En busca de la estabilidad dentro de la volatilidad:

¿Cómo los riesgos emergentes sitúan a las gerencias de riesgos en el centro del negocio financiero?

12° encuesta anual sobre la gestión de riesgos bancarios globales

EY Building a better working world

IIF Institute of International Finance

C O N T E N I D O

Resumen ejecutivo

Los eventos mundiales y las fuerzas externas han distorsionado las categorías tradicionales de la gestión de riesgos, ampliando las responsabilidades y reorganizando las prioridades de las gerencias de riesgo en la industria bancaria.

La compleja interacción entre los riesgos superpuestos y las fuerzas externas e internas pueden generar problemas de riesgos inesperados.

La incertidumbre y la volatilidad parecen aumentar a la par. La sensación de que "todo sucede a la vez" y la necesidad de mirar más allá de los límites están impulsando a las gerencias de riesgos a encontrar nuevas herramientas y talento para operar de manera efectiva en un panorama de riesgo altamente dinámico.

Los gerentes de riesgos priorizarán la ciberseguridad en los próximos 12 meses y la resiliencia operativa, durante los próximos tres años. También cabe destacar que el riesgo geopolítico dió el mayor salto en la agenda de los gerentes de riesgos, respecto a la encuesta del año pasado. De cara al futuro, es probable que la prioridad de los riesgos ambientales, sociales, de gobernanza, climáticos y de transformación digital aumente durante los próximos 36 meses.

Cuanto más difícil sea modelar un riesgo y menos claridad haya por parte de los reguladores, puede ser más retador gestionarlo. Esto es especialmente cierto cuando los riesgos pueden tener implicaciones graves a corto plazo, y las amenazas de nivel empresarial trascienden.

Eso es especialmente cierto cuando los riesgos podrían tener implicaciones graves a corto plazo y las amenazas a nivel empresarial trascienden las disciplinas y capacidades tradicionales de la gestión de riesgos. En estas situaciones, los bancos a menudo deciden mantener mayor capital, lo que puede resultar en un análisis detallado del rendimiento de este y una evaluación cuidadosa de los objetivos comerciales frente a las metas de gestión de riesgos.

CINCO HALLAZGOS CLAVE DE LA ENCUESTA DE ESTE AÑO

1.

El riesgo geopolítico agrega incertidumbre a la turbulencia económica, impactando de forma diferente en las distintas regiones.

Nuestros resultados muestran que los gerentes de riesgos (CRO, por sus siglas en inglés) continúan prestando mucha atención a las diversas manifestaciones posibles del riesgo geopolítico, incluida la volatilidad económica y del mercado, sanciones adicionales, aumento de los ataques cibernéticos de actores patrocinados por el estado y amenazas a la resiliencia operativa. Los bancos ven sus perfiles de riesgo geopolítico de manera diferente, en función de su tamaño y huella operativa, con riesgos que se materializan más allá de las dificultades derivadas de la guerra en Ucrania.

Es probable que el próximo año se vean evaluaciones más formales y amplias relacionadas a la gestión de riesgos en el ámbito del riesgo geopolítico. Los CRO también están atentos a mayores disturbios sociales, en caso de que una recesión económica exacerbe las crecientes tensiones políticas en los diversos países del mundo.

2.

Las amenazas cibernéticas encabezan la agenda, debido a su creciente complejidad y constante evolución.

A pesar de los miles de millones invertidos para salvaguardar los sistemas centrales y proteger los datos vitales, los CRO consideran que los riesgos cibernéticos son la principal amenaza que puede provocar una crisis o una interrupción operativa importante. Incluso cuando perciben que sus propios sistemas internos son seguros, los CRO ven posibles amplificaciones y concentraciones del riesgo cibernético al acecho en todas partes: dentro de la turbulencia geopolítica, las estrategias del ecosistema y las vastas redes de socios, proveedores y vendedores de los que dependen cada vez más.

La interconexión de esas redes y las tecnologías integradas que soportan todo el sistema financiero global representan una superficie de ataque masiva y un enorme perímetro para asegurar. Debido a que los malos actores son implacables en la búsqueda de vulnerabilidades y a que los ataques exitosos son tan lucrativos, vale la pena preguntarse si las amenazas cibernéticas dejarán la prioridad de las agendas de los CRO.

3.

El riesgo de crédito mantiene una prioridad alta, ya que los bancos buscan riesgos ocultos que puedan materializarse en la recesión económica que se avecina.

Dadas las lecciones aprendidas desde la pasada crisis financiera mundial y el aumento de los niveles de capital y liquidez, los resultados de nuestra encuesta indican que, en general, los CRO confían en su capacidad para gestionar las fuentes tradicionales de riesgo de crédito. La gestión del riesgo de crédito es una competencia fundamental para cualquier banco. Sin embargo, los CRO son especialmente cautelosos sobre la incierta gravedad y duración de una recesión económica. Nuestros encuestados parecen reconocer que existe un amplio consenso de que los principales riesgos financieros están bajo control, sin embargo el potencial de riesgo sistémico puede aumentar.

En el momento de la encuesta, las métricas de riesgo de crédito tradicionales aún no habían mostrado un deterioro significativo y los balances se mostraban sólidos. Pero con los desarrollos macroeconómicos de los meses posteriores, incluidos episodios de volatilidad en los mercados financieros, los CRO deben continuar desafiando a sus equipos para evitar caer en la autocomplacencia. Ciertamente, los reguladores también están monitoreando de cerca los efectos de una recesión económica en los balances de las instituciones financieras.

Además, los CRO deben estar atentos a la clase de activos y las vulnerabilidades de la contraparte, incluso de los canales indirectos o no tradicionales (por ejemplo, el contagio a través de ecosistemas financieros conectados, dependencias de la cadena de suministro, efectos dominó de eventos geopolíticos y la acumulación de riesgos en el mercado).

4.

Desde nuevos productos y modelos comerciales hasta activos y ecosistemas digitales, el crecimiento de los clientes y las estrategias de innovación de productos exigen la atención de los CRO.

Los bancos están invirtiendo en la transformación digital para innovar cuando se trata de nuevos productos y servicios, desarrollando nuevos modelos de negocio y aumentando la eficiencia operativa. Los CRO se enfocan en establecer controles estrictos para estos programas, especialmente cuando tienen un compromiso con terceros, como pueden ser las *FinTechs* o partes de su ecosistemas y plataformas con muchos participantes.

Pero también, deben comprometerse de manera proactiva con los líderes empresariales en la planificación y el diseño de los esfuerzos de transformación para respaldar una toma de decisiones más informada sobre el riesgo e incorporar controles directamente en los procesos digitales. Para hacerlo de la manera más efectiva, los CRO deberán transformar sus propias capacidades y equipos para que sean más ágiles, especialmente dada la presión de lanzar nuevos productos al mercado más rápido. Los CRO que impulsan dicho cambio pueden desempeñar un papel más propicio cuando trabajan con el negocio, en lugar de verse obligados a actuar como una "puerta de peaje" más adelante en el proceso de transformación.

5.

Las gerencias de riesgos buscan equipos más adaptables y ágiles para gestionar los riesgos en todo el negocio y lograr aumentar el rendimiento dentro de sus propias funciones.

La escasez de talento, el aumento de las expectativas de los empleados y el modelo híbrido contribuyen a un mayor riesgo de talento en toda la organización. Por lo tanto, los CRO deben volverse expertos en temas de capital humano y comprometerse con los gerentes de recursos humanos de manera más estratégica y frecuente en los asuntos culturales y del personal. Las gerencias de riesgos también se ven afectadas por estas tendencias y existe presión para agregar nuevas capacidades y fortalecer la cultura a medida que los equipos de riesgo asumen más responsabilidades.

Data Science encabeza la lista de habilidades en demanda, pero los CRO también valoran la agilidad y la adaptabilidad. Específicamente, los CRO necesitan personas que comprendan mejor el negocio y puedan identificar vulnerabilidades correlacionadas en todas las disciplinas de riesgos. Es demasiado pronto para decir si un entorno recesivo aliviará la escasez de mano de obra y la inflación salarial, o en qué medida, se espera que los efectos varíen entre las regiones del mundo.

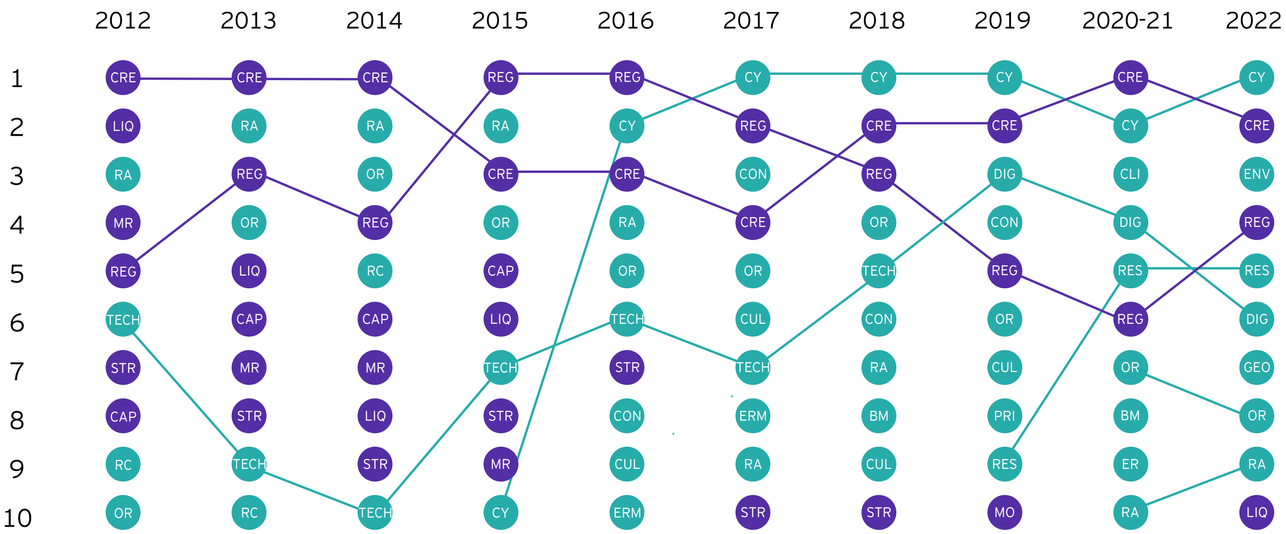
> Lo que se espera de la función de riesgos ha crecido enormemente, incluso en el último año. Realmente tenemos que pensar globalmente sobre las políticas, las regulaciones, los eventos extremos, y modelar sus impactos tanto en términos de conducta como prudenciales. Sin embargo, nuestra función a menudo ha valorado habilidades técnicas limitadas, especializadas y profundas. Los tipos de personas que pueden equilibrar una amplia complejidad son pocos y distantes entre sí.
>
> Gerente de riesgos encuestado

PRINCIPALES PRIORIDADES PARA LOS GERENTES DE RIESGOS

En la "carrera de caballos" anual por la máxima prioridad de riesgo, el riesgo cibernético superó al de crédito. Eso puede deberse a que los bancos cuentan con fuertes controles y reservas de capital y liquidez o porque las gerencias de riesgos sienten que han hecho más durante los últimos doce años para abordar el riesgo de crédito. Sin embargo, el riesgo de crédito puede convertirse pronto en un punto focal si las condiciones económicas empeoran.

Las posiciones fluctuantes del riesgo digital y regulatorio durante los últimos cinco años muestran cuán cambiante ha sido la agenda de los CRO en términos de sus prioridades más urgentes. Si bien estos temas siempre son importantes, en algunos años se volverán menos urgentes a medida que otros temas los desplazan en la agenda de los CRO. El grupo de problemas en el siguiente nivel después del riesgo cibernético y de crédito demuestra la complejidad de riesgos interconectados que enfrentan los CRO en la actualidad.

Gráfico 1: Las 10 principales prioridades de los gerentes de riesgos entre el 2012 y el 2022



LEYENDA

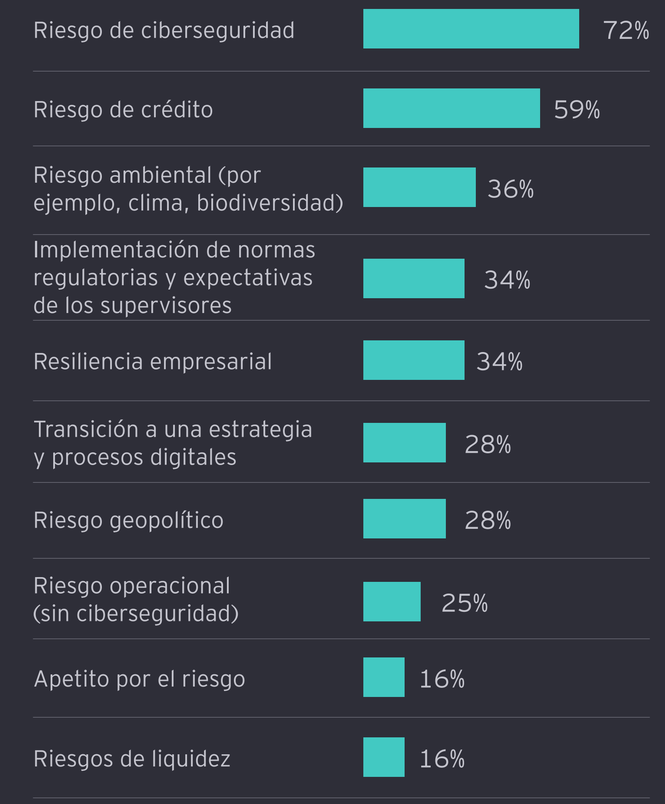
RIESGOS FINANCIEROS

- CAP Manejo de capital regulatorio
- CRE Crédito
- LIQ Liquidez
- MR Riesgo de Mercado
- MO Modelo
- REG Implementación regulatoria
- STR Pruebas de stress

RIESGOS NO FINANCIEROS

- BM Modelo de negocio
- COM Cumplimiento
- CON Conducta
- CUL Cultura
- CY Ciberseguridad
- DIG Transición a estrategias digitales
- ENV Medio ambiente
- ER Riesgos relacionados con los empleados
- ERM Gestión de riesgos empresariales
- GEO Riesgos geopolíticos
- OR Operacional
- PRI Privacidad de los datos
- RA Apetito de riesgos
- RC Control de riesgos
- REP Reputacional
- RES Resiliencia operativa
- TECH Riesgos de arquitectura tecnológica

LAS 10 PRINCIPALES PRIORIDADES DE LOS GERENTES DE RIESGOS PARA LOS PRÓXIMOS 12 MESES



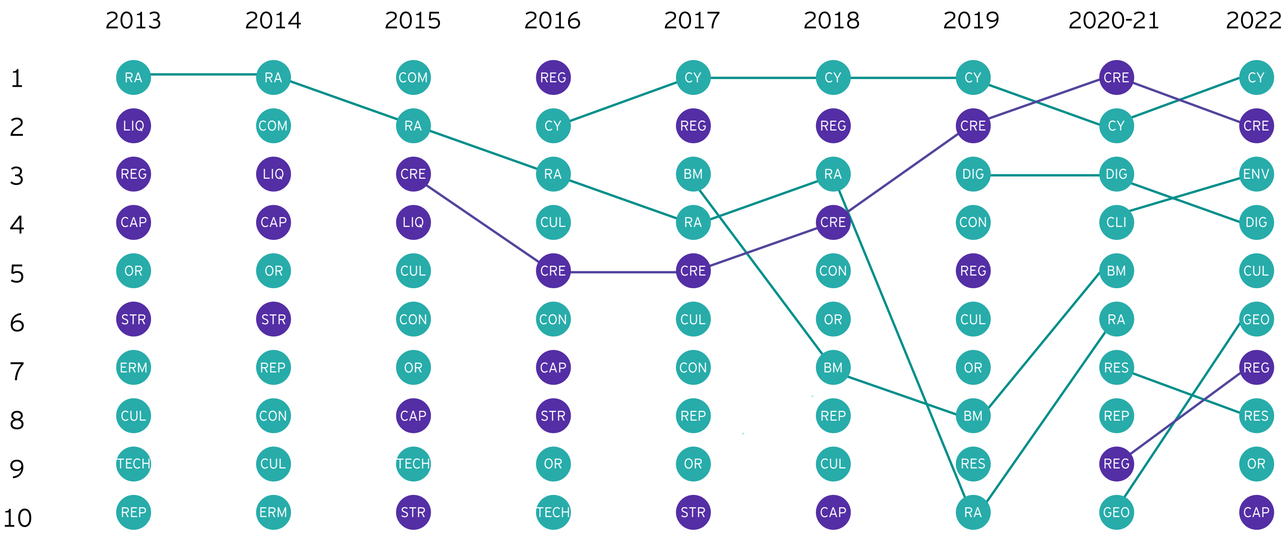
> Cabe destacar que el **83 %** de los bancos de importancia sistémica mundial de nuestra encuesta clasificaron el riesgo geopolítico como la principal amenaza, seguido del riesgo medioambiental y de crédito, ambos con un **58 %.**

Casi dos tercios (62%) de los CRO de los bancos europeos eligieron el riesgo geopolítico como una prioridad principal, cifra superior a sus contrapartes en la región de Asia-Pacífico (28%) y América del Norte (17%). Exactamente un tercio de los encuestados de Asia-Pacífico eligió las pruebas de estrés y más de una cuarta parte (27%) de América Latina eligió el riesgo de modelo, porcentajes mucho más altos que sus pares en otras regiones.

PRINCIPALES RIESGOS DESDE LA PERSPECTIVA DEL DIRECTORIO

Los CRO creen que están alineados en gran medida con los puntos de vista de los Directorios sobre las prioridades de sus riesgos. Están más preocupados por la resiliencia operativa y la implementación regulatoria y están un poco menos preocupados por el riesgo geopolítico de lo que perciben los Directores. Si bien los CRO clasifican el riesgo de liquidez como su décima prioridad más alta, creen que los Directores colocarían el riesgo de capital en esa posición.

Gráfico 2: Las 10 principales prioridades del Directorio entre el 2013 y el 2022



LEYENDA

RIESGOS FINANCIEROS

- CAP Manejo de capital regulatorio
- CRE Crédito
- LIQ Liquidez
- MR Riesgo de Mercado
- MO Modelo
- REG Implementación regulatoria
- STR Pruebas de stress

RIESGOS NO FINANCIEROS

- BM Modelo de negocio
- COM Cumplimiento
- CON Conducta
- CUL Cultura
- CY Ciberseguridad
- DIG Transición a estrategias digitales
- ENV Medio ambiente
- ER Riesgos relacionados con los empleados
- ERM Gestión de riesgos empresariales
- GEO Riesgos geopolíticos
- OR Operacional
- PRI Privacidad de los datos
- RA Apetito de riesgos
- RC Control de riesgos
- REP Reputacional
- RES Resiliencia operativa
- TECH Riesgos de arquitectura tecnológica

Si bien los CRO creen que los Directorios confían en los controles para protegerse contra el riesgo de crédito, es posible que hayan subestimado la creciente preocupación de los Directores sobre el impacto de una recesión. Tres de cada cuatro CRO en los bancos de importancia sistémica mundial dicen que el riesgo geopolítico es el principal problema para los Directores, seguido por el riesgo ambiental y la ciberseguridad, ambos con un 58 %. Los CRO europeos ven a sus directorios mucho más centrados en el riesgo de crédito (77 %) y el riesgo geopolítico (62 %).

LAS 10 PRINCIPALES PRIORIDADES DE RIESGO DEL DIRECTORIO PARA LOS PRÓXIMOS 12 MESES (SEGÚN LOS CRO)

Riesgo de ciberseguridad	72%
Riesgo de crédito	45%
Riesgo ambiental (por ejemplo, clima, biodiversidad)	39%
Transición a una estrategia y procesos digitales	33%
Cultura de la empresa, comportamientos y valores	30%
Riesgo geopolítico	30%
Implementación de normas regulatorias y expectativas del supervisor	25%
Resiliencia operativa	25%
Riesgo operacional (excepto ciberseguridad)	23%
Asignación de capital	23%

RIESGOS EMERGENTES MÁS IMPORTANTES PARA LOS PRÓXIMOS CINCO AÑOS

De cara al futuro, los CRO dicen que se centrarán en gran medida en los mismos riesgos que sus reguladores, aunque las prioridades divergen significativamente cuando se trata de las interrupciones impulsada por las nuevas tecnologías, la obsolescencia de las tecnologías actuales y la privacidad de los datos. Una vez más, los CRO de bancos de importancia sistémica mundial se centran significativamente más en el riesgo geopolítico y la fragmentación regulatoria que sus pares en organizaciones más pequeñas y más de lo que lo perciben los reguladores. Los CRO dicen que priorizarán el riesgo de las nuevas tecnologías y la digitalización en mayor medida que los reguladores, quienes esperan que se centren en la privacidad de los datos y otros problemas de datos. Curiosamente, ningún CRO de los bancos de importancia sistémica mundial seleccionó la privacidad de los datos como un riesgo emergente relativamente importante. Ver gráfico 3.

En cuanto a los puntos de vista regionales, la preocupación por el riesgo climático es más alta entre los CRO en Asia-Pacífico (89 %) y Europa (77 %) y más baja en América Latina (40 %). Los CRO de América del Norte están más preocupadas por la escala del cambio organizacional (67 %), el riesgo climático (57 %) y el ritmo y la amplitud de la digitalización (53 %).

Gráfico 3: Principales riesgos emergentes durante los próximos cinco años

P ¿Qué cinco riesgos emergentes cree que serán los más importantes para su organización en los próximos cinco años?

	General	Banco de importancia sistémica	Banco no de importancia sistémica
Riesgo climático	65%	83%	63%
Disrupciones en la industria debido a nuevas tecnologías	43%	33%	44%
Obsolescencia de TI y sistemas heredados	42%	33%	43%
Ritmo y amplitud del cambio a partir de la digitalización	42%	33%	43%
Riesgo geopolítico	38%	83%	31%
Escala de cambio en toda la organización	36%	25%	38%
Interrupción de la industria debido a nuevos participantes	32%	17%	35%
Integridad de los datos y destrucción de datos	31%	42%	29%
Disponibilidad de datos	27%	17%	29%
Cambios en curso en la cadena de suministro global	20%	17%	21%
Riesgo de modelo relacionado con el aprendizaje automático y la Inteligencia Artificial	18%	17%	18%
Fragmentación regulatoria global	18%	42%	14%
Privacidad de los datos	17%	N/A	19%
Uso de *machine learning* e Inteligencia Artificial	13%	N/A	15%
Interrupción de la industria debido al arbitraje regulatorio	12%	8%	13%
Impactos continuos del ataque ruso a Ucrania en la economía global	10%	17%	8%
Impactos de la desglobalización	10%	25%	7%

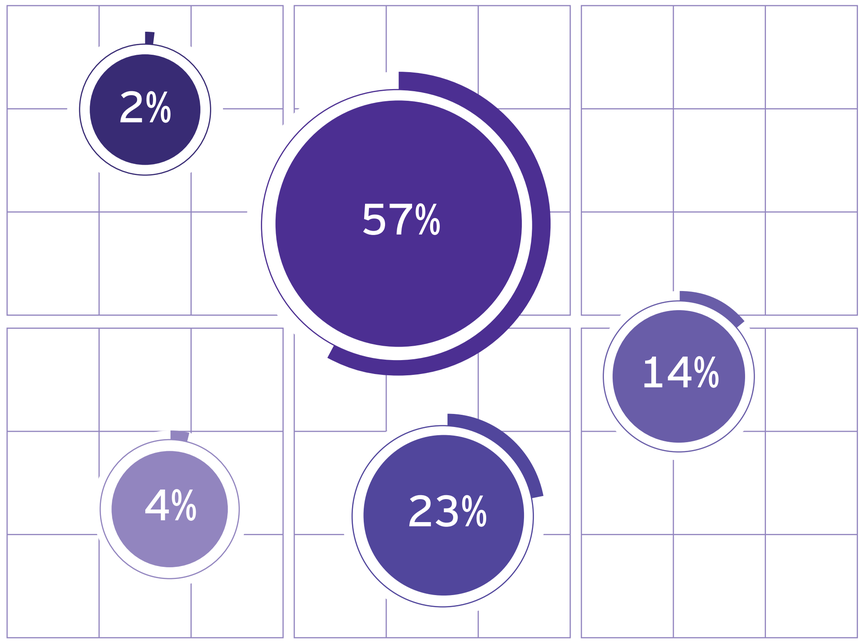
OPINIÓN DE LOS CRO SOBRE EL NIVEL DE CAMBIO EN SUS ORGANIZACIONES

Los CRO parecen confiar en gran medida en la gestión del ritmo de cambio en sus organizaciones. Eso es un testimonio de una década de progreso en el establecimiento de controles sólidos, la creación de nuevas capacidades y la participación más amplia en los debates estratégicos. Los CRO con más confianza se encuentran en Europa (69 %) y Asia-Pacífico (67 %) y las que menos confían en América del Norte (53 %) y Oriente Medio/África del Norte (44 %). Ver gráfico 4.

Gráfico 4: Cantidad de cambio organizacional

P ¿Cómo caracterizaría el nivel de cambio que ocurre en su organización?

- Cada vez me preocupa más que estemos cambiando a un nivel insostenible.
- Muchos cambios, pero confío en que estamos desarrollando las capacidades adecuadas para gestionar el cambio.
- Muchos cambios, pero tenemos las capacidades para gestionarlos.
- Más cambios de lo normal, pero manejables.
- Mismo nivel de cambio que en los últimos cinco años.



01

Las fuerzas y eventos externos encabezan la agenda de las gerencias de riesgos

Al considerar las vulnerabilidades más significativas de sus bancos, los CRO están más preocupadas por los eventos y fuerzas externas que ocurren fuera de los límites de sus organizaciones y que se encuentran en gran medida fuera de su control. Las amenazas a la resiliencia operativa, incluidas las amenazas cibernéticas y los riesgos geopolíticos, se encuentran entre las principales prioridades, al igual que los riesgos de crédito causados por la incertidumbre macroeconómica. Los bancos han hecho extensos preparativos para una gran variedad de escenarios posibles, pero escenarios desconocidos y altamente complejos, aquellos que actualmente parecen inimaginables, pueden representar el mayor riesgo sistémico.

LA UBICUIDAD DE LAS CIBER AMENAZAS

Los CRO ven el riesgo cibernético en todas partes, como lo demuestran ampliamente los resultados de nuestra encuesta. Es inherente a todas las líneas de negocio, en las operaciones diarias y los programas de cambio estratégico clave, y en las extensas redes de socios, proveedores y prestadores de servicios de los que dependen cada vez más los bancos. Además, el creciente interés regulatorio y la probabilidad de nuevos estándares asociados a este tema se suman a la agenda de cada CRO.

La creciente sofisticación de las herramientas y técnicas de piratería y la superficie de ataque en constante expansión de las operaciones están siendo cada vez más digitalizadas, amplificando los riesgos cibernéticos.

Existe una complejidad interna que gestionar cuando los directores pueden no estar completamente familiarizados con los controles cibernéticos existentes y ellos sólo tienen una comprensión limitada de los riesgos; de hecho, los CRO a menudo deben explicar e interpretar los informes detallados proporcionados por el Gerente de Seguridad de la Información (CISO, por sus siglas en inglés).

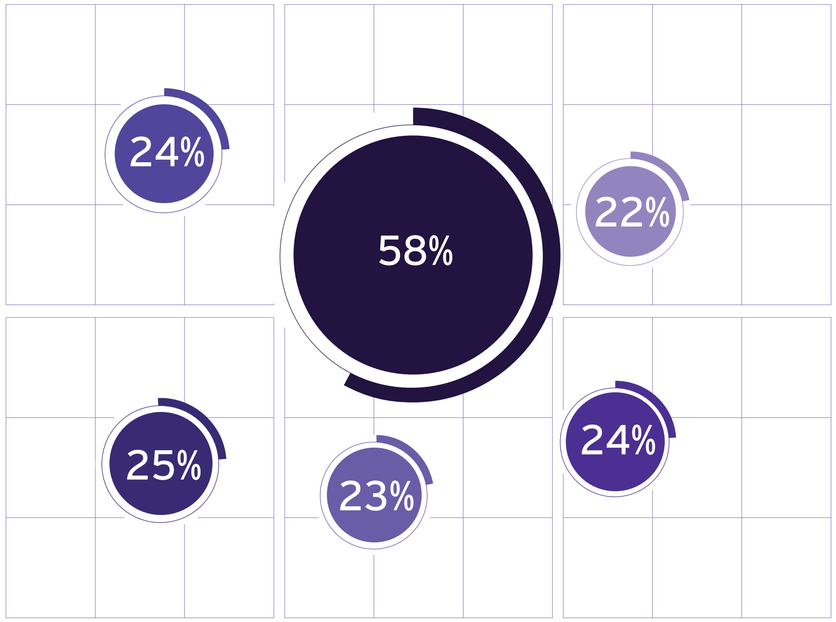
Al igual que con otros riesgos no financieros, el riesgo cibernético causa más preocupación porque los CRO no pueden ver ni administrar todas las vulnerabilidades, particularmente aquellas asociadas con los terceros parte de la organización. Luego están las dificultades de garantizar que los empleados del banco no abran la puerta para atacar; a pesar de todas las herramientas de alta tecnología que tienen los atacantes, el error humano sigue siendo un factor predominante en la mayoría de las infracciones.

El riesgo cibernético es prominente en las agendas tanto a corto como a largo plazo. El hecho de que nuestros encuestados eligieran, en su mayoría, su incapacidad para administrar el riesgo de seguridad cibernética como el principal riesgo estratégico para los próximos tres años sugiere que la presencia y la urgencia de estos no caerán en la agenda de los CRO en el corto plazo, si es que lo hacen. Ver gráfico 5.

Gráfico 5: Principales riesgos estratégicos en los próximos tres años

P ¿Cuáles son los principales riesgos estratégicos que le preocupan en los próximos tres años?

- **58%** Incapacidad para gestionar el riesgo de ciberseguridad.
- **25%** Incapacidad para administrar la nube y el riesgo de datos
- **24%** Incapacidad para gestionar los riesgos ambientales, sociales y de gobernanza
- **24%** Incapacidad para capturar oportunidades ambientales, sociales y de gobernanza
- **23%** Evento(s) importante(s) de continuidad del negocio
- **22%** Incapacidad para gestionar los riesgos de terceros.



CONTEXTO DEL **RIESGO DE CRÉDITO**

Para los bancos globales más grandes, con los modelos de seguridad más robustos y capacidades sofisticadas de detección y respuesta, la principal amenaza proviene de ataques financiados y patrocinados por el Estado que utilizan las técnicas más avanzadas. Es menos probable que los bancos regionales y las instituciones más pequeñas sufran ataques de grupos afiliados al Estado que buscan interrumpir todos sus sistemas, pero pueden estar más expuestos porque los atacantes rechazados por la seguridad efectiva en una empresa simplemente pasan al siguiente objetivo.

Los temas cibernéticos se han vuelto tan omnipresente que algunos CRO buscan alejarse de las unidades aisladas de competencias centradas en la cibernética y, en su lugar, incorporar la experiencia cibernética en cada franja de riesgo y en todos los programas de gestión de riesgos.

También están adoptando tecnologías más poderosas para contraatacar; el 35% de los CRO dicen que están usando la inteligencia artificial y *machine learning* para identificar ataques cibernéticos. Eso es algo bueno, porque los reguladores están poniendo mayor atención a la cibernética después de la pandemia, lo que otorgó una prima a la resiliencia operativa y la planificación de la continuidad del negocio.

Los CRO pueden sentirse alentados por la magnitud del daño de los ataques cibernéticos en Ucrania, que fueron menores a los esperados. Lo mismo ocurre con los ataques a la infraestructura vital, incluidos los sistemas de servicios financieros, de los países que apoyan a Ucrania. La fuerte reserva de talento cibernético del país se vio favorecida por el intercambio de información, tanto con el sector privado como con las agencias de inteligencia, lo que destaca que la seguridad cibernética requiere altos niveles de cooperación y colaboración.

En el momento de la encuesta, la mayoría de los bancos se sentían satisfechos con la calidad de la cartera de préstamos y la estabilidad de las medidas más tradicionales de riesgo de crédito. Los fuertes controles que se han establecido en los 15 años transcurridos desde la crisis financiera mundial le han servido a los bancos y han reforzado la confianza entre el Directorio y las principales gerencias.

Sin embargo, el entorno macroeconómico se encuentra en declive a nivel mundial, probablemente hará que los CRO piensen más sobre el crédito y otros riesgos financieros que lo que han hecho últimamente, con énfasis en abordar las fuentes ocultas de riesgo.

El riesgo de crédito tradicionalmente presentado en el balance general (por ejemplo, la probabilidad de incumplimiento) es generalmente bien conocido, aunque los riesgos asociados con las pérdidas en caso de incumplimiento pueden ser más difíciles de evaluar. Es por eso que, a medida que empeora el entorno se vuelve cada vez más recesivo, los CRO prudentes analizarán más a fondo los "conocimientos conocidos", evaluarán los "conocimientos desconocidos" de manera más amplia e investigarán los riesgos de crédito ocultos que acechan el sistema bancario en la sombra y más allá. Estos riesgos pueden incluir:

- Apalancamiento en mercados privados
- Financiamiento puente
- Rebajas en obligaciones de préstamos garantizados e instrumentos financieros similares

Más allá del sistema bancario en la sombra, los CRO también monitorearán las vulnerabilidades de las contrapartes y la clase de activos, incluidos aquellos que podrían surgir de canales indirectos, que incluyen:

- Ecosistemas financieros conectados
- Efectos dominó de los eventos geopolíticos
- Dependencias de la cadena de suministro

También vale la pena mencionar el riesgo de complacencia, aunque solo sea porque está en la mente de algunos reguladores prominentes que sostienen que el riesgo sistémico a menudo aumenta junto con la confianza en los controles. El declive macroeconómico en curso y la volatilidad periódica del mercado inspirarán a los CRO a mantenerse alerta contra el riesgo de complacencia, tanto dentro de sus propios equipos como en todo el negocio.

> "Actualmente no estoy demasiado preocupado por el riesgo de crédito. ¿Se deteriorará algo el riesgo de crédito? Claro, pero es poco probable que sea una catástrofe o una crisis. Creo que hemos aprendido lo suficiente como industria a través de la crisis financiera. El riesgo financiero no va a ser el próximo gran problema.

> "Nuestra política crediticia es sólida, pero otras áreas del negocio necesitan comprender mejor el apetito por el riesgo del banco.

Gerente de riesgos encuestado

LA DIFICULTAD DE IDENTIFICAR Y GESTIONAR LOS **RIESGOS GEOPOLÍTICOS**

La invasión rusa a Ucrania en febrero de 2022 puso los riesgos geopolíticos en primer plano para los bancos globales. Pero está lejos de ser el único. Las tensiones latentes entre Estados Unidos y China, los conflictos regionales y la retirada de la globalización —o "lentización"— ahora forman parte de los debates sobre el apetito por el riesgo. Los bancos globales más grandes están reevaluando el riesgo de mercado y repensando dónde hacer nuevas inversiones comerciales.

Estos riesgos son únicos, ya que tienen impactos tangibles (por ejemplo, el esfuerzo requerido para cumplir con más sanciones) pero también presentan una gran incertidumbre, lo que obliga a los bancos a determinar sus niveles de comodidad con factores que escapan a su control inmediato.

El malestar social y la política interna son preocupaciones relacionadas. Estos temas han surgido con más frecuencia en nuestras ultimas interacciones con los CRO, altos ejecutivos y miembros del Directorio. "En la arena política, la paciencia escasea a medida que aumenta la polarización", nos dijo recientemente un CRO con sede en EE.UU. "El bajo apetito por la cooperación entre los distintos sectores y la naturaleza del entorno político pueden ser más un motivo de preocupación que los impactos comerciales de los temas políticos actuales". Hemos escuchado muchas opiniones similares de ejecutivos europeos.

El riesgo geopolítico a menudo se manifiesta en forma de un aumento de los ataques cibernéticos, que es la mayor preocupación para los líderes; el número de CRO que citan estos ataques como el principal riesgo geopolítico saltó del 39 % en la encuesta del año pasado al 62 % este año. Algunos bancos están evaluando dónde reubicar los centros de operaciones de seguridad y si deberán trasladar las operaciones fuera de Europa del Este y otras regiones potencialmente vulnerables.

Aquí nuevamente, los CRO de los bancos de importancia sistémica tienen diferentes preocupaciones; el 58 % seleccionó el papel cambiante de China como el principal riesgo geopolítico y solo el 50 % eligió la escalada de los ataques cibernéticos.

Los bancos europeos están más enfocados en la guerra en Ucrania. Ver gráficos 6, 7.

Otras variaciones en nuestros datos resaltan la forma en que el riesgo geopolítico se desarrolla a nivel regional, incluso local. Por ejemplo, los CRO de América del Norte están más preocupadas por la guerra cibernética entre Estados (70 %) que sus pares en Europa (46 %). Los CRO para los bancos de la región de Asia-Pacífico son los que más se centran en los cambios en el entorno comercial mundial (67 %) y en el rol global cambiante de China (78 %).

Los riesgos geopolíticos complican y amplifican otros riesgos y los gerentes de riesgos son muy conscientes de su importancia:

62%

de los encuestados dijo que los riesgos geopolíticos tendrían un efecto "mucho más significativo" o "algo más significativo" en su organización durante el próximo año; para los bancos de importancia sistémica, ese número fue del 84%.

45%

dijo que la volatilidad del mercado por el riesgo geopolítico tendría un impacto "importante" o "moderado a alto" en la exposición al riesgo de mercado.

31%

de todos los encuestados, pero solo el 8% de los CRO en los bancos de importancia sistémica, dijo que la volatilidad del tipo de cambio tendría un impacto "importante" o "moderado a alto" en su exposición al riesgo de mercado.

Gráfico 6: Principales riesgos geopolíticos que afectarán a su organización durante el próximo año

P ¿Cuáles son los principales riesgos geopolíticos que más afectarán a su organización durante el próximo año?

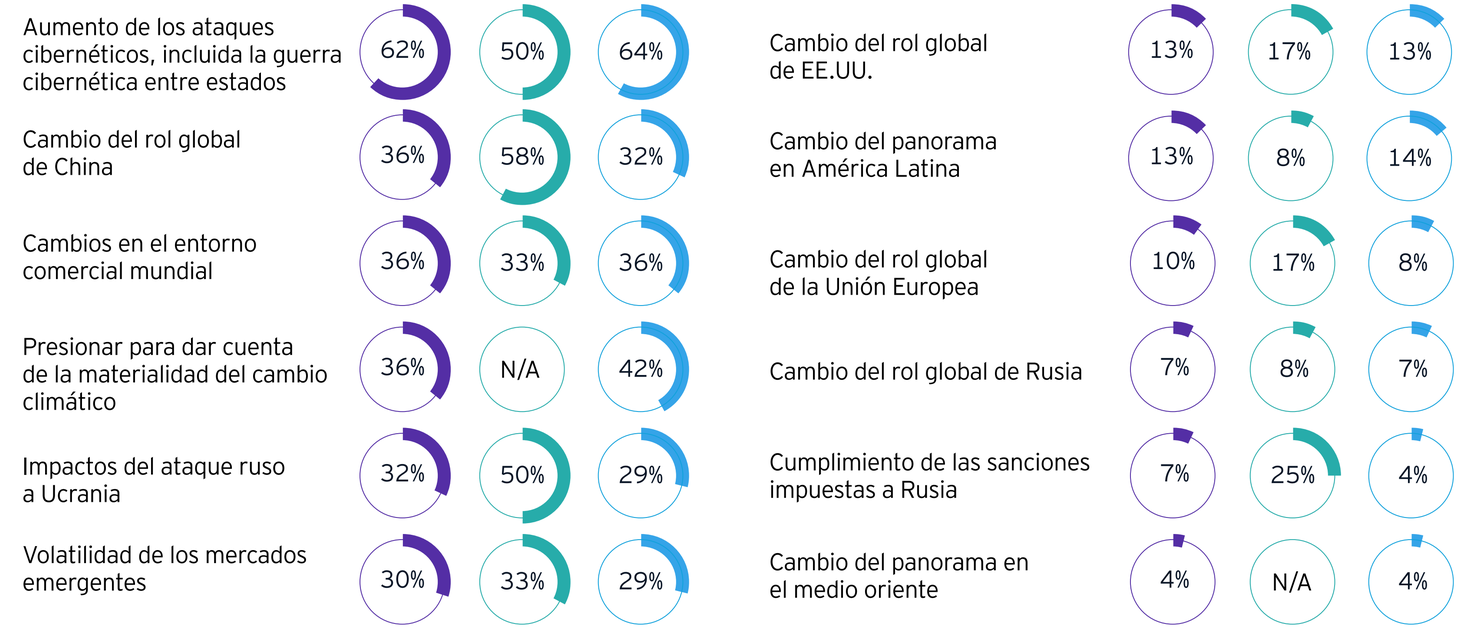
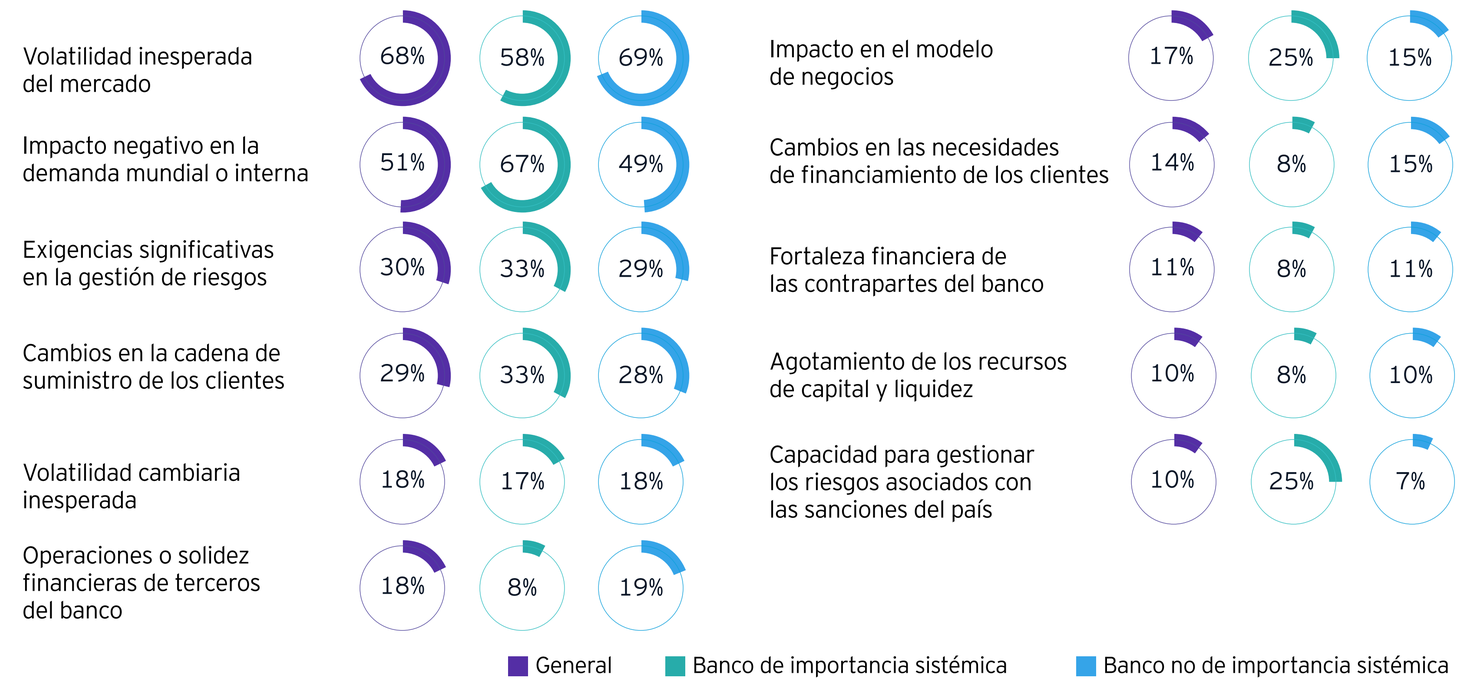


Gráfico 7: Principales impactos de los riesgos geopolíticos

P ¿Cuáles son las principales formas en que su organización podría verse afectada por los riesgos geopolíticos?

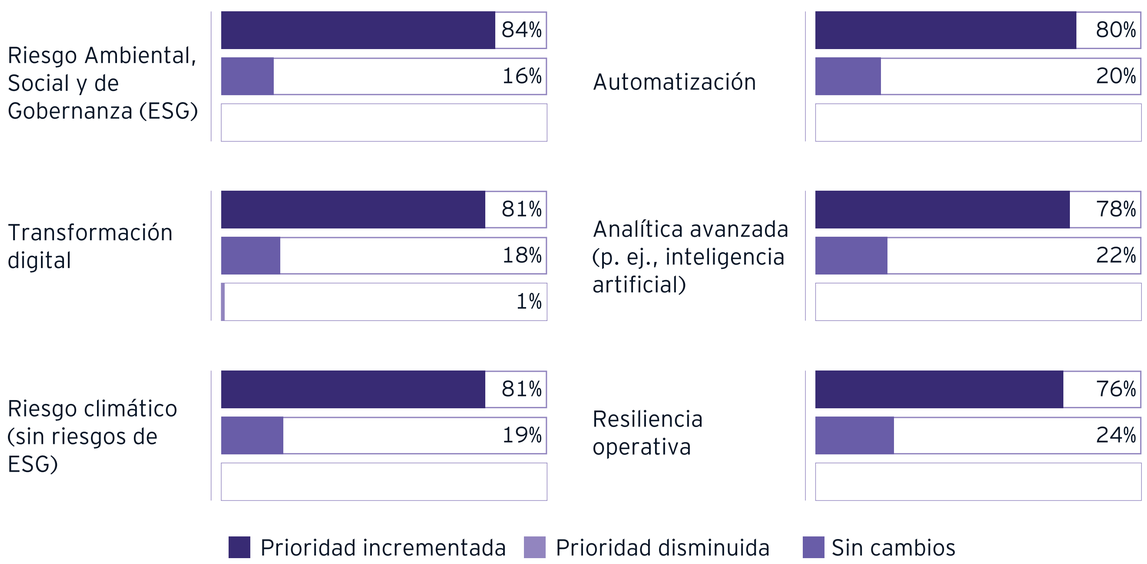


Aunque la pandemia y las preocupaciones geopolíticas han generado más titulares estos últimos años, el riesgo climático sigue siendo uno de los tres principales riesgos tanto para los Directores como para los CRO durante los próximos 12 meses. En la encuesta de este año, solo el 36% de los CRO mencionaron el riesgo ambiental como uno de los cinco problemas principales que demandarán de su atención los próximos 12 meses, en comparación con el 49% de los encuestados del año pasado. Es probable que esta caída sea debido a la urgencia en torno a los riesgos cibernéticos y geopolíticos. También vale la pena señalar que el 58% de los CRO de los bancos de importancia sistémica seleccionaron el riesgo ambiental como uno de sus cinco principales puntos focales.

Sin embargo, de cara al futuro, los CRO esperan que los riesgos ambientales, sociales y de gobierno corporativo (ESG, por sus siglas en inglés), de transformación digital y climáticos experimenten el mayor aumento de prioridad durante los próximos 36 meses. Ver gráfico 8. Claramente, el riesgo climático y ambiental, en sus múltiples formas, todavía está en la mente de los CRO y es probable que la gravedad y la frecuencia de los desastres naturales lo mantengan. La guerra en Ucrania también plantea cuestiones ambientales relacionadas con la matriz energética europea y la necesidad de expandir el uso de los combustibles fósiles. Para los CRO, el enfoque seguirá estando en el desarrollo de mejores medidas y modelos de riesgos climáticos (incluidos los riesgos físicos y los asociados con la transición a una economía más verde) con el fin de lograr una suscripción de crédito más efectiva.

Gráfico 8: Áreas de riesgo que probablemente aumentarán su prioridad en los próximos tres años

P Para cada una de las siguientes áreas de enfoque de riesgo, indique si aumentará en prioridad, disminuirá en prioridad o no habrá cambios en los próximos tres años.



Los resultados de nuestra encuesta dejan en claro cuánto trabajo queda para los CRO. Un 84% de los encuestados dijo que sus bancos tenían un "conocimiento preliminar", (51%) o un "conocimiento algo completo" (33%) de las exposiciones climáticas. Ver gráfico 9.

Gráfico 9: Madurez de la comprensión de la exposición al riesgo climático, incluidos los riesgos físicos y de transición

P ¿Cómo caracterizaría la madurez de su comprensión de su exposición tanto a los riesgos físicos del cambio climático como a los riesgos de transición?

No es sorprendente que los bancos de importancia sistémica tengan capacidades más sólidas para incorporar factores climáticos en las actividades de gestión de riesgos. Por ejemplo, el 92% cita el modelado de escenarios y las pruebas de estrés como actividades importantes para incorporar el riesgo climático en su enfoque más amplio de gestión de riesgos, en comparación con el 28% de otros bancos. La mitad de los CRO en los bancos de importancia sistémica dicen que los riesgos del cambio climático son inherentes a las evaluaciones de exposiciones crediticias materiales, en comparación con un tercio de otros bancos.

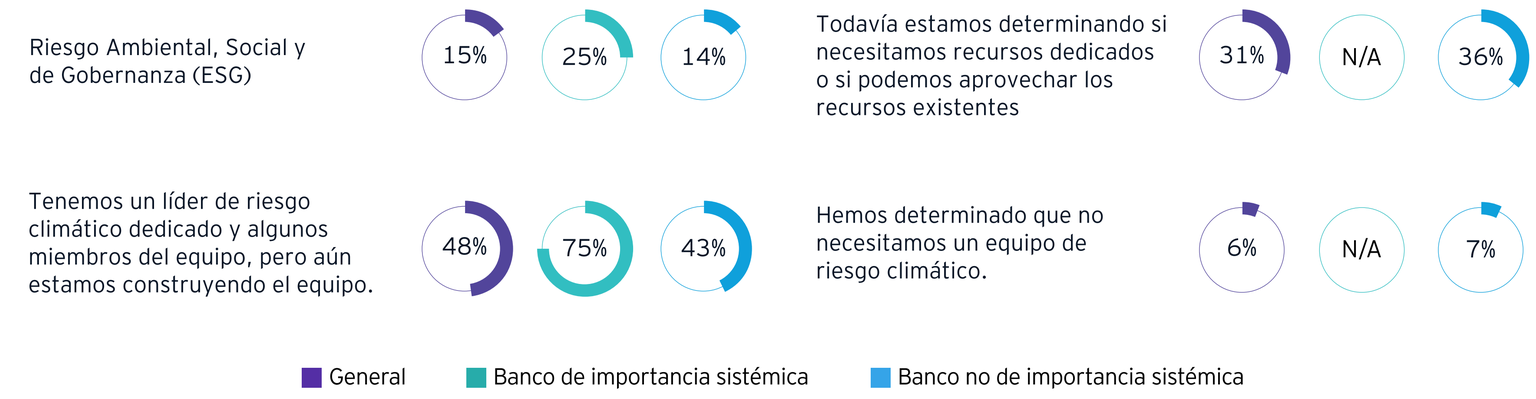
Mirando hacia un horizonte de cinco años, el 65% de los CRO mencionaron el riesgo climático como la preocupación más importante para sus organizaciones, muy por delante de la disrupción impulsada por la tecnología (42%), la obsolescencia de TI (42%) y el ritmo y la amplitud del cambio de la digitalización (42%). La implicación es que estos últimos riesgos parecen más manejables para los CRO, en comparación con los riesgos ambientales, que incluyen tanto amenazas físicas como las interrupciones causadas por la transición a una economía más verde.

Satisfacer los requisitos reglamentarios y madurar las capacidades: de manera similar, el 71% espera que el riesgo climático sea una preocupación para los reguladores durante los próximos cinco años, muy por delante de las preocupaciones relacionadas con la privacidad de los datos (40%) y el ritmo y la amplitud de la digitalización (37%).

Dada la naturaleza de gran alcance del riesgo climático, no sorprende que casi la mitad de los CRO esperan que el riesgo climático se convierta en una prioridad mayor durante los próximos tres años. Los bancos están tomando una serie de medidas; casi la mitad (48%) de todos los bancos y las tres cuartas partes de los CRO de los bancos de importancia sistémica dicen que están desarrollando sus equipos de riesgo climático. Véase la gráfico 10. También esperaríamos que la mayoría del 31% que aún evalúa sus necesidades eventualmente determine que necesita más recursos dedicados.

Gráfico 10: Madurez de los equipos de gestión de riesgos climáticos de segunda línea

P ¿Cómo caracterizaría la madurez de su equipo de gestión de riesgos de riesgo climático de segunda línea?



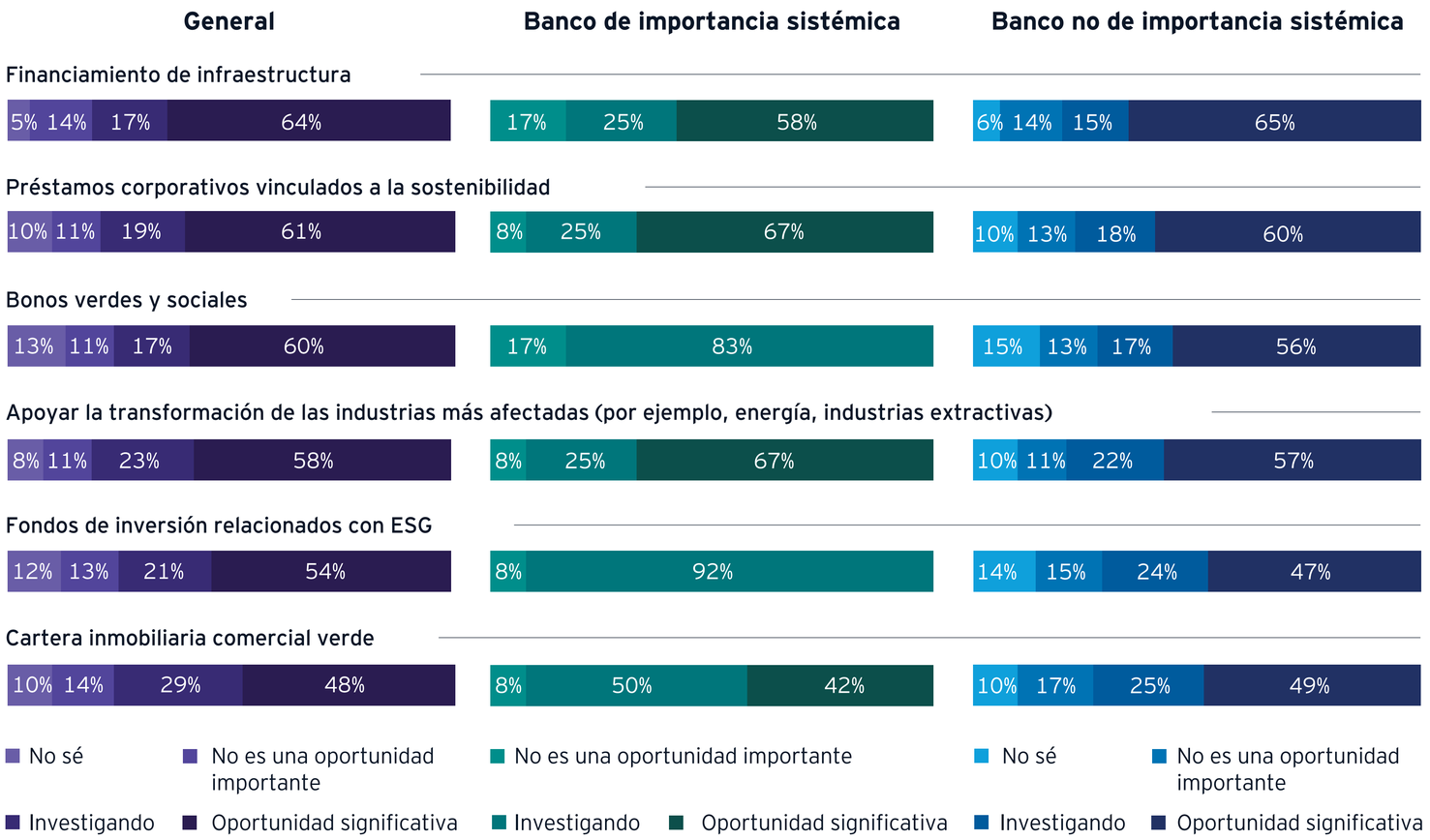
Además, las actividades futuras ciertamente incluirán respuestas a los nuevos requisitos regulatorios, especialmente en los EE. UU.; se espera que la Oficina del Contralor de la Moneda (OCC, por sus siglas en inglés) actualice su borrador de Principios para la Gestión de Riesgos Financieros Relacionados con el Clima para Grandes Bancos. Las propuestas de la Comisión de Bolsa y Valores (SEC, por sus siglas en inglés) han llevado a los equipos de finanzas y riesgo a colaborar en la presentación de informes sobre divulgaciones voluntarias. En otras palabras, los CRO no actuarán solos al abordar las dimensiones regulatorias del riesgo climático.

La ventaja de ESG:

Si bien el riesgo climático se considera principalmente como una amenaza externa, los CRO también lo ven a través de las iniciativas ESG, que se extienden desde los requisitos de informes hasta el desarrollo de nuevos productos. Los CRO consideran que la financiación de infraestructuras, los préstamos corporativos vinculados a la sostenibilidad y los bonos verdes y sociales son los productos que ofrecen el mayor potencial de crecimiento relacionado con ESG. Véase la gráfico 11. Los bancos de importancia sistémica ven un potencial mucho mayor con los bonos verdes y los fondos de inversión ESG.

Gráfico 11: Productos con la mayor cantidad de oportunidades de crecimiento relacionadas con ESG

P ¿Qué productos considera su empresa que tienen oportunidades de crecimiento asociadas con ESG?

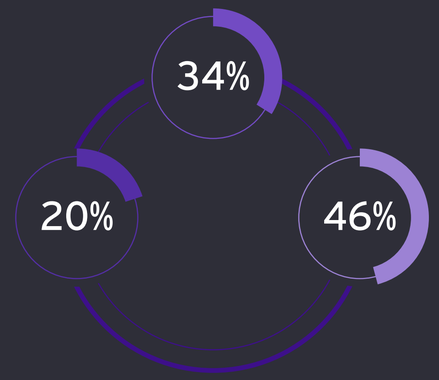


La importancia del financiamiento de la infraestructura destaca cómo la transición a una economía baja en carbono está en la mente de los CRO y los líderes bancarios. Las prioridades de los productos evolucionarán en función de las regulaciones, así como de las percepciones de qué ofertas ecológicas pueden tener un impacto significativo en el desempeño financiero. Estas consideraciones variarán según la región y el tamaño y la estructura de la organización.

Nuestros resultados indican que todavía hay trabajo por hacer en el diseño de taxonomías sólidas y enfoques de monitoreo para productos ESG. Ver gráfico 12. Estas medidas serán especialmente importantes para que los bancos naveguen por el creciente interés regulatorio en los productos ESG y eviten cargos de *greenwashing*.

Gráfico 12 Enfoques actuales para el seguimiento de los riesgos relacionados con los productos y servicios ESG

P ¿Qué tan seguro está de que su banco tiene un enfoque sólido para rastrear qué productos y servicios deben considerarse relacionados con ESG?



20% Hemos adoptado una taxonomía robusta para identificar todos los productos y servicios relacionados con ESG

34% Hemos adoptado una taxonomía robusta para ciertos productos y servicios (por ejemplo, bonos verdes), pero no para todos

46% Todavía estamos en una etapa temprana para determinar qué productos y servicios deben considerarse relacionados con ESG

CAPÍTULO

02

El imperativo de la transformación digital y otras presiones internas presentan desafíos únicos y serios

Así como los diferentes tipos de riesgos externos están cada vez más correlacionados, los riesgos internos también suelen superponerse. Y aunque los CRO suelen tener mayor urgencia en abordar los riesgos internos, también deben considerar estos vínculos e intersecciones complejas.

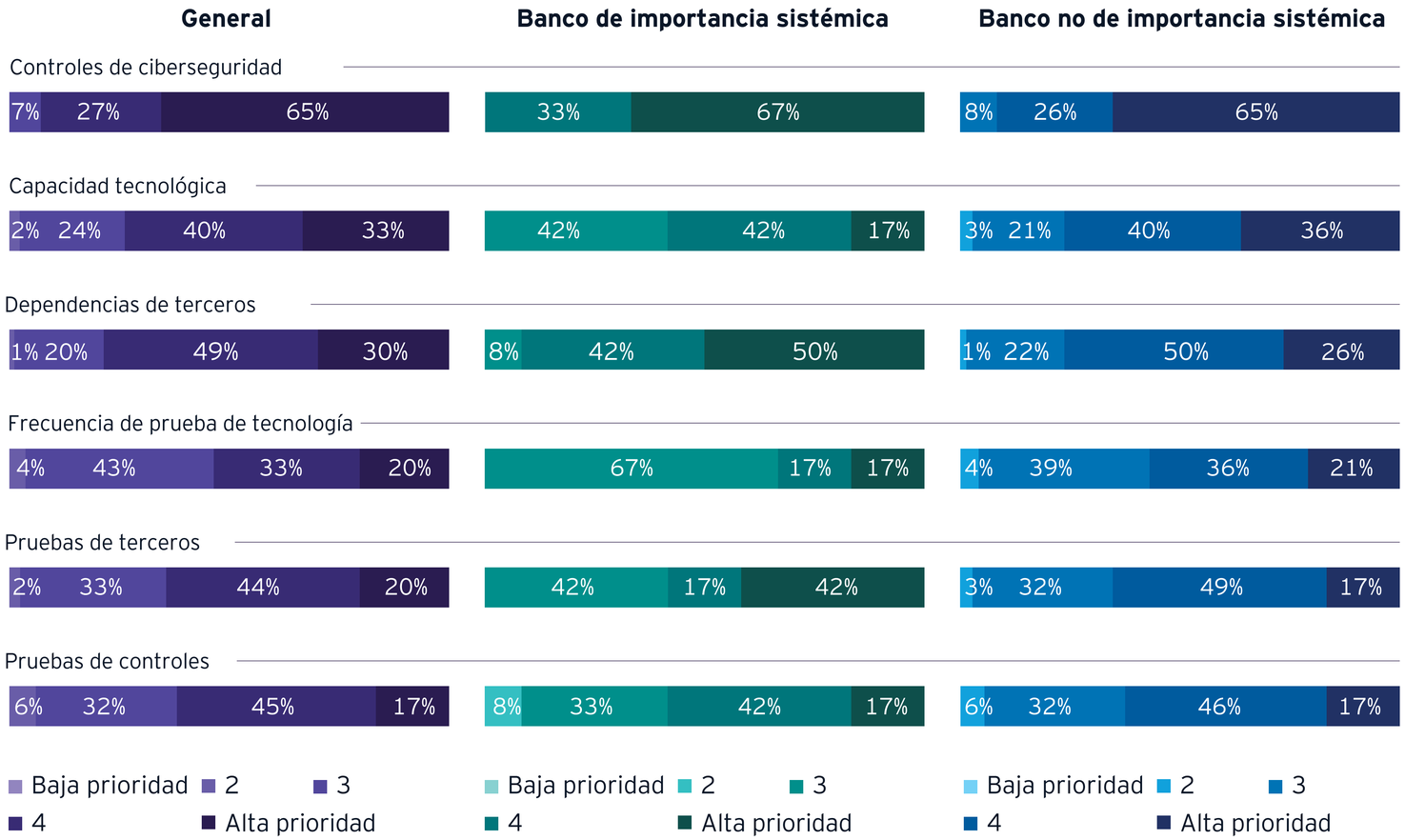
LAS MÚLTIPLES FORMAS DE **RESILIENCIA OPERATIVA**

Es bueno que los bancos hayan trabajado e invertido para aumentar su resiliencia operativa en los últimos años, porque actualmente hay más amenazas que nunca. Por lo tanto, los CRO ahora tienen una visión integral de la resiliencia operativa, desde las preocupaciones relacionadas con la ciberseguridad y la tecnología hasta los riesgos de terceros.

Los controles cibernéticos son la máxima prioridad para impulsar la resiliencia operativa, seguidos de la capacidad tecnológica y las dependencias de terceros. Más del 50% de los CRO de los bancos de importancia sistémica consideran que las dependencias de terceros son una prioridad más alta que sus contrapartes en bancos de tamaño medianos (26%). Véase la gráfico 13. Eso no es una sorpresa, dada la mayor dependencia de los bancos más grandes en sus ecosistemas y asociaciones. A medida que los bancos medianos buscan expandir su uso de la subcontratación en el futuro, pueden aumentar sus preocupaciones sobre la resiliencia en relación con terceros.

Gráfico 13: Prioridades para las mejoras de resiliencia operativa en los próximos tres años

P ¿Qué nivel de prioridad le asignaría a cada una de las siguientes áreas de resiliencia operativa para mejoras durante los próximos tres años?

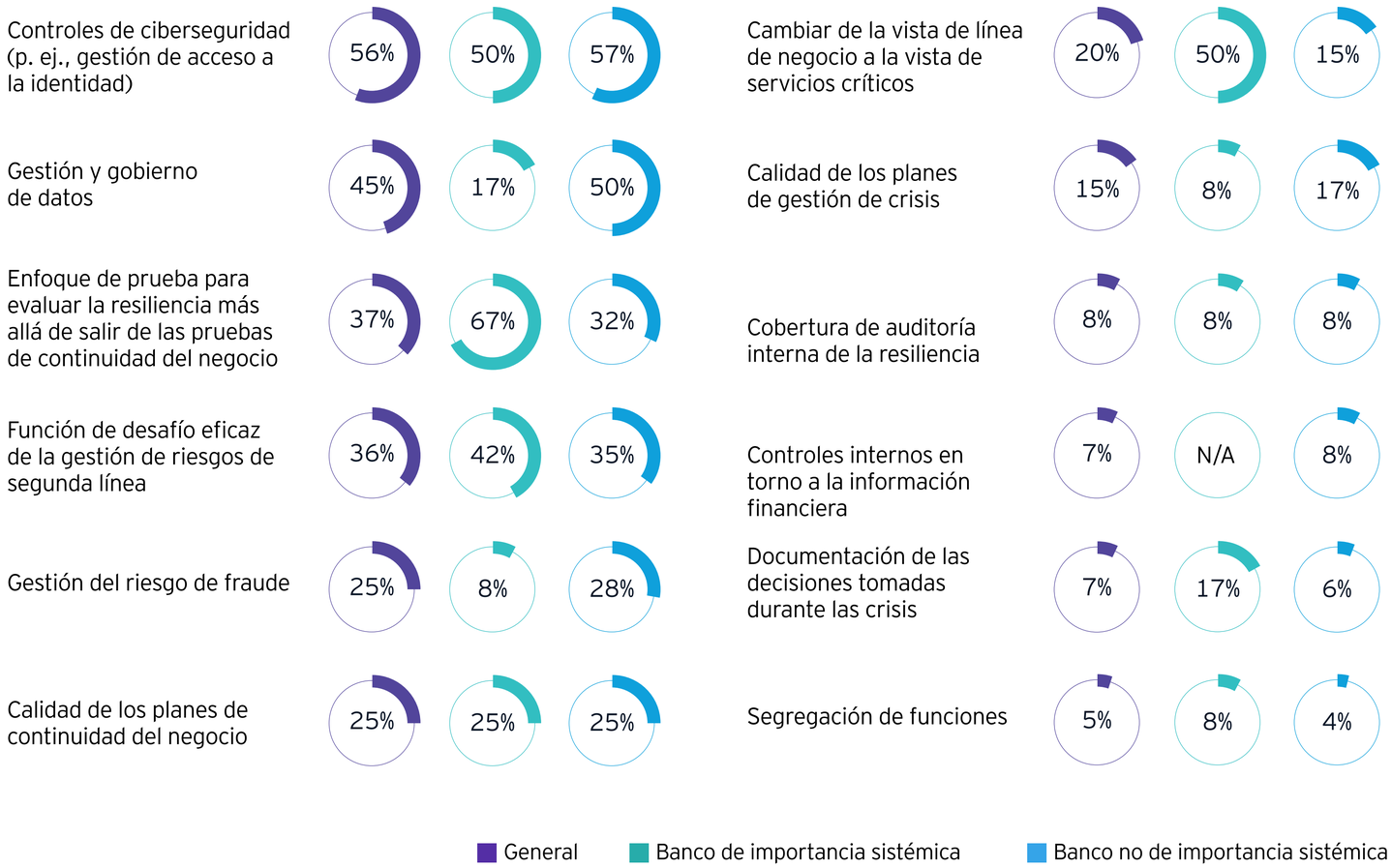


La ciberseguridad también encabeza la lista de las áreas para mejoras en el entorno de control de riesgos que los CRO esperan realizar. Eso es cierto para todos los tipos y tamaños de bancos, aunque surgen otras diferencias en los resultados de nuestra investigación. Por ejemplo, el 50% de los bancos medianos priorizan la gestión y el gobierno de datos, mientras que solo el 17% de los bancos de importancia sistémica lo hacen. Es posible que los bancos globales más grandes ya hayan realizado estas inversiones necesarias, y sus pares regionales pueden estar buscándolos en busca de lecciones aprendidas y prácticas líderes.

Por el contrario, es mucho más probable que los bancos de importancia sistémica (50%) prioricen el alejamiento de las perspectivas de línea de negocio que los bancos de tamaño mediano (15%). Además, los bancos más grandes pueden estar siguiendo un enfoque basado en los riesgos cuando se trata de fortalecer el entorno de control. Ver gráfico 14.

Gráfico 14: Prioridades para las mejoras del entorno de control para fortalecer la resiliencia operativa

P ¿Qué mejoras planea realizar en su entorno de control para fortalecer la resiliencia operativa?



Es posible que se requieran nuevos controles para actualizar las protecciones de la infraestructura tecnológica. Muchas políticas existentes se diseñaron para ataques físicos y se establecieron después de los atentados del 11 de septiembre. Dado que los riesgos cibernéticos ahora son una prioridad principal, los planes de continuidad comercial deben actualizarse regularmente para garantizar que los procesos de respaldo y recuperación puedan resistir ataques y prevenir nuevas vulnerabilidades.

La gestión de riesgos de terceros es una prioridad permanente, aunque está lejos de ser una disciplina estática. Los ataques de alto perfil que explotan los eslabones débiles en las redes de proveedores o la cadena de valor tienden a hacer que el riesgo de terceros destaque en la agenda. La mayor digitalización y la interconectividad del negocio bancario hacen que el riesgo de terceros sea una gran amenaza para la resiliencia operativa de todas las empresas que participan en el ecosistema financiero más amplio.

Si necesitaran más razones para centrarse en la resiliencia

> La resiliencia operativa es clave, pero la mayoría de los bancos todavía luchan con ella porque es complicada y un objetivo móvil. Los reguladores están subiendo la temperatura y esperan que seamos perfectos en la prestación de servicios al consumidor.
>
> Gerente de riesgos encuestado

operativa, casi la mitad (48%) de los CRO esperan requisitos adicionales para monitorear a los proveedores de servicios externos, además de que los reguladores eleven sus estándares de ciberseguridad en los próximos dos años (48%) y estándares más altos para la protección de datos (47%). Ver gráfico 15.

Gráfico 15: Requisitos adicionales de resiliencia operativa esperados de los reguladores durante los próximos dos años

El mayor costo de los controles: dada la creciente necesidad de controles más sólidos, no sorprende que el 85% de los encuestados espere que el costo de los controles aumente en los próximos tres años; casi un tercio (32%) espera aumentos superiores al 15%. El año pasado, solo el 69% de los CRO dijeron que esperaban costos más altos y un porcentaje significativo de los encuestados esperaba una disminución, esto se puede haber dado por una mayor automatización.

El aumento esperado en el costo de los controles se puede atribuir en parte a la expansión del mandato de la gestión de riesgos y a la lista cada vez más larga de responsabilidades. Sin embargo, la perspectiva de recortes de empleos y medidas de reducción de costos en el caso de una recesión económica prolongada puede impedir una mayor inversión en los controles o, de hecho, la función de gestión de riesgos en su conjunto.

Según los CRO, las nuevas regulaciones y expectativas de supervisión (56%), la transformación tecnológica acelerada (56%) y una ciberseguridad más amplia (53%) son los principales impulsores de los aumentos de costos. En particular, el principal impulsor de costos del año pasado (la necesidad de automatizar los procesos manuales) cayó al cuarto lugar este año, con un 40%, frente al 76% de la encuesta de 2021. La implicación es que ya se han realizado inversiones en automatización. Sin embargo, es posible que los bancos se estén dando cuenta de que los costos más bajos de la automatización pueden no compensar la necesidad de invertir en nuevas capacidades, más personal y controles más sólidos.

LOS RIESGOS CRECIENTES RELACIONADOS A LOS PROGRAMAS DE TRANSFORMACIÓN NECESARIOS

Los bancos buscan canales digitales tanto para el crecimiento futuro como para una mayor eficiencia operativa, lo que explica el amplio alcance y el rápido ritmo de los programas de transformación en todo el negocio. Estos programas también son esenciales para la innovación de los productos y servicios y el desarrollo de nuevos modelos de negocio. Como tal, la transformación digital es una oportunidad para que los CRO interactúen con los demás líderes de una manera más favorable, en lugar de restrictiva.

Por ejemplo, los CRO pueden intentar integrar la medición, el seguimiento y los controles de riesgos directamente en los procesos de manera que no comprometan la eficiencia ni la experiencia del cliente. Colaborar con la empresa para planificar programas de transformación o diseñar nuevas ofertas también presenta a los CRO la oportunidad de demostrar su conocimiento y perspectiva sobre los riesgos.

Para acelerar la transformación digital, los bancos se centrarán en la modernización de las plataformas centrales, la generación de información sobre los clientes, la automatización de un mayor número de procesos y el traslado de un mayor número de operaciones a la nube. Ver gráfico 16.

Los CRO en América Latina informan que los bancos están priorizando los conocimientos de los clientes (80%) y la migración y adopción de la nube (80%) sobre la modernización de las plataformas principales (33%).

Gráfico 16: Principales formas en que la transformación digital se acelerará en los próximos tres años.

P ¿Cuáles son las principales formas en que su banco acelerará la transformación digital en los próximos tres años?

A pesar de lo claro y convincente que es el caso comercial, estas iniciativas también presentan nuevos riesgos que deberían estar en los radares de los CRO. Nuestros resultados muestran que los CRO prestan mucha atención a los esfuerzos de transformación digital, poniendo énfasis en establecer los controles correctos, especialmente en relación con las estrategias de los activos digitales.

Paciencia con los activos digitales: los CRO parecen estar en modo de "esperar y ver" en relación de las estrategias de los activos digitales, una postura que refleja en gran medida la de las gerencias. Casi la mitad (49%) de los bancos todavía están definiendo sus estrategias de activos digitales. Más allá de los bancos de importancia sistémica, pocas organizaciones han comenzado a ejecutar sus planes.

	Todos los encuestados	Banco de importancia sistémica
Habilitar compras de activos digitales	19%	33%
Procesar pagos y liquidaciones de activos digitales	15%	42%
Facilitar las inversiones en activos digitales	14%	33%
Apoyar los esfuerzos de la industria para mejorar la aceptación de los activos digitales	13%	42%

La implosión de los grandes intercambios de criptomonedas en otoño del 2022 sirvió como un recordatorio de la necesidad de contar con prácticas sólidas de gestión de riesgos en las empresas nativas digitales, *FinTechs* y en todas las empresas de servicios financieros no tradicionales. La incertidumbre regulatoria seguirá siendo una barrera formidable para una mayor actividad y desarrollo de soluciones, incluso si los CRO reconocen que el negocio se sentirá atraído por el potencial transformador de la tecnología de contabilidad distribuida para optimizar los procesos administrativos clave.

Aún así, los CRO entienden que deberán tomar medidas en varios frentes, incluida la política, la tecnológica, la capacitación y el talento, cuando los activos digitales finalmente se conviertan en una característica más común en las carteras bancarias. Casi todos los CRO de los bancos de importancia sistémica esperan tales cambios. Ver gráficos 17, 18.

> Podríamos jugar en el espacio de los activos digitales, pero los reguladores no están familiarizados. Nos mantendremos al margen hasta que tengamos una buena comprensión de lo que podemos hacer con ellos como banco y cuál es un servicio o solución apropiado para ofrecer a nuestros clientes y con el que nuestros reguladores se sientan cómodos.
>
> Gerente de riesgos encuestado

Gráfico 17: Principales cambios que deberán realizar en su enfoque de gestión de riesgos empresariales para abordar los riesgos asociados con la estrategia de activos digitales de su banco.

P ¿Cuáles son los principales cambios que deberá realizar en su enfoque de gestión de riesgos empresariales para abordar los riesgos asociados con la estrategia de activos digitales de su banco?

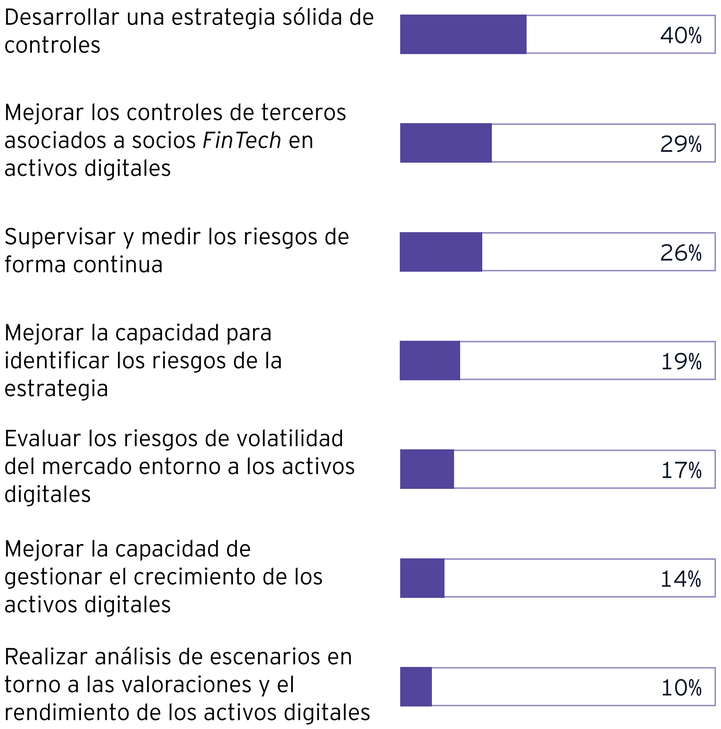
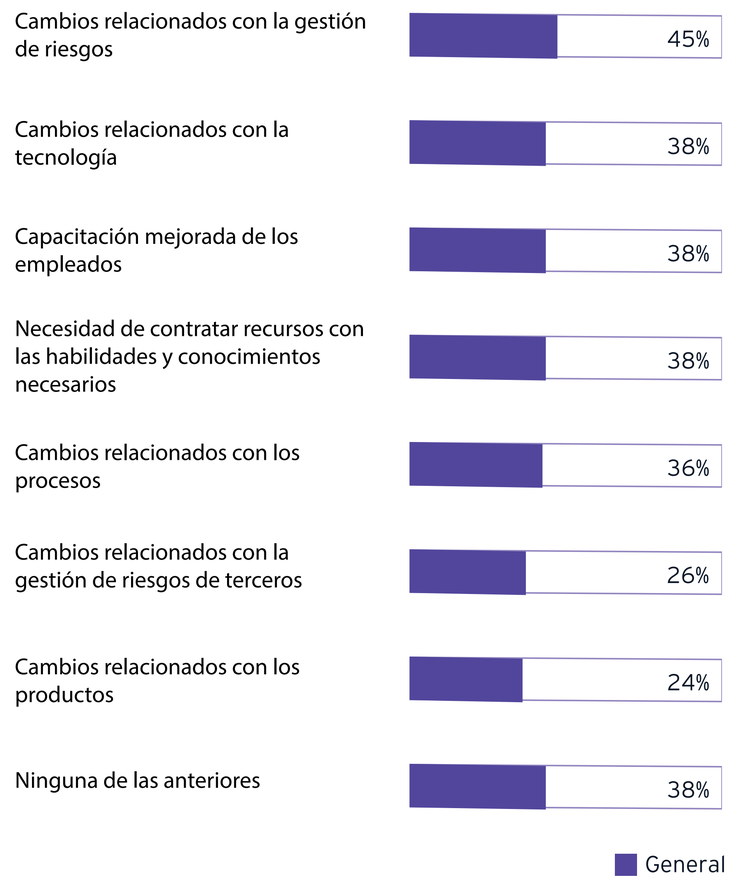


Gráfico 18: Cambios necesarios para gestionar los riesgos asociados con las estrategias de activos digitales.

P ¿Qué cambios deberá hacer su banco para gestionar los riesgos asociados con su estrategia de activos digitales?



El imperativo de crecer a través de la innovación del modelo de negocio apunta inevitablemente a más operaciones digitales. Sin embargo, cuanto más digital es un banco, más vulnerable es. Esa tensión justifica la estrecha participación de los CRO en los debates estratégicos clave con los líderes del negocio.

EL PERFIL DE RIESGO DE LAS ALIANZAS Y LOS ECOSISTEMAS

La transformación digital proporciona una base para que los bancos crezcan a través de ecosistemas y estrategias de alianza. De hecho, casi dos tercios de los bancos (65%) están ejecutando o desarrollando estrategias para sus ecosistemas. Casi la misma cantidad (63%) se enfoca en la adquisición de clientes en su ecosistema y estrategias de alianza. Casi nueve de cada diez CRO (86%) en Asia-Pacífico dicen que la adquisición de clientes es la máxima prioridad para las alianzas y los ecosistemas. Para los bancos norteamericanos, el aumento de la eficiencia y la reducción de los costos son el principal objetivo de los ecosistemas y las alianzas, según el 70% de los CRO.

Todos los beneficios potenciales de los ecosistemas y las alianzas van acompañados de un mayor riesgo. La ciberseguridad y la privacidad de los datos son las principales prioridades en relación con los ecosistemas y las alianzas, aunque existen otros problemas potenciales para rastrear, especialmente el riesgo de terceros y cuartas partes. Véase la gráfico 19. Así como el éxito de los ecosistemas depende en gran medida de la fortaleza de los participantes, las vulnerabilidades de los bancos dependen de las prácticas de seguridad y privacidad de datos de sus socios. Estos riesgos pueden variar considerablemente en función de las diferentes estrategias (desarrollo y orquestación completos del ecosistema, inversiones directas en empresas conjuntas, alianzas menos estrictas) que pueden adoptar los bancos. También varían según la región: solo el 40% de los CRO de los bancos en Europa citan la ciberseguridad como uno de los principales riesgos del ecosistema, frente al 77% de sus pares en Oriente Medio y África del Norte.

Gráfico 19: Principales riesgos que requerirán la mayor atención de los CRO en los próximos tres años con respecto al ecosistema y las estrategias de alianza.

P ¿Cuáles son los principales riesgos que requerirán la mayor atención del CRO con respecto a su ecosistema y estrategia de alianza en los próximos tres años?

La mitad de los CRO esperan que los nuevos requisitos regulatorios sobre las alianzas con las FinTechs tengan un impacto moderado o importante en estas estrategias; el mismo número espera un impacto mínimo o nulo. Los bancos globales más grandes están más preparados para hacer frente a los nuevos requisitos y están más enfocados en los riesgos de terceros y cuartas partes, presumiblemente porque estarán involucrados en ecosistemas más grandes. Lo que está mucho más claro es que los ecosistemas y las alianzas llegaron para quedarse y los CRO se centrarán más en ellos en los próximos años.

RIESGO DE TALENTO PRESENTE EN TODA LA EMPRESA

Por mucho que el negocio bancario se esté digitalizando y automatizando, la gran mayoría de los CRO, junto con sus pares de las gerencias, ven el talento como temas fundamental para el éxito futuro.

En primer lugar, los bancos aún luchan por atraer el talento que necesitan, tanto en la función de gestión de riesgos (consulte el capítulo 3) como en todo el negocio. No está claro cuánto, en todo caso, una recesión podría debilitar el mercado laboral. Pero el hecho de que las unidades de negocio y las funciones (sin mencionar a los CRO) busquen científicos de datos, analistas de datos y otras habilidades orientadas a la tecnología es un argumento para mejorar las habilidades.

Los CRO ven los riesgos de talento y cultura para el negocio desde perspectivas a corto y largo plazo, y desde múltiples ángulos. Consulte la gráfico 20. Trabajo remoto e híbrido, bienestar mental, uso más generalizado de relaciones y alianzas con terceros: todo esto está relacionado con la escasez continua de talento que los bancos están experimentando en todo el negocio.

Gráfico 20: La importancia de los riesgo de talento para los bancos

P ¿Qué tan importante es el riesgo de talento para su banco y la industria bancaria?

> Me preocupa tener las habilidades adecuadas y atraer talento, pero también el capital humano como riesgo de resiliencia.
>
> Gerente de riesgos encuestado

El hecho de que más CRO ahora consideren el talento como una cuestión de resiliencia operativa ilustra cuán urgente se ha vuelto el riesgo de talento. Incluso los cambios estratégicos ahora se ven en términos de competir por el talento. De hecho, el 49% de todos los encuestados mencionaron una mayor capacidad para atraer y retener talento como una de las tres razones principales para mejorar el modelo de negocio en los próximos tres años, solo detrás de la implementación de las principales tecnologías (65%) y la mejora de la rentabilidad (61%).

Ese número refleja la realidad de que la planificación estratégica de la fuerza laboral ahora es un asunto de la alta gerencia y las juntas, además de los recursos humanos.

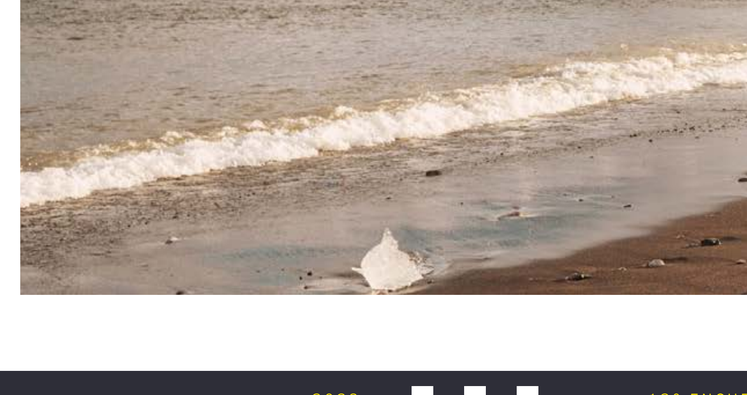
Cuando se les preguntó a los CRO cómo evalúan la capacidad de su organización para gestionar el cambio, dos de las tres opciones principales estaban relacionadas con los empleados, con porcentajes notablemente más altos en los bancos de importancia sistémica. Nuevamente, está claro lo difícil que es para los líderes de negocios bancarios encontrar a las personas que necesitan para mantenerse al día en un entorno que cambia rápidamente.

	Todos los encuestados	Banco de importancia sistémica
Rotación de empleados	52%	75%
Número de acciones regulatorias	50%	67%
Compromiso de los empleados	45%	67%

Los bancos han adoptado una variedad de estrategias y tácticas para abordar sus brechas de talento y, a pesar de las perspectivas de la industria para la última temporada de bonificación, han comenzado con una compensación más alta. Véase la gráfico 21. Es probable que estos enfoques de "todo lo anterior" se conviertan en un procedimiento operativo estándar a medida que los bancos y las empresas de otros sectores continúan luchando por las mismas habilidades escasas.

Gráfico 21: Formas en que los bancos buscan atraer y retener talento

P ¿De cuál de las siguientes maneras está abordando su banco la guerra por el talento?



Los CRO y otros ejecutivos bancarios sénior, en particular aquellos con base en los EE.UU., están interesados en cómo se verá afectado el mercado de talento altamente líquido por una recesión. Se preguntan si la demanda laboral finalmente se debilitará y, de ser así, cuál será el impacto en la inflación salarial. Los CRO también pueden considerar los impactos culturales si se hacen necesarias reducciones de la fuerza laboral o si los programas para empleados (por ejemplo, bienestar mental) lanzados durante la pandemia se recortan debido a consideraciones de costos. Si la experiencia de los empleados se deteriora junto con la economía, a los bancos les resultará cada vez más difícil encontrar y retener a las personas adecuadas.

Hoy en día, los CRO colaboran con los gerentes de recursos humanos principalmente para responder a consultas regulatorias (por ejemplo, evaluaciones de las habilidades para los auditores internos). Mirando hacia el futuro, las competencias de riesgo de la fuerza laboral deberán ser sofisticadas con especialistas dedicados capaces de modelar y mitigar diferentes formas de riesgo de talento serán un sello distintivo de las funciones de gestión de riesgos de alto rendimiento.

CAPÍTULO

03

La creación de una función de gestión de riesgos de alto rendimiento

Al igual que sus contrapartes en el negocio, los CRO buscan una mejor tecnología y nuevos conjuntos de habilidades para impulsar la transformación en busca de mejores resultados y más eficiencia. Esas necesidades compartidas crean empatía y la base para colaboraciones más estratégicas y productivas con líderes sénior en toda la empresa. Parte de la presión que enfrentan los CRO para determinar cuántas personas necesitan y dónde desplegarlas lleva a que a menudo se ven obligadas a hacer malabarismos con múltiples interrupciones (programas de transformación interna y nuevos requisitos regulatorios, por ejemplo) además de las constantes de amenazas a la ciberseguridad, riesgo de crédito y riesgo operacional.

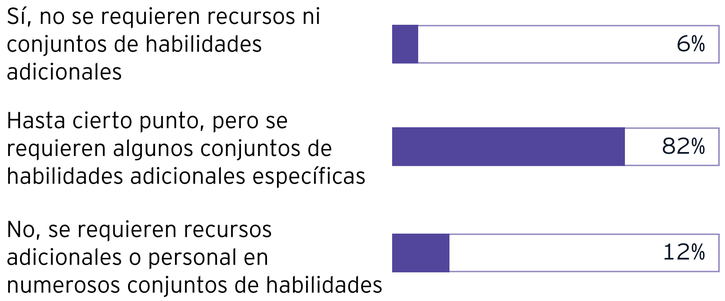
> “Sigo viendo que las personas son quienes marcan la diferencia. Si se tiene el talento adecuado, se pueden descubrir las herramientas necesarias.”
>
> Gerente de riesgos encuestado

NECESIDADES DE PERSONAL Y TALENTO

La gestión de riesgos altamente efectiva comienza con personas de alto rendimiento, según los CRO. Una gran mayoría (94%) dice que necesita algunas o muchas habilidades y recursos nuevos para satisfacer las necesidades cambiantes de la función de gestión de riesgos. Solo una fracción piensa que tiene el talento que necesita. Ver gráfico 22

Gráfico 22: Presencia de habilidades requeridas para abordar las necesidades cambiantes de gestión de riesgos

P ¿Está equipado su grupo de talentos para satisfacer las necesidades cambiantes de la función de gestión de riesgos en los próximos tres años?



> Necesitamos habilidades especializadas para desafiar lo que está pasando en la tecnología.
>
> Gerente de riesgos encuestado

Las seis habilidades más importantes para las funciones de gestión de riesgos son las mismas que en la encuesta del año pasado, con la ciencia de datos y la cibernética encabezando la lista. Ver gráfico 23. Que todos busquen las mismas habilidades es un patrón que aumenta el riesgo de talento, así como los costos laborales, una dinámica que se aplica dentro de la gestión de riesgos y otras funciones del banco.

Las habilidades más demandadas reflejan la naturaleza cada vez más basada en datos de la gestión de riesgos. Los CRO, al igual que sus pares en las área del negocio, necesitan profesionales con mentalidad analítica y expertos en tecnología que puedan revisar grandes cantidades de datos y encontrar tendencias y patrones significativos, especialmente aquellos que abarcan disciplinas de gestión de riesgos. Pero las necesidades de talento se transformarán con el tiempo, a medida que cambien los perfiles de riesgo y evolucionen los requisitos regulatorios. Considere cómo los profesionales de gestión de riesgos con habilidades de pensamiento de diseño pueden ayudar a garantizar que los procesos se configuren para cumplir con requisitos complejos, como lo es la regulación de derechos del consumidor del Reino Unido.

Curiosamente, los CRO en los bancos de importancia sistémica ven una mayor necesidad de contar con mayor talento en gobernanza, riesgo y controles (58%), cambio climático (50%) y resiliencia operativa (50%) que sus pares. La agilidad y la adaptabilidad son atributos muy buscados por los profesionales de la gestión de riesgos, especialmente en las grandes organizaciones que intentan romper los silos organizativos de sus funciones de gestión de riesgos. Ver gráfico 24.

Hay muchas razones para creer que estas habilidades transferibles seguirán creciendo en importancia.

Gráfico 23: Habilidades principales requeridas en la función de gestión de riesgos durante los próximos tres años

P ¿Cuáles son los conjuntos de habilidades más importantes que se requieren en la función de gestión de riesgos durante los próximos tres años?

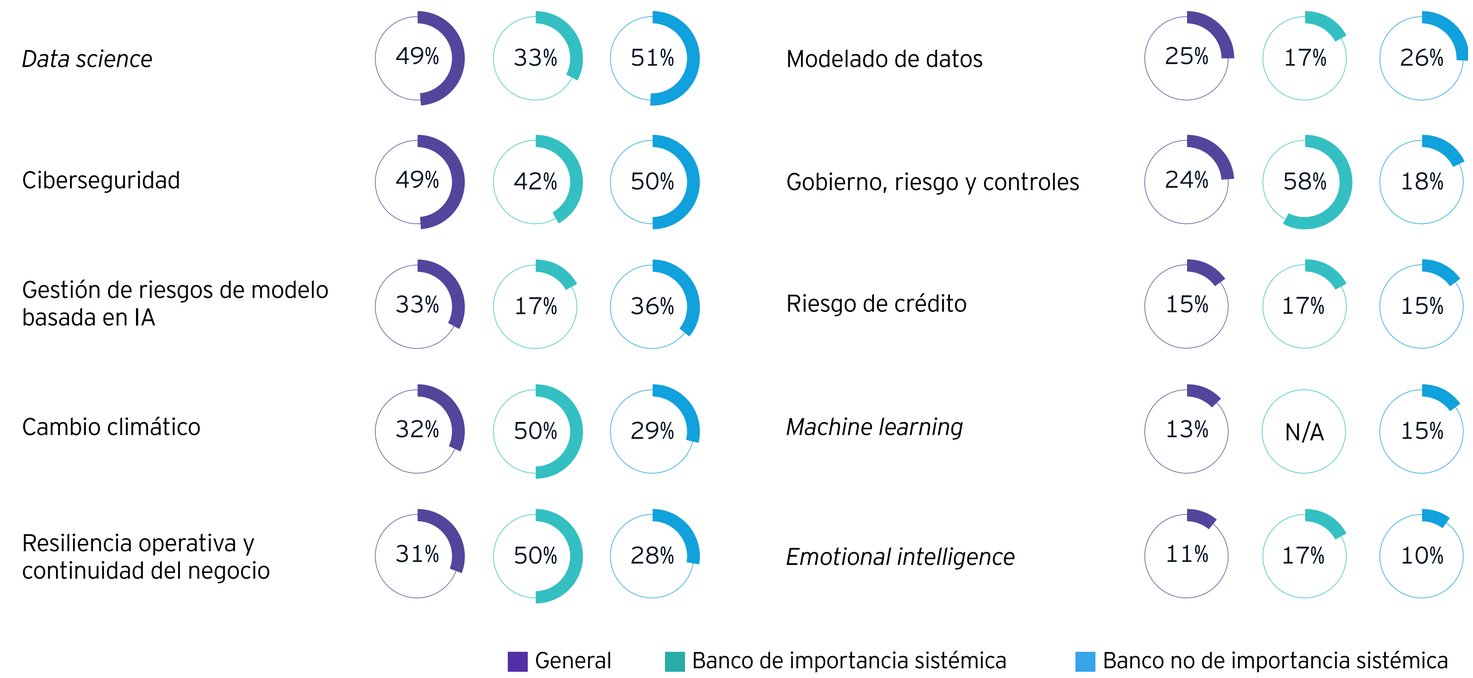
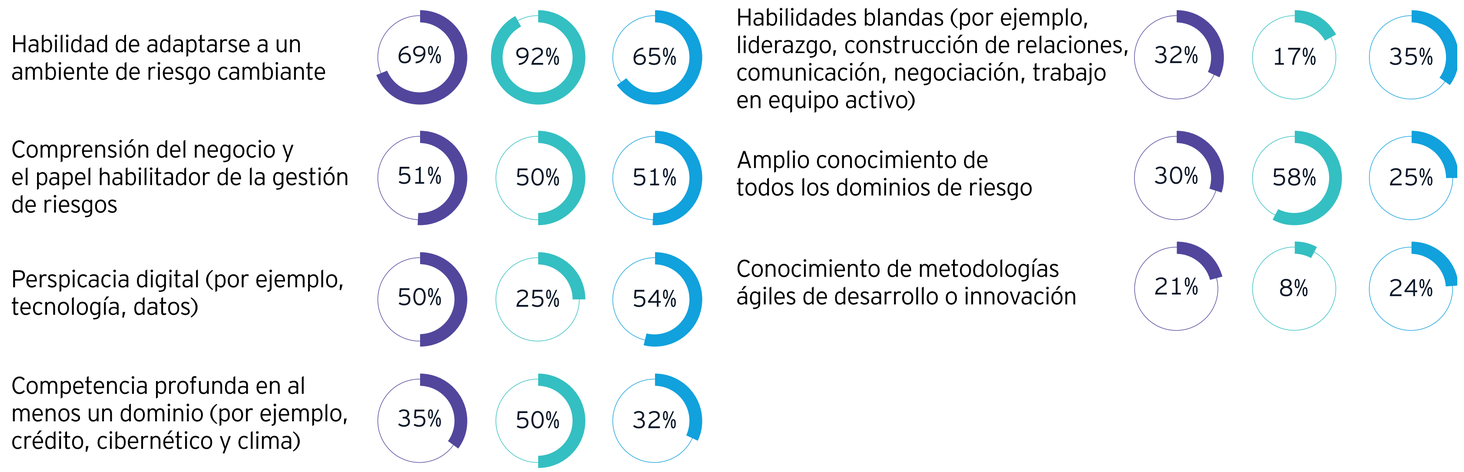


Gráfico 24: Habilidades de máxima prioridad para los equipos de gestión de riesgos para gestionar mejor el riesgo

P En los próximos años, ¿cuáles son los principales conjuntos de habilidades que sus recursos de gestión de riesgos deberían priorizar para gestionar mejor los riesgos?



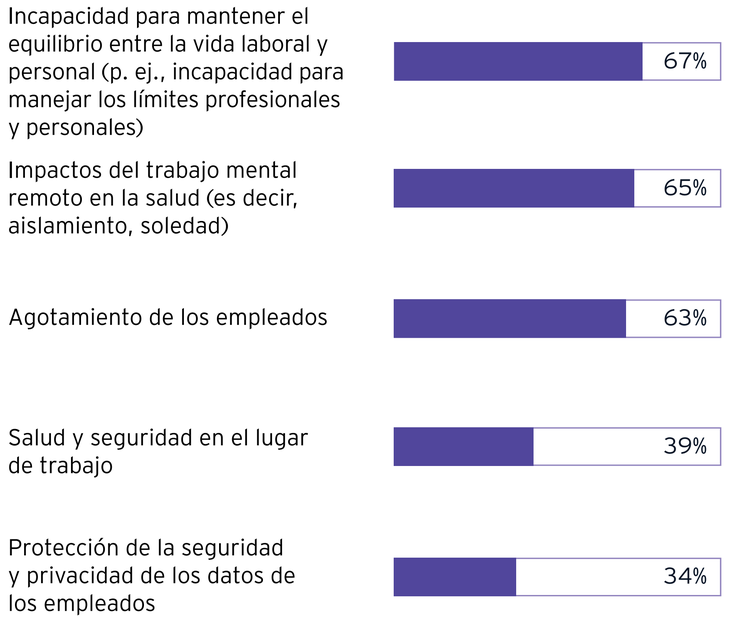
En muchos casos, los CRO buscan volver a capacitar al personal de riesgo existente en áreas particulares de especialización, incluidas las competencias emergentes, como el clima. Algunos bancos están contratando proveedores externos para estos servicios críticos. Aunque el 77% de los CRO esperan aumentar su número de empleados, una recesión puede obligarlas a operar con un menor número de personal, pero más capacitados. Sus contrapartes en el lado comercial probablemente enfrentarán el mismo desafío. Se necesita más perspicacia comercial para anticiparse al riesgo, en lugar de simplemente responder a las amenazas entrantes.

Apoyar a los equipos y talentos actuales: los CRO se centran en la salud mental de sus empleados y están preocupados por el impacto cultural del trabajo remoto e híbrido, al igual que el resto de la empresa. Ver gráfico 25. Como se subrayó durante la pandemia, los problemas de salud mental resaltan el vínculo entre la resiliencia operativa y la resiliencia de la fuerza laboral.

> Creo firmemente en tener empleados que comiencen en el negocio, ganen experiencia y luego pasen a un rol de riesgo con la perspectiva de esos otros puestos.
>
> Gerente de riesgos encuestado

Gráfico 25: Principales preocupaciones asociadas con la protección continua del bienestar, la salud y la seguridad de los empleados

P Al considerar su enfoque para una nueva normalidad posterior a COVID-19, ¿cuáles son sus principales preocupaciones asociadas con la protección continua del bienestar, la salud y la seguridad de los empleados?



Los desafíos relacionados con el aislamiento y el equilibrio entre la vida laboral y personal pueden ser sustanciales en algunas organizaciones. Sin embargo, algunos CRO nos dicen que están acostumbrados al trabajo híbrido porque han mantenido operaciones durante mucho tiempo en diferentes mercados y regiones. Otras CRO pueden buscar obtener talento de más ubicaciones si sus bancos admiten modelos de "trabajo desde cualquier lugar" en el futuro.

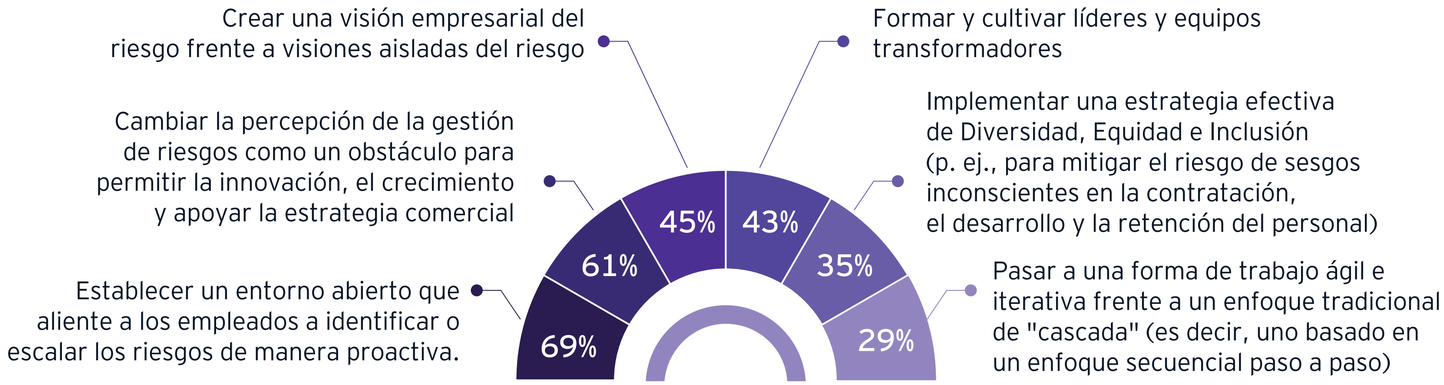
MANTENER UNA CULTURA SÓLIDA CON LA **GESTIÓN DE RIESGOS**

Los CRO aspiran a construir culturas que fomenten la identificación proactiva de riesgos y que sean capaces de habilitar el negocio y estén motivados para hacerlo. Ver gráfico 26. Eso significa algo más que compartir conocimientos sobre riesgos y prácticas líderes con el negocio. Más bien, el objetivo de los líderes de riesgo debe ser participar plenamente en la formación de nuevos modelos de negocios y en la ejecución de estrategias de crecimiento e innovación.

Debido a que el trabajo híbrido ha creado nuevos desafíos para la gestión de personas, es probable que más bancos enfaticen la capacitación para el liderazgo transformador en el futuro. La disciplina en la gestión de riesgos debe ser un principio de liderazgo transformador en el sector bancario, particularmente dado el grado de disrupción que plantean los modelos de trabajo híbridos y remotos.

Gráfico 26: Pasos principales para construir culturas, comportamientos y formas de trabajar positivos en su organización de riesgo

P ¿Cuáles son los pasos principales para construir una cultura positiva, comportamientos y formas de trabajar en su organización de riesgo?



Dos tercios de los encuestados citaron la cultura como la principal preocupación relacionada con los modelos de trabajo híbridos y remotos, un salto notable desde el 55 % del año pasado. Ver gráfico 27. En particular, la información, la seguridad de los datos y el riesgo cibernético ahora son preocupaciones menos urgentes (citadas por solo el 33 % de los CRO en la encuesta de este año), ya que muchos bancos reforzaron los puntos finales de los sistemas y plataformas que admiten el trabajo remoto. Los CRO ven el trabajo remoto e híbrido como un desafío para mantener culturas sólidas y desarrollar personas y equipos. Ver gráfico 28.

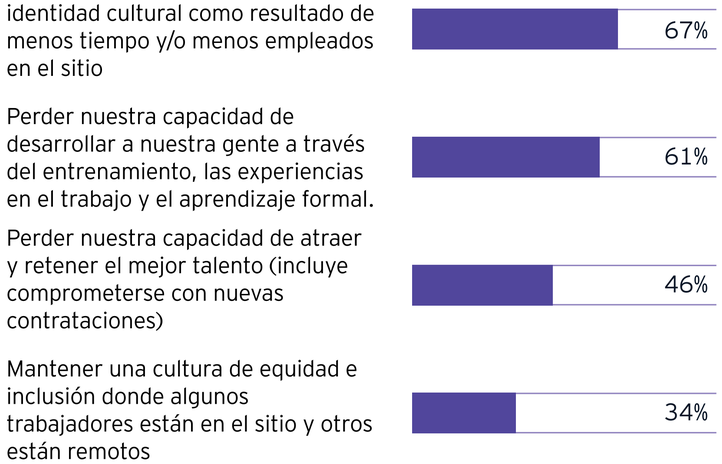
> El bienestar del talento sigue siendo un riesgo. Estamos mitigando la rotación al abordar las dependencias de una sola persona.
>
> Gerente de riesgos encuestado

Gráfico 27: Mayores preocupaciones sobre los modelos de trabajo remoto e híbrido

P Muchas organizaciones han llegado a la conclusión de que el aumento de los niveles de trabajo remoto formará parte de su futuro modelo operativo híbrido. ¿Cuáles son sus mayores preocupaciones acerca de este modelo de trabajo?

Gráfico 28: Principales desafíos para mantener una cultura común

P De cara al futuro, ¿cuáles son los principales desafíos para mantener una cultura común?



Reflejando la importancia de mantener las culturas, los CRO planean monitorear más activamente el bienestar y el compromiso de los empleados a través de una variedad de herramientas y métricas, que incluyen:

- Más encuestas de rutina a empleados: 59%
- Indicadores culturales: 48%
- Rotación, número de puestos vacantes y ocupados y otros
- medidas de capital humano: 42%
- Uso más rutinario de grupos focales y entrevistas: 36%
- Seguimiento de control y métricas de riesgo: 34%

Estas pueden ser herramientas efectivas, aunque en el futuro esperamos ver la adopción de técnicas aún más sofisticadas para analizar el sentimiento de los empleados a través de la escucha continua (por ejemplo, canales de retroalimentación siempre activos, encuestas de "pulso" y temáticas, y monitoreo del compromiso en el metaverso) .

AVANCES EN LA TECNOLOGÍA DE GESTIÓN DE RIESGOS

Al igual que sus pares en el negocio, los CRO ven a la tecnología como un medio para optimizar sus propias operaciones y abastecer a sus equipos para realizar su trabajo de manera más eficiente y efectiva. Actualmente, la IA y el aprendizaje automático se utilizan principalmente en la gestión de riesgos para automatizar tareas manuales, respaldar una mejor toma de decisiones crediticias, identificar ataques cibernéticos y monitorear posibles delitos financieros. Ver gráfico 29. Los CRO esperan que esas aplicaciones también sean las prioridades durante los próximos años. En los bancos de importancia sistémica, hay un enfoque mucho mayor en la automatización y el monitoreo de los delitos financieros. Ver gráfico 30.

Gráfico 29: Actividades con el uso más significativo de IA y aprendizaje automático

P ¿Cuáles son las formas más significativas en que su organización utiliza el aprendizaje automático y/o la IA?

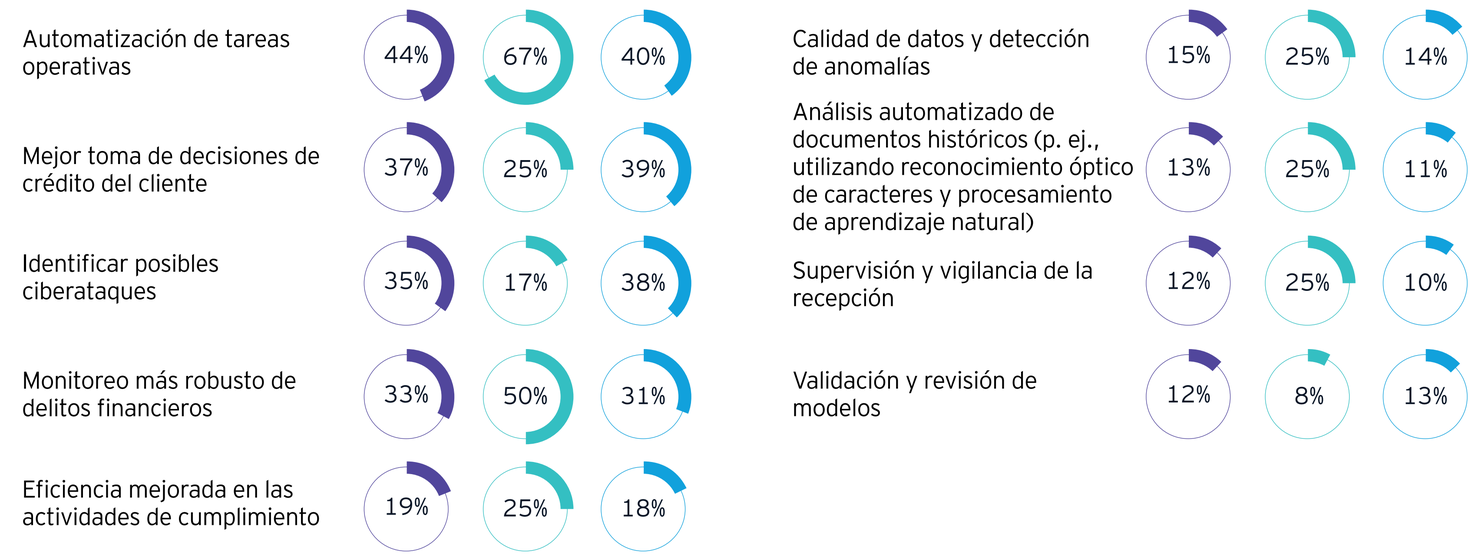
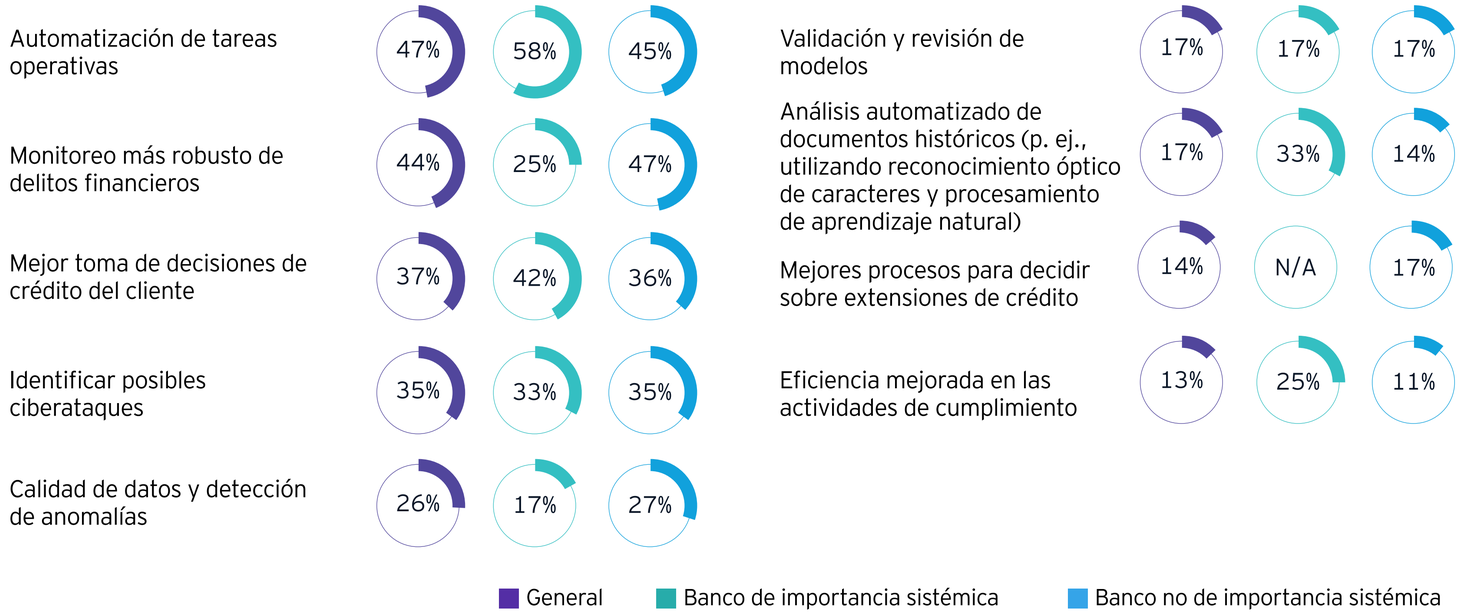


Gráfico 30: Actividades en las que el aprendizaje automático y la IA aumentarán materialmente en los próximos tres años

P ¿Para cuáles de las siguientes actividades su organización utiliza aprendizaje automático y/o IA que aumentarán materialmente en los próximos tres años?



Los CRO también están liderando iniciativas de transformación digital dentro de las operaciones de riesgo, con muchas de las mismas prioridades, además de un uso más amplio de análisis y automatización. Ver gráfico 31.

Gráfico 31: Prioridades de transformación digital para la gestión de riesgos y la segunda línea de defensa

P ¿En qué áreas cree que acelerará su transformación digital de segunda línea de defensa y gestión de riesgos (seis opciones principales)?

De cara al futuro: una matriz de riesgos en constante evolución

Los resultados de la última encuesta indican que la gestión de riesgos sigue siendo el núcleo del sector bancario. Los hallazgos también dejan en claro que el trabajo de los CRO no será más fácil en el futuro cercano. Las prioridades a corto plazo se ven interrumpidas con frecuencia por acontecimientos mundiales y otras fuerzas externas. Considere cómo el empeoramiento constante de las condiciones económicas en los meses transcurridos desde que realizamos nuestra encuesta probablemente haya aumentado el enfoque de los CRO en el riesgo de crédito.

Si bien el riesgo cibernético se situó por delante del crédito como la principal prioridad de los CRO para los próximos 12 meses, según los resultados de la encuesta de este año, las posiciones respectivas podrían cambiar el próximo año si el entorno económico resulta en mayores pérdidas crediticias que la que los bancos han visto en años. Los ciberataques a gran escala y la volatilidad geopolítica podrían ejercer más presión sobre la situación financiera de los bancos. De hecho, las intrincadas conexiones entre estos diferentes tipos de riesgos requieren que los CRO observen amenazas fuera de las categorías tradicionales, así como diseñar nuevos tipos de controles y, en algunos casos, mejorar la forma en la que estructuran sus equipos.

Los riesgos emergentes que repentinamente se vuelven urgentes hoy no alivian la necesidad de que los CRO piensen en lo que vendrá mañana, o el próximo trimestre, o el próximo año, o en 36 meses. La descripción del trabajo requiere que los CRO se encuentren alertas ante cualquier amenaza para que puedan responder de manera oportuna. Los CRO bancarios más eficaces deben sobresalir tanto en el ámbito estratégico como en el táctico, al mismo tiempo que ayudan a la empresa a tener éxito en la prestación de servicios innovadores, diferenciadores y totalmente seguros que satisfagan las expectativas cada vez mayores de los clientes.

No se puede negar que los bancos han realizado importantes progresos desde la crisis financiera mundial en la mejora de las prácticas de gestión de riesgos y el establecimiento de controles sólidos en todo el negocio. La gestión eficaz de los riesgos durante la próxima década requiere construir sobre ese historial impresionante, con pensamiento creativo y acción audaz, tecnología más avanzada y nuevos talentos.

Metodología de la investigación y demografía de los participantes

EY y el Instituto de Finanzas Internacionales (IIF) encuestaron a bancos e instituciones diversas miembros del IIF y a otros bancos pertenecientes a los top cinco de cada región a nivel global desde junio hasta octubre de 2022. Los CRO de los bancos participantes u otros altos ejecutivos de riesgo fueron entrevistados, completaron una encuesta, o ambos.

En total, participaron

88

instituciones financieras de

30

países.

Los bancos participantes eran bastante diversos en términos de tamaño de activos, alcance geográfico y tipo de banco. A nivel regional, esos bancos tenían su sede en Asia-Pacífico (11%), Europa (16%), América Latina (18%), Oriente Medio y África (19%) y América del Norte (36%). De ellos, el 14% son bancos de importancia sistémica.

CONTACTOS

José Carlos Bellina
Socio Líder de Consultoría
para la Industria Financiera

jose.bellina@pe.ey.com

Numa Arellano
Socio de Consultoría
para la Industria Financiera

numa.arellano@pe.ey.com

Tania Sánchez
Associate Partner de Consultoría
para la Industria Financiera

tania.sanchez@pe.ey.com

Ana Lucia Maeda
Gerente Senior de Consultoría
para la Industria Financiera

ana-lucia.maeda@pe.ey.com

Building a better working world

EY | Construyendo un mejor mundo de negocios

EY existe para construir un mejor mundo de negocios, ayudando a crear valor de largo plazo para sus clientes, su gente y la sociedad, así como para generar confianza en los mercados de capitales.

Mediante los datos y la tecnología, los equipos diversos e inclusivos de EY, ubicados en más de 150 países, brindan confianza a través de la auditoría y ayudan a los clientes a crecer, transformarse y operar.

A través del enfoque multidisciplinario en auditoría, consultoría, servicios legales, estrategia, impuestos y transacciones, EY busca que sus equipos puedan hacer mejores preguntas para encontrar nuevas respuestas a los asuntos complejos que hoy enfrenta nuestro mundo.

EY se refiere a la organización global y podría referirse a una o más de las firmas miembro de Ernst & Young Global Limited, siendo cada una de ellas, una entidad legal independiente. Ernst & Young Global Limited, una compañía inglesa limitada por garantía, no presta servicios a clientes. Para obtener información sobre cómo EY recaba y utiliza los datos personales y una descripción de los derechos de los individuos conforme a la ley de protección de datos, ingrese a ey.com/privacy. Las firmas miembro de EY no ofrecen servicios legales en aquellas jurisdicciones en donde está prohibido por regulación local. Para obtener mayor información acerca de nuestra organización, por favor ingrese a ey.com

ey.com

IIF Institute of International Finance

Sobre el Instituto de Finanzas Internacionales
El Instituto de Finanzas Internacionales (IIF) es la asociación global de la industria financiera, con cerca de 400 miembros en más de 60 países. Su misión es apoyar a la industria financiera en la gestión prudente de los riesgos; desarrollar prácticas sólidas de la industria; y abogar por políticas regulatorias, financieras y económicas que sean de interés general para sus miembros y fomenten la estabilidad financiera global y el crecimiento económico sostenible. Los miembros del IIF incluyen bancos comerciales y de inversión, gestores de activos, compañías de seguros, fondos soberanos, fondos de cobertura, bancos centrales y bancos de desarrollo.
Para más información visite:

El Instituto de Finanzas Internacionales (IIF)
1333 H St NW, Suite 800E
Washington, DC 20005-4770
Estados Unidos

Tel: +1 202 857 3600
Fax: +1 202 775 1430
www.iif.com
info@iif.com