectativas minimiza riesgos sociales y reputacionales". Mantener un diálogo abierto y constante con clientes, empleados, proveedores y comunidades ayuda a anticipar problemas y a desarrollar soluciones conjuntas que fortalezcan la relación con estos actores clave.

Prepararse para incidentes potenciales también es crucial. Jean Paul Heymans resalta la importancia de **crear playbooks** específicos y realizar simulaciones que permitan gestionar crisis de manera ágil y eficaz. Estos ejercicios no sólo mejoran la capacidad de respuesta, sino que también demuestran a los stakeholders el compromiso de la organización con la transparencia y la resolución de problemas.

En un entorno de alta competencia y constante escrutinio, gestionar el riesgo reputacional requiere un enfoque integral que combine gobernanza, sostenibilidad, comunicación efectiva y preparación ante crisis. Las empresas que prioricen estos elementos estarán mejor posicionadas para fortalecer la confianza de sus stakeholders y asegurar su continuidad operativa en el largo plazo.

6.2

Riesgos ASG (Ambientales, Sociales y de Gobernanza)

"Los riesgos ASG no solo impactan financieramente; también definen cómo las empresas son percibidas por sus stakeholders, lo que hace vital gestionarlos con un enfoque estratégico y transparente." **Esperanza Hernandez**

El cambio climático, la desigualdad social y los desafíos de gobernanza destacan como factores críticos que incrementan la relevancia de los riesgos ambientales, sociales y de gobernanza (ASG). Para 2025, las empresas de Latinoamérica enfrentarán presiones por parte de reguladores, inversionistas y consumidores para integrar prácticas sostenibles en sus operaciones, según Estefanía Rubio, quien resalta que "la presión por reportar prácticas ASG y cumplir con estándares globales será fundamental para acceder a capital y mejorar la reputación"

La crisis climática, evidenciada por fenómenos como sequías, huracanes y deshielo de glaciares, ya no es un riesgo emergente, sino una realidad constante. Esto implica que las empresas deben reforzar su **compromiso con la sostenibilidad** y adoptar medidas de descarbonización para cumplir con regulaciones más estrictas, como los impuestos al carbono y la transición a energías renovables. Esperanza Hernandez advierte que "los riesgos ambientales ya no se presentan de forma esporádica; su frecuencia ha aumentado significativamente, y su impacto es cada vez más alto"

En el ámbito social, la desigualdad y los movimientos sociales también plantean riesgos significativos. Las empresas que no aborden estos temas podrían enfrentar críticas, boicots o pérdida de mercado. Además, las expectativas de los consumidores evolucionan hacia productos más sostenibles y éticos. Las compañías que no logren adaptarse a estas demandas corren el riesgo de rezagarse frente a competidores más comprometidos.

La gobernanza deficiente sigue siendo un desafío en la región. La corrupción, la falta de transparencia y el incumplimiento de normas pueden limitar el acceso a financiamiento y generar sanciones. Hernández subraya que, aunque la región ha avanzado en la adopción de códigos de buen gobierno, "Es crucial fortalecer las prácticas de medición y control para gestionar los riesgos ASG de manera efectiva"

Para enfrentar estos desafíos, las empresas deben integrar los riesgos ASG en su estrategia corporativa. Esto incluye identificar factores críticos, evaluar su impacto y establecer mecanismos de control y monitoreo. Implementar tecnologías emergentes, como la inteligencia artificial, puede ser clave para anticipar y gestionar estos riesgos. Por ejemplo, la IA puede facilitar el análisis predictivo de eventos climáticos y la trazabilidad en las cadenas de suministro, promoviendo operaciones más sostenibles.

6.3 Riesgos emergentes

"Los riesgos emergentes exigen una visión estratégica que combine adaptación, innovación y sostenibilidad para enfrentar un futuro cada vez más incierto" **Juan Carlos Medina**

El entorno empresarial enfrenta una aceleración en la aparición de riesgos emergentes, impulsados por cambios tecnológicos, económicos, sociales y ambientales. Estos riesgos a menudo impredecibles y multifacéticos, representan una amenaza creciente para la continuidad y sostenibilidad de las organizaciones. La gestión de estos desafíos requerirá un enfoque dinámico y adaptativo en 2025, con especial énfasis en la identificación temprana, el análisis holístico y la implementación de soluciones innovadoras.

Entre los principales riesgos emergentes se encuentra la intensificación del cambio climático, los avances tecnológicos no regulados y las crecientes tensiones sociales. Según Estefania Rubio: "La evolución de los eventos climáticos externos y la presión por descarbonizar las operaciones redefinirán las prioridades de sostenibilidad en la región". Estos fenómenos demandan la adopción de tecnologías limpias, la diversificación de las cadenas de suministro y la reducción de emisiones como elementos clave de la estrategia empresarial.

En el ámbito tecnológico, el uso creciente de **inteligencia artificial y la transformación digital** presentan oportunidades, pero también riesgos considerables. Jean Paul Heymans advierte que "la falta de preparación ante ciberamenazas puede amplificar los impactos de los ataques, especialmente en infraestructuras críticas". Por ello será esencial invertir en ciberseguridad y establecer protocolos que permitan responder rápidamente a incidentes, asegurando la continuidad operativa y la protección de los datos.

Por otro lado, la gobernanza y la capacidad de adaptación serán determinantes para gestionar riesgos sociales y de gobernanza. Esperanza Hernandez señala que "Los riesgos sociales como la desigualdad y las tensiones comunitarias no sólo generan conflictos internos, sino que pueden materializarse en crisis reputacionales". Abordar estos riesgos requiere la construcción de relaciones sólidas con los stakeholders, asegurando que las decisiones corporativas sean transparentes, inclusivas y éticamente responsables.

El análisis predictivo se posiciona como una herramienta clave para anticipar y mitigar riesgos emergentes. Herramientas como el aprendizaje automático permiten identificar patrones que facilitan la prevención de interrupciones en la cadena de suministro o problemas financieros. Según Juan Carlos Medina, "el análisis constante de parámetros y riesgos permite ajustar estrategias en tiempo real, evitando grandes impactos y fortaleciendo la resiliencia organizacional"

6.4 Gestión del talento humano

"El talento humano es el activo más valioso de una organización; gestionarlo eficazmente no sólo minimiza riesgos, sino que asegura la sostenibilidad y competitividad en el futuro"
Estefanía Rubio

En 2025, la gestión del talento humano se consolidará como uno de los riesgos más importantes para las organizaciones, en gran parte debido a la creciente escasez de habilidades, el impacto de la tecnología en el mercado laboral y los cambios en las expectativas de los empleados. Según un informe reciente de Deloitte [5], el 61% de las empresas a nivel mundial ya enfrenta desafíos para cubrir roles clave debido a la falta de competencias técnicas y blandas en sus equipos. Este fenómeno, conocido como **skill gap**, podría agravarse en los próximos años si no se implementan estrategias efectivas para atraer, retener y desarrollar el talento.

La integración de tecnologías emergentes, como la inteligencia artificial, también plantea riesgos en la gestión del talento humano. Jean Paul Heymans señala que "aunque la tecnología puede automatizar procesos operativos, su implementación sin una estrategia clara puede generar resistencia al cambio y una sensación de inseguridad entre los empleados". Para mitigar este riesgo, las empresas deben enfocarse en la capacitación continua y en fomentar una cultura organizacional que valore la adaptación y la innovación tecnológica.

61%

DE LAS EMPRESAS GLOBALES ENFRENTA DIFICULTADES PARA CUBRIR ROLES CLAVE POR FALTA DE COMPETENCIAS TÉCNICAS Y BLANDAS.

+50%

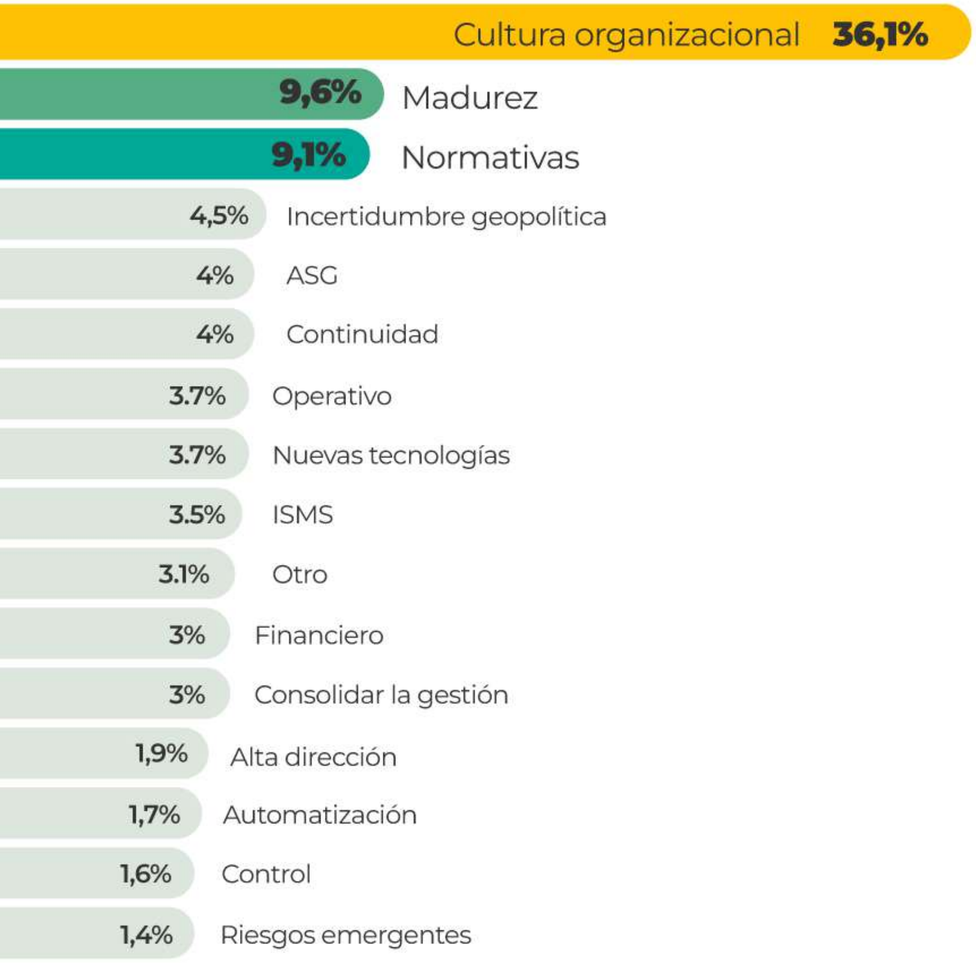
DE LAS ORGANIZACIONES CARECEN DE PLANES CLAROS PARA IDENTIFICAR Y PREPARAR A SUS FUTUROS LÍDERES

Por otro lado, las expectativas de los empleados han cambiado significativamente. Las nuevas generaciones buscan entornos laborales más flexibles, inclusivos y alineados con valores sostenibles. Según Estefania Rubio, “una gestión inadecuada de los riesgos sociales, como la desigualdad o la falta de diversidad puede derivar en altos índices de rotación y pérdida reputacional”. Esto subraya la importancia de promover prácticas de inclusión y equidad que fortalezcan la confianza y el compromiso de los equipos.

La falta de planificación sucesoria es otro desafío clave en la gestión del talento. Empresas de diversos sectores enfrentan el riesgo de perder conocimiento crítico debido al envejecimiento de la fuerza laboral o falta de desarrollo de líderes internos. Como advierte un artículo reciente de McKinsey [6] más del 50% de las organizaciones carecen de planes claros para identificar y preparar a sus futuros líderes, lo que podría afectar la continuidad operativa y estratégica.

Para gestionar estos riesgos, las organizaciones deben adoptar un enfoque integral que combine herramientas tecnológicas, programas de desarrollo profesional y estrategias de bienestar. Implementar plataformas de aprendizaje personalizadas basadas en inteligencia artificial puede ayudar a cerrar brechas de habilidades, mientras que fomentar el bienestar emocional y físico de los empleados fortalece su compromiso y productividad. Además, la comunicación clara y transparente sobre los objetivos y valores de la organización es clave para alinear a los equipos.

DIFICULTADES ACTUALES Y RETOS EN GESTIÓN DE RIESGOS PARA 2025



GRÁFICA: ¿Cuáles serán los riesgos más importantes para tu organización en 2025?

Como de costumbre, en nuestro **Estudio de Gestión de Riesgos en Latinoamérica 2025** también preguntamos a los participantes por las principales dificultades a las que se ve enfrentada el área de gestión

1. Falta de cultura de riesgos

Con el 36.1% de las respuestas, la falta de la cultura de riesgos se posiciona, por cuarto año consecutivo, como la principal dificultad en las organizaciones de Latinoamérica para gestionar de manera eficaz los riesgos. Este hallazgo resalta la necesidad urgente de implementar estrategias que promuevan una comprensión integral de los riesgos en todos los niveles de las empresas.

Que esta siga siendo la principal dificultad refleja un desafío persistente: la gestión de riesgos no está plenamente integrada en la cultura organizacional. Esto limita la capacidad de las empresas para anticiparse a las amenazas y adaptarse a un entorno dinámico. Según Estefania Rubio “La cultura de riesgos no debe ser solo un conjunto de normas, sino una mentalidad que se traduzca en acciones y decisiones diarias”.

Para abordar este problema, es esencial que las organizaciones fomenten el compromiso de la alta dirección, dado que su liderazgo establece el tono ético operativo para toda la empresa. Además, deben invertir en programas de formación continua que incluyan ejemplos prácticos y simulaciones, lo que permite a los empleados comprender cómo identificar y gestionar los riesgos en sus funciones específicas.

La comunicación interna también juega un papel clave. Las empresas con una comunicación clara y consistente sobre riesgos son más efectivas en prevenir su materialización. Esto incluye divulgar políticas, procedimientos y empleos de éxito en la gestión de riesgos para inspirar confianza y alineación.

Otro aspecto crucial es el diseño de incentivos que premien el comportamiento proactivo en la identificación y mitigación de riesgos. Esto refuerza la idea de que todos los empleados, independientemente de su rol, son responsables de contribuir a la resiliencia organizacional.

Construir una cultura de riesgos requiere tiempo, compromiso y acciones concretas que vayan más allá de simples capacitaciones. Las organizaciones que logren interiorizar la gestión de riesgos como parte de su ADN estarán mejor preparadas para enfrentar las incertidumbres del futuro y asegurar su sostenibilidad.

2. Poca madurez en gestión de riesgos

Con el 9,6% de las respuestas, la poca madurez en la gestión de riesgos se posiciona como la segunda mayor dificultad enfrentada por las organizaciones en Latinoamérica. Esta situación refleja que, aunque se han dado pasos importantes hacia una mayor conciencia sobre la importancia de gestionar riesgos, muchas empresas aún carecen de sistemas robustos y metodologías efectivas para hacerlo de manera estratégica.

Esta dificultad refleja la necesidad de avanzar en la implementación de marcos y herramientas más estructurados. La falta de madurez en la gestión de riesgos limita la capacidad de las organizaciones para identificar, evaluar y responder adecuadamente a las amenazas, especialmente en un entorno de negocios cada vez más volátil. Según Jorge Pinzón, “La gestión de riesgos debe ir más allá de matrices y mapas; debe integrarse a la toma de decisiones para generar valor real en el negocio”.

Para mejorar este aspecto, es importante que las empresas adopten estándares internacionales como **ISO 31000**, que ofrecen guías prácticas para establecer procesos sólidos de gestión de riesgos. Esto debe complementarse con evaluaciones periódicas que permitan identificar áreas de mejora y medir el avance hacia una mayor madurez en la implementación de controles y procesos.

Además, la falta de madurez está directamente relacionada con una insuficiente alineación entre la gestión de riesgos y los objetivos estratégicos de la organización. Otro paso importante es la capacitación y el desarrollo de competencias específicas en los equipos de gestión de riesgos.

La poca madurez en la gestión de riesgos es un desafío que debe abordarse con una visión integral y de largo plazo. Las organizaciones que logren fortalecer sus procesos, capacitar a sus equipos y alinear la gestión de riesgos con sus objetivos estratégicos estarán mejor posicionadas para enfrentar las complejidades del entorno actual y garantizar su sostenibilidad.

3. Cumplimiento normativo

Con el 9,1% de las respuestas, el cumplimiento normativo se ubica como el tercer desafío más relevante en la gestión de riesgos para las organizaciones en Latinoamérica. Este reto refleja la creciente presión por adaptarse a un entorno regulatorio en constante evolución, marcado por normativas más estrictas en áreas como protección de datos, sostenibilidad, prevención de delitos financieros. Según Pablo Camacho, “Las regulaciones están en constante cambio y su incumplimiento puede ser costoso y complejo para las entidades”. Para superar esta dificultad, es esencial que las empresas implementen sistemas de monitoreo proactivo, automatización de procesos de compliance y capacitación continua, asegurando que cada área esté preparada para cumplir con los estándares locales e internacionales.

Un factor clave para enfrentar el cumplimiento normativo es **integrar la gestión de riesgos con las áreas de compliance**. Esto permite identificar los requisitos críticos y establecer controles internos que minimicen las probabilidades de incumplimiento. Como señala Mariano López, “Tener asesoramiento adecuado y una evaluación constante de los cambios normativos es esencial para garantizar la continuidad del negocio y mantener la reputación corporativa”.

Además, la comunicación interna efectiva es fundamental para garantizar que todos los empleados comprendan su papel en el cumplimiento normativo. Las políticas deben estar claramente documentadas y divulgadas, acompañadas de capacitaciones regulares que incluyan casos prácticos relacionados con las normativas más relevantes para el sector. Esto asegura una mayor alineación entre las operaciones diarias y los requisitos regulatorios.

Finalmente, las empresas deben estar atentas a la convergencia de normativas internacionales, especialmente en áreas como sostenibilidad y protección de datos. Estefania Rubio, advierte que “La doble materialidad en los estándares ESG será un punto de inflexión para muchas organizaciones, exigiendo mayor transparencia en la gestión ambiental y social”. Prepararse para estos desafíos ayudará a las organizaciones no sólo a cumplir con la exigencias legales, sino también a generar confianza en sus stakeholders y fortalecer su posición en el mercado.

4. Incertidumbre geopolítica

La incertidumbre geopolítica se posiciona como la cuarta dificultad para el área de gestión de riesgos con un 4,5% de los votos, esto, dado su impacto directo en la estabilidad operativa y financiera. Los cambios de gobierno, las políticas impredecibles y la polarización social generan un entorno de alta volatilidad que dificulta la planificación estratégica. Esta falta de claridad en el panorama político obliga a las empresas a gestionar riesgos adicionales relacionados con regulaciones cambiantes, restricciones comerciales y conflictos sociales.

Una de las principales complicaciones que genera esta incertidumbre es la dificultad para prever el impacto de nuevas normativas y políticas fiscales. Según Pablo Camacho, “Los cambios regulatorios repentinos pueden aumentar significativamente los costos operativos y alterar los modelos de negocio”. Esto afecta especialmente a sectores altamente regulados, como energía, tecnología y finanzas, donde las políticas gubernamentales tienen un papel determinante en su viabilidad y crecimiento.

La polarización política y social también representan un desafío crítico, ya que puede derivar en conflictos, protestas y pérdida de confianza en el entorno empresarial. Esto no sólo dificulta la atracción de inversión extranjera, sino que también pone en riesgo la continuidad de las operaciones. Las empresas deben ser ágiles para adaptarse a estas tensiones y mantener una comunicación constante con los stakeholders para mitigar posibles impactos en su reputación.

Por último, la incertidumbre política complica la toma de decisiones estratégicas a largo plazo. Las organizaciones se ven obligadas a operar en ciclos cortos, priorizando la supervivencia sobre la innovación. Para enfrentar esa dificultad, las empresas deben fortalecer sus sistemas de **monitoreo político y económico**, diversificar sus mercados y desarrollar planes de contingencia robustos. De esta manera, podrán mitigar los efectos de un entorno político impredecible y preservar su sostenibilidad operativa.

5. Falta de herramientas tecnológicas

La falta de herramientas tecnológicas adecuadas se posiciona como la cuarta dificultad, con un 3,7% de las respuestas. Este desafío refleja que, aunque muchas organizaciones han iniciado su transición digital, aún enfrentan limitaciones significativas en términos de infraestructura tecnológica y acceso a soluciones avanzadas. Estas carencias dificultan la identificación, monitoreo y mitigación de riesgos de manera eficiente, dejando a las empresas vulnerables frente a amenazas emergentes y convencionales.

Uno de los principales problemas derivados de esta dificultad es la falta de automatización en los procesos de gestión de riesgos. Según un informe de Gartner, las empresas que no implementan herramientas digitales enfrentan costos operativos más altos y una capacidad limitada para responder a incidentes en tiempo real. Sin sistemas adecuados, como plataformas de análisis predictivo o soluciones de ciberseguridad, las organizaciones deben depender de procesos manuales, que son menos efectivos y más propensos a errores.

Además, esa falta de herramientas tecnológicas afecta directamente la capacidad de las empresas para adaptarse a un entorno regulatorio en constante cambio. Las normativas modernas exigen reportes más detallados y frecuentes, así como una mayor transparencia en la gestión de riesgos. Sin soluciones digitales para centralizar y analizar datos, cumplir con estas exigencias puede volverse un proceso complejo y costoso, generando riesgos adicionales para la continuidad del negocio.

Para superar esta dificultad, es esencial que las empresas prioricen la inversión en tecnología, seleccionando herramientas que se alineen con sus necesidades específicas y su nivel de madurez en la gestión de riesgos. Esto incluye soluciones basadas en inteligencia artificial para detectar patrones anómalos, sistemas de monitoreo en tiempo real y plataformas colaborativas que faciliten la gestión integral de riesgos. La capacitación tecnológica del personal también será clave para maximizar el uso de estas herramientas y garantizar su efectividad en la mitigación de amenazas.

PRINCIPALES RIESGOS RELACIONADOS CON **INTELIGENCIA ARTIFICIAL**

Como novedad en esta edición del **Estudio de Gestión de Riesgos en Latinoamérica**, preguntamos a los encuestados sobre los principales riesgos relacionados a la inteligencia artificial, un tema que en los pasados estudios fue una fuerte tendencia, pero en 2024, ya es una herramienta implementada dentro de las labores de las organizaciones de todo tipo.

GRÁFICA: ¿Qué riesgos nuevos crees que surgirán con el uso creciente de inteligencia artificial en tu industria?

Amenazas de ciberseguridad

23,7%

DE LOS ENCUESTADOS DESTACA LA **IA** COMO UN FACTOR QUE AGRAVA LAS AMENAZAS DE CIBERSEGURIDAD.

La integración de la inteligencia artificial (IA) en los sistemas empresariales ha intensificado las amenazas de ciberseguridad, siendo un riesgo destacado por el 23,7% de los encuestados. Este avance de la IA ha llevado a ataques más sofisticados, como deepfakes, phishing automatizado y el uso de bots para identificar y explotar vulnerabilidades. Estas técnicas hacen que las amenazas sean más difíciles de detectar y mitigar, impactando tanto a empresas como a usuarios individuales.

Jean Paul Heymans subraya la importancia de la preparación frente a estos riesgos: “Definir equipos de respuesta y playbooks específicos para escenarios cibernéticos es fundamental”. Este enfoque proactivo ayuda a las organizaciones a reaccionar rápidamente y minimizar el impacto de depender de herramientas tradicionales, que no sean efectivas contra los ataques basados en IA, como los zero days exploits (Ataques basado en encontrar vulnerabilidades desconocidas por el desarrollador)

Una solución útil es adoptar tecnologías de ciberseguridad impulsadas por IA, que puedan identificar anomalías en tiempo real y anticipar amenazas antes de que se materialicen. Herramientas basadas en aprendizaje automático analizan patrones de comportamiento, detectan desviaciones y reaccionan automáticamente a actividades sospechosas, ayudando a prevenir grandes pérdidas.

Además, las organizaciones deben fomentar la concienciación en ciberseguridad entre sus empleados. Según el Foro Económico Mundial [7], muchas amenazas cibernéticas son facilitadas por errores humanos, por lo que invertir en formación es tan crucial como contar con la tecnología adecuada. Este enfoque es tan crucial como contar con la tecnología adecuada. Este enfoque combinado permite a las empresas enfrentar los riesgos con mayor eficacia, protegiendo tanto sus datos como su reputación.

7. World Economic Forum. Cybersecurity and AI: *The challenges and opportunities*

Falta de comprensión de la IA por la alta dirección

18,7%

DE LAS ORGANIZACIONES CONSIDERA QUE LA FALTA DE COMPRENSIÓN DE LA IA EN LA ALTA DIRECCIÓN ES UN RIESGO SIGNIFICATIVO.

La falta de comprensión sobre la inteligencia artificial por parte de la alta dirección es un riesgo significativo, según el 18.8% de las organizaciones. A medida que la IA se convierte en un motor clave para la innovación y la competitividad, la incapacidad de los líderes para entender sus implicaciones puede obstaculizar la implementación efectiva de tecnologías que mejoren la eficiencia y la toma de decisiones. La brecha entre los avances tecnológicos y la comprensión ejecutiva genera **decisiones poco informadas** que retrasan la adopción de herramientas disruptivas.

La alta dirección debe estar involucrada en el aprendizaje y la implementación de IA, no sólo delegarla a departamentos técnicos. Sin un entendimiento claro de las capacidades y riesgos de la IA, los líderes pueden subestimar el potencial de estas herramientas para transformar sus operaciones, o peor aún, implementar soluciones inadecuadas que no se alineen con los objetivos estratégicos de la organización. Esta falta de visión estratégica es un obstáculo considerable para las empresas que buscan mantenerse competitivas en un entorno de rápida transformación digital.

La solución a este desafío es promover una cultura de educación tecnológica dentro de las organizaciones. Los líderes deben invertir tiempo en entender los **beneficios y riesgos de la IA**, y formar equipos interdisciplinarios que faciliten la integración de la IA en todos los niveles. Según el Foro Económico Mundial [8], las empresas más exitosas serán aquellas en las que la alta dirección tenga una comprensión sólida de la IA y se involucre activamente en su implementación estratégica.

8. World Economic Forum. *What does 2024 have in store for the world of cubersecurity?*

Riesgos éticos

16,9%

DE LAS ORGANIZACIONES ALERTA SOBRE LOS RIESGOS ÉTICOS DE LA IA, COMO SESGOS, FALTA DE TRANSPARENCIA Y USO INDEBIDO.

Los riesgos éticos asociados con la inteligencia artificial (IA) están ganando relevancia a medida que las organizaciones dependen más de estas tecnologías. Con un 16.9% de las respuestas, este desafío refleja preocupaciones sobre el impacto de la IA en la equidad, la privacidad y la transparencia en la toma de decisiones. Como menciona un análisis del Markkula Center For Applied Ethics [9], la dependencia de datos históricos para entrenar algoritmos puede perpetuar sesgos preexistentes, lo que afecta negativamente a grupos marginados. Un ejemplo de esto fue el caso de Amazon, donde un sistema de contratación basado en IA discriminó a las mujeres debido a datos sesgados utilizados para su desarrollo.

La falta de explicabilidad en las decisiones tomadas por la IA es otro punto crítico. Los sistemas no siempre brindan claridad sobre cómo se llegan a sus conclusiones, lo que puede ser problemático en sectores como la banca o la salud, donde las decisiones tienen impactos de largo alcance. El Foro Económico Mundial, indica que la regulación como la Ley de la IA de la Unión Europea, busca abordar esta falta de transparencia mediante requisitos claros para desarrolladores y usuarios de estas tecnologías.

El uso indebido de la IA también plantea preocupaciones éticas significativas. Herramientas avanzadas, como *deepfakes* y algoritmos de desinformación, ya están siendo utilizadas para manipular opiniones públicas y causar daño reputacional a individuos y empresas. Este tipo de riesgos subraya la necesidad de implementar principios éticos sólidos durante el desarrollo de despliegue de la IA.

Para gestionar estos riesgos, es esencial que las organizaciones adopten un enfoque proactivo basado en principios de responsabilidad y ética. Integrar la ética en la estrategia corporativa desde el desarrollo de la IA no sólo ayuda a prevenir problemas legales y reputacionales, sino que también construye confianza entre los stakeholders. Las empresas deben priorizar la transparencia, garantizar la diversidad en los datos de entrenamiento y establecer mecanismos de auditoría continua para mitigar estos riesgos éticos.

9. The Itec Handbook. *Ethics in the age of disruptive technologies.*

Dependencia excesiva en la tecnología

16,3%

DE LAS ORGANIZACIONES ADVIERTE QUE LA DEPENDENCIA EXCESIVA EN LA TECNOLOGÍA AUMENTA LAS VULNERABILIDADES CRÍTICAS.

La dependencia excesiva en la tecnología, mencionada por el 16.3% de los encuestados, es un riesgo emergente significativo para el 2025. Esta dependencia puede generar vulnerabilidades críticas, especialmente cuando las infraestructuras tecnológicas fallan, se enfrentan a ciberataques o no cumplen con las expectativas operativas. Como señala Fernando Barrio, profesor en Queen Mary University Of London, "Todo lo que está conectado es inseguro" [10], subrayando que el mal manejo de la tecnología puede limitar la capacidad de las empresas para adaptarse y responder ante imprevistos.

Un problema relacionado es la **pérdida de habilidades humanas** para resolver problemas críticos sin apoyo tecnológico. Esto se evidencia en escenarios donde los sistemas automatizados toman decisiones sin supervisión, lo que podría amplificar errores y riesgos éticos. Un estudio del Stafford Human-Centered AI institute [11],muestra que, aunque las explicaciones de las IA pueden mejorar la compresión, también pueden generar una falsa confianza si las decisiones se automatizan sin un análisis crítico humano.

Para mitigar este riesgo, las empresas deben equilibrar el uso de tecnologías con procesos resilientes que incluyan protocolos manuales en caso de fallos sistémicos. Fomentar la capacitación tecnológica para los empleados y establecer auditorías periódicas puede fortalecer la resiliencia organizacional y reducir la sobredependencia en sistemas digitales avanzados.

Finalmente las organizaciones deben priorizar inversiones en tecnologías seguras y actualizadas, mientras aseguran que los sistemas sean escalables y fácilmente adaptables.

Esto no sólo refuerza la continuidad de negocio, sino que también ayuda a evitar que la dependencia en la tecnología se convierta en un obstáculo más que en un aliado para la gestión de riesgos.

10. Pew Research Center. *Experts say the "new normal" in 2025 will be far more tech-driven, presenting more big challenges.*

11. Stanford University Human-Centered Artificial Intelligence. *AI overreliance is a problem. Are explanations a solution?*

Sesgo en la toma de decisiones

13,9%

DE LAS ORGANIZACIONES IDENTIFICA EL SESGO EN LA IA COMO UN RIESGO QUE IMPACTA LA EQUIDAD Y CREDIBILIDAD EMPRESARIAL.

El sesgo en la toma de decisiones es un riesgo destacado por el 13,9% de los encuestados, un fenómeno que se da especialmente en las organizaciones que dependen de la inteligencia artificial (IA) para tomar decisiones críticas. Estos sistemas, aunque diseñados para ser objetivos, reflejan los **sesgos presentes en los datos utilizados para entrenarlos.** Esto puede perpetuar desigualdades sociales o económicas, como señala Esperanza Hernandez, “Si los sistemas de IA no consideran la diversidad en sus datos, los riesgos éticos y sociales se amplifican, afectando tanto a los empleados como a los clientes”.

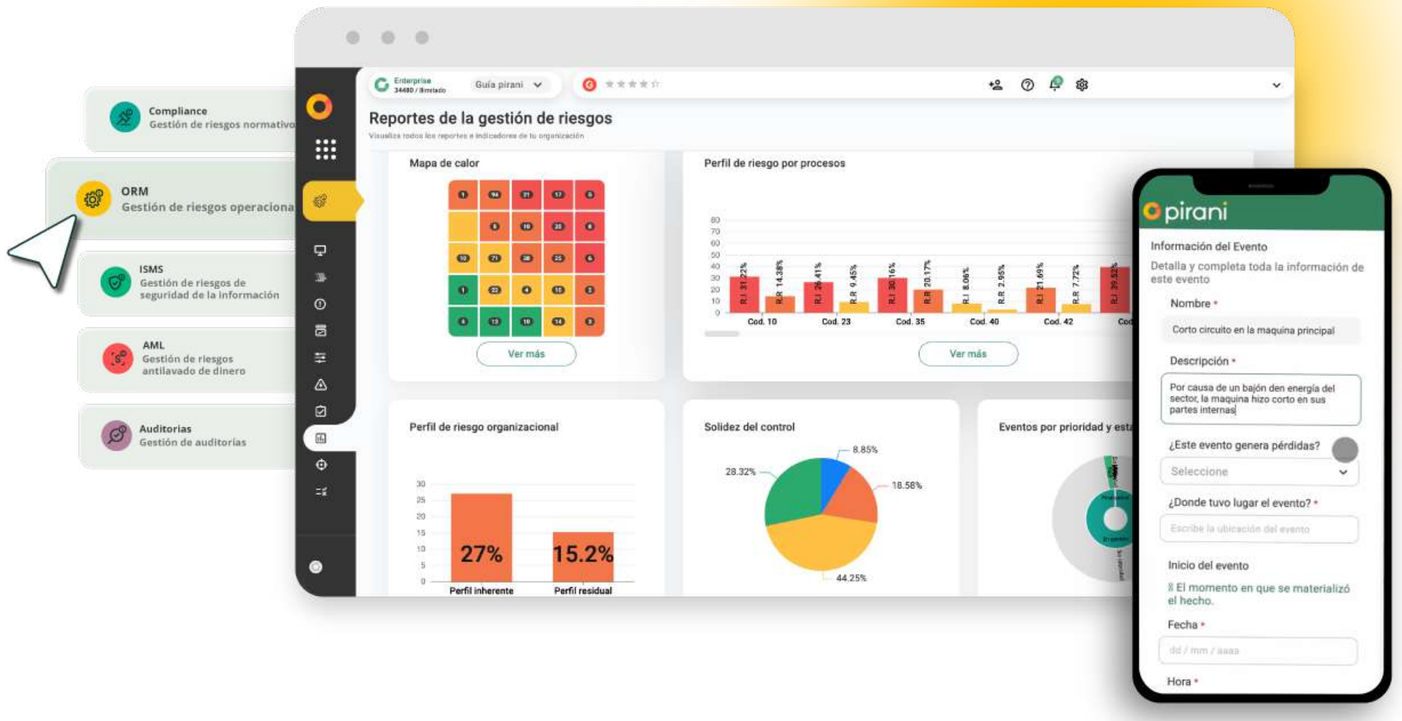
Este riesgo no sólo afecta la equidad, sino también la credibilidad de las decisiones empresariales. Un ejemplo conocido es el sistema de crédito que, basados en datos históricos, tiende a discriminar a ciertas poblaciones debido a patrones implícitos. La falta de transparencia en los algoritmos agrava el problema, dificultando que las organizaciones identifiquen dónde y cómo ocurren estas decisiones sesgadas.

Para mitigar el sesgo, las organizaciones deben **priorizar auditorías regulares** de sus algoritmos de IA y fomentar la inclusión en los equipos que desarrollan estas tecnologías. Estefania Rubio destaca que “es necesario construir sistemas que no sólo cumplan con estándares éticos, sino que también sean capaces de adaptarse y evolucionar frente a nuevos desafíos sociales”. Además, implementar procesos para corregir los sesgos detectados es esencial para garantizar que las decisiones sean justas y alineadas con los valores corporativos.

Finalmente, la educación y capacitación en ética tecnológica deben ser prioridad para los líderes y responsables de la toma de decisiones. Sólo a través de un enfoque consciente y proactivo se pueden minimizar los sesgos y construir confianza entre los stakeholders, garantizando que las decisiones basadas en IA no sólo sean efectivas, sino también justas y responsables.

Para las organizaciones que buscan una gestión integral y eficiente de sus riesgos, Pirani, ofrece módulos especializados para gestionar riesgos de Compliance, Gestión de riesgos Operacionales (ORM), Gestión de Seguridad de la Información (ISMS), Prevención de Lavado de Activos (AML), y Gestión de Auditorías. Cada módulo está diseñado para afrontar desafíos específicos, desde el cumplimiento normativo hasta la protección frente a ciberamenazas y la mitigación de riesgos operativos.

Al centralizar estas funciones en una plataforma, Pirani no sólo optimiza los procesos de gestión de riesgos, sino que también promueve una cultura de cumplimiento y resiliencia organizacional. Además, su capacidad de integración y personalización. Además, su capacidad de integración y personalización permite que las organizaciones adapten las herramientas a sus necesidades únicas, asegurando que los riesgos sean identificados, analizados y tratados de manera oportuna y efectiva.



Te contamos lo que tu organización puede lograr con Pirani

Reduce 60%

Reducción de la carga operativa en un 60% gracias a la automatización

Reduce 30%

Reducción de errores humanos en un 30% al tener una mejor calidad de información y evitar reprocesos

Reduce 40%

Reduce en un 40% los tiempos de detección y respuestas ante eventos

Aumento 70%

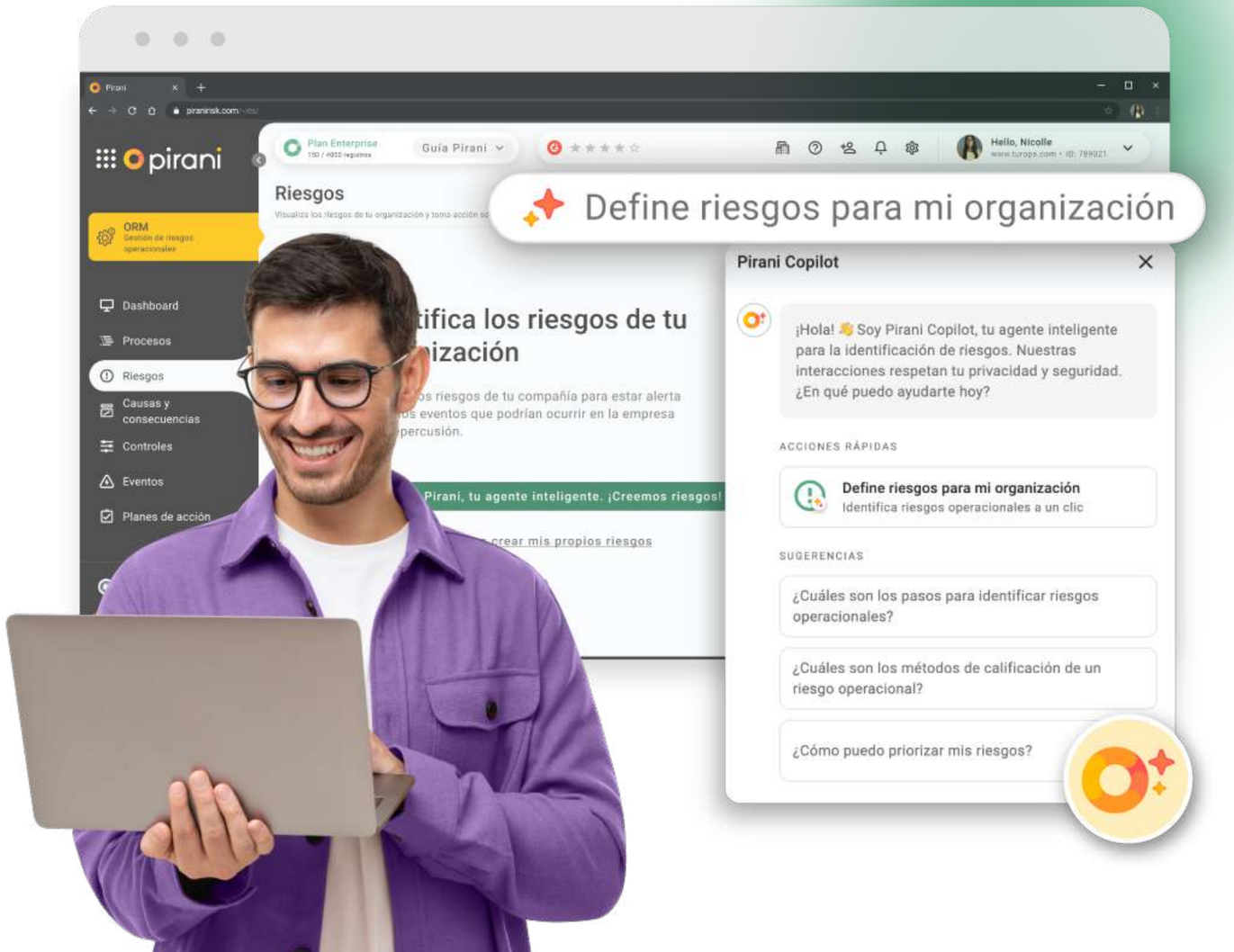
Aumento en un 70% en la participación de los miembros de la organización y fomento de la cultura de riesgos.

Madurez Percibida

Mejora en la percepción de la madurez de riesgos ante clientes y entes reguladores

ROI 9 meses

En promedio, el ROI de utilizar Pirani como software de gestión de riesgos se ven en 9 meses.



Además, este año estrenamos, Pirani Copilot, tu nuevo asistente para la gestión de riesgos con Inteligencia Artificial (IA). Con esta herramienta puedes tener mayor rapidez en la identificación de riesgos, consultas 24/7 sobre gestión de riesgos, base de datos con múltiples fuentes actualizadas y vigentes. Actualmente este asistente está disponible en el módulo ORM.

Te invitamos a descubrir cómo Pirani puede transformar la gestión de riesgos en tu organización. Prueba nuestra herramienta y experimenta sus beneficios sin necesidad de una tarjeta de crédito. Optimiza tus procesos, refuerza el cumplimiento normativo y afronta los riesgos con confianza utilizando soluciones integrales y herramientas avanzadas.

REFERENCIA BIBLIOGRÁFICA

- **Routledge.** Managing Cyber Risk, Ariel Evans
- **Packt Publishing.** Practical Cybersecutiry Architecture, Ed Moyley, Diana Kelley
- **Chartered Institute of Management Accountants.** Fraud Risk Management: A guide to good practice
- **World Economic Outlook,** October 2024: Policy Pivot, Rising Threats
- **Deloitte Insights.** 2024 tendencias globales de capital humano.
- **McKinsey & Company.** Un nuevo liderazgo para una nueva era de organizaciones prósperas.
- **World Economic Forum.** Cybersecurity and AI: The challenges and opportunities
- **World Economic Forum**. What does 2024 have in store for the world of cubersecurity?
- **The Itec Handbook.** Ethics in the age of disruptive technologies.
- **Pew Research Center.** Experts say the “new normal” in 2025 will be far more tech-driven, presenting more big challenges.
- **Stanford University Human-Centered Artificial Intelligence.** AI overreliance is a problem. Are explanations a solution?

pirani

Hacemos simple la gestión de riesgos

WWW.PIRANIRISK.COM