Deloitte.

Nuevos riesgos en el horizonte empresarial

Proyecciones de riesgos globales. Análisis de tendencias en un mundo en cambio constante

Introducción

El panorama de riesgos empresarial está cambiando de manera drástica en todo el mundo y muy particularmente en ciertas geografías. Los riesgos cuya probabilidad de ocurrencia parecía remota, en algunas ocasiones ya se han materializado o parecen mucho más cercanos; incluso, con base en la experiencia, el impacto pudiera ser mucho mayor a lo esperado. Se trata de nuevos -y otros no tan nuevos- riesgos en el horizonte que merecen una revisión y también una reflexión.

Recurrentemente, diversas empresas llevan a cabo ejercicios para la administración de riesgos. Dichos ejercicios pretenden prevenir o mitigar la materialización de amenazas o contingencias y por lo regular se alimentan de asuntos coyunturales, eventos pasajeros o situaciones que se perciben importantes respecto de los cuales no hay un análisis a detalle. Pueden ser aspectos relacionados con los mercados en los que operan, nueva y más estricta regulación, compromisos de sostenibilidad (gestión ambiental, social y de gobernanza) cada vez más integrados en la estrategia del negocio, preferencias de los consumidores, innovación en productos, competencia no tradicional, implementación de tecnología innovadora, sucesión, bienestar y cultura empresarial, entre otros. Sin embargo, al final de un ejercicio para la identificación de riesgos en cualquier organización, con frecuencia se plantean estas preguntas:

¿Hay otros riesgos que no tenemos en el radar?

¿Qué otros riesgos pudieran surgir en función de los avances tecnológicos o del deterioro ambiental?

Es común sentir cierto nivel de confort al tener varios riesgos en la pantalla; no obstante, ¿qué es lo que no estamos viendo? Por lo regular, la pregunta no tiene respuesta y el ejercicio para la identificación de riesgos concluye.

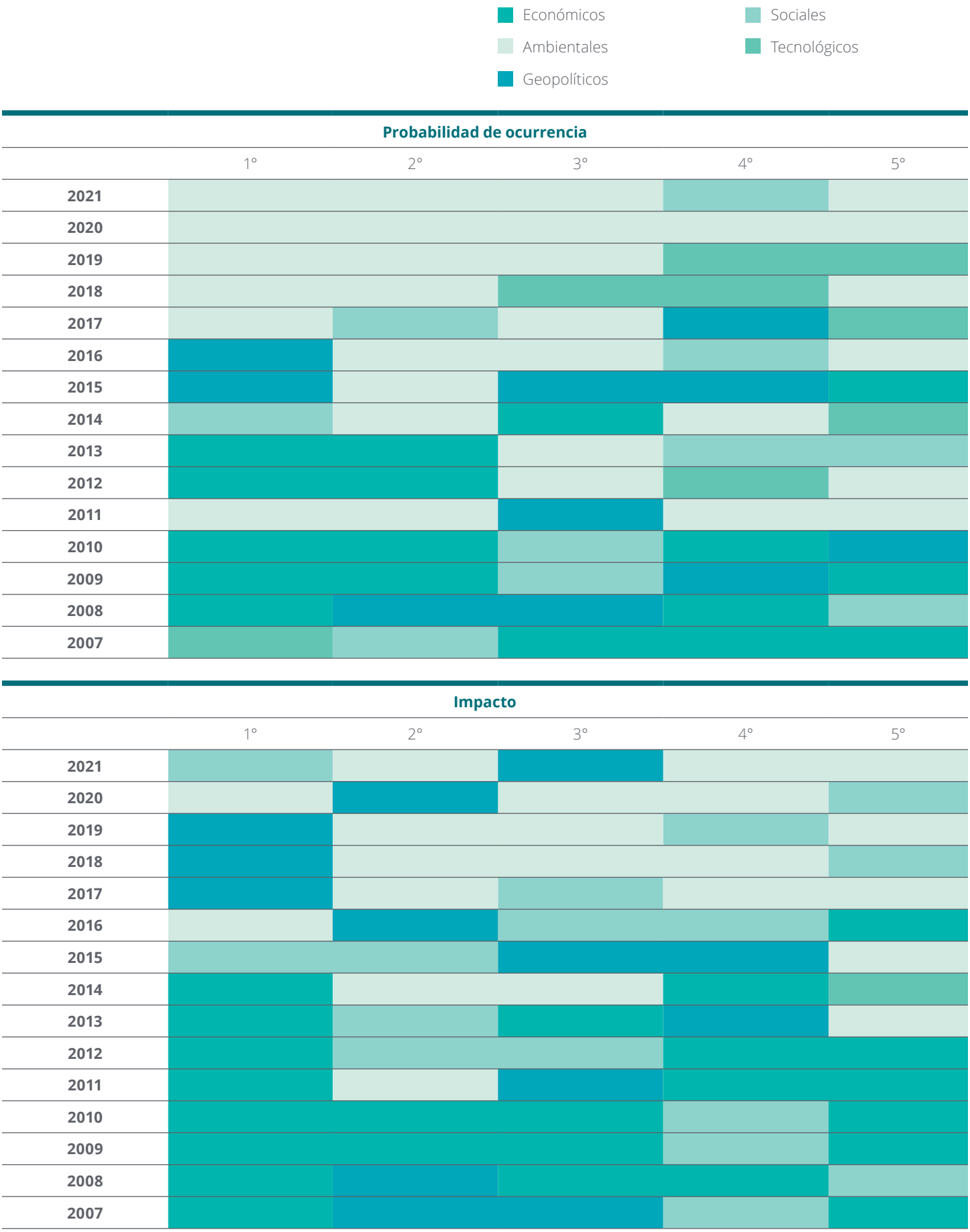
La administración de riesgos empresariales debe incorporar al futuro en su análisis y con mucho mayor ahínco; es decir, no solo debe tener en cuenta lo que ocurrió, lo que está ocurriendo y lo que ocurrirá en el plazo inmediato. Hoy en día se debe considerar la probabilidad de ocurrencia en el mediano y largo plazo, se debe reflexionar respecto de la probabilidad de que sucedan eventos con impacto en la organización en un período de al menos cinco años.

Prácticamente ninguna organización es finita. Una empresa no se crea con una fecha de conclusión, o con una terminación definida, por lo regular las empresas se crean para persistir; pretenden trascender generaciones y adecuarse a los tiempos venideros. Por ejemplo, si una empresa tiene una visión y un plan estratégico a tres o cinco años, el ejercicio de riesgos debiera incluir la probabilidad de ocurrencia de riesgos por el mismo período.

A través de un análisis a los reportes emitidos por el *World Economic Forum*, titulados *The Global Risks Report*, de 2007 a 2024, y proyectados para 2034, identificamos tendencias relevantes que deben considerarse en los ejercicios para la identificación de riesgos empresariales en el corto, mediano y largo plazo. Asimismo, deben invitar a la reflexión, ya que ciertos riesgos no son exclusivos de países, gobiernos y empresas; hay riesgos globales que tienen ya un efecto puntual en las personas.

Figura 1. Riesgos por categoría

Nota: En 2022 la presentación de los riesgos identificados se modifica.


Económicos
Sociales
Ambientales
Tecnológicos
Geopolíticos
Probabilidad de ocurrencia
1°
2°
3°
4°
5°
2021
2020
2019
2018
2017
2016
2015
2014
2013
2012
2011
2010
2009
2008
2007
Impacto
1°
2°
3°
4°
5°
2021
2020
2019
2018
2017
2016
2015
2014
2013
2012
2011
2010
2009
2008
2007

En cuanto a probabilidad de ocurrencia e impacto, en los primeros siete años (2007 a 2014) predominan los riesgos relacionados con la economía, entre los que destacan:

- Crisis financieras y fiscales.
- Precios de petróleo y gas.
- Desaceleración abrupta de China.
- Disparidad en el ingreso.

Por otra parte, los riesgos relacionados con el medio ambiente comienzan a ganar terreno para convertirse en los riesgos predominantes en los siguientes 10 años (2014 a 2024), destacando entre ellos:

- Clima extremo.
- Fracaso en la implementación de iniciativas con impacto climático.
- Desastres naturales.
- Escasez de agua.

Finalmente, llama la atención que los riesgos relacionados con la tecnología, particularmente los Ciberataques -a pesar de la gran amenaza que representan-, no se percibe que pudieran tener un gran impacto y su probabilidad de ocurrencia es relativamente baja. Definitivamente no es algo que debiera salir del panorama de riesgos, de hecho, el riesgo de ciberataques es un riesgo que está cobrando mayor relevancia y seguirá siendo crítico a futuro debido a la mayor transaccionalidad electrónica entre organizaciones y personas, así como el mayor volumen de información que se transmite digitalmente.

Durante los siguientes tres años (2022, 2023 y 2024), una vez concluida la pandemia de COVID-19, los riesgos sociales se incrementan. La mayor consciencia sobre el impacto en las comunidades, salud y seguridad de los colaboradores, derechos humanos, diversidad, equidad e inclusión, retención del talento, satisfacción de los clientes, entre otros factores, está generando que las organizaciones incorporen los asuntos sociales como parte de su estrategia. Por otro lado, en la proyección a 10 años los riesgos ambientales vuelven a ser los más relevantes.

A continuación, ahondaremos en tres de los riesgos más relevantes que aportan a la reflexión que cada organización debiera tener al llevar a cabo sus ejercicios para la identificación de riesgos. Siendo el tema de riesgos sumamente amplio, en futuras entregas estaremos profundizando con otros aspectos.

Cambio climático

Los riesgos presentados por el cambio climático están entrelazados con otros que son clave, desde tormentas y degradación de ecosistemas, hasta regulaciones y precios de la energía a largo plazo[1].

El cambio climático no aparece entre los cinco riesgos más relevantes en los reportes anuales sino hasta 2011, cuando señalan con alta probabilidad de ocurrencia los siguientes:

- Tormentas y ciclones.
- Inundaciones.
- Pérdida de biodiversidad.

Sin embargo, a partir de 2011 y hasta el reporte de 2024, los riesgos relacionados con el cambio climático están dentro de los cinco más relevantes[2]:

- Emisión de gases de efecto invernadero.
- Clima extremo.
- Fracaso en iniciativas climáticas.
- Catástrofes naturales.

Partiendo de 2017 y hasta 2024, los riesgos relacionados con el cambio climático ocupan el lugar número uno de los informes de riesgos anuales. Para redondear la reflexión, el ejercicio proyectado en 2024 hacia 2026 y 2034, subraya los principales temas a resolver: riesgos relacionados con cambios climáticos, condiciones climatológicas extremas, eventos derivados de condiciones climatológicas, pérdida de la biodiversidad y escasez de recursos naturales.

No hay empresa, gobierno o persona en el mundo que escape a los riesgos que el cambio climático representa. De acuerdo con el Monitor de Sequía de México al 31 de octubre de 2024, la sequía persiste en estados del norte y noroeste del país pese a las lluvias torrenciales generadas hasta ese momento[3].

En contraste, en México está fresca la imagen de un Acapulco devastado por el paso del huracán "Otis" en octubre de 2023. En menos de 24 horas, el fenómeno meteorológico se fortaleció a huracán categoría 5, la máxima que establece la escala de huracanes de Saffir-Simpson. Nadie esperaba un golpe tan fuerte, pues el tiempo en el que el meteoro incrementó su fuerza impidió aplicar medidas preventivas eficaces y, en consecuencia, el saldo fue catastrófico. Casi un año después, la noche del 23 y madrugada del 24 de septiembre, "John" golpeó la costa del puerto guerrerense. Esta vez, el huracán categoría 3 dejó en cuatro días el 85% de agua que equivale a todo un año de lluvia en el estado de Guerrero, según autoridades federales de protección civil[4].

Otra demostración de que el cambio climático se hace más evidente es el calentamiento del agua en la costa sudamericana del Océano Pacífico, principalmente en la peruana, que afectó a la biomasa de anchoveta generando la disminución del volumen de dicha especie marina y que desencadenó en la reducción de la cuota de captura de la anchoveta por el gobierno peruano en 2023, impactando de manera significativa los ingresos de las empresas productoras y exportadoras de harina de pescado.

La ciudad de Valencia, en España, es otro ejemplo de catástrofes relacionadas con el cambio climático. A finales de octubre de 2024, la Depresión Aislada en Niveles Altos (DANA) dejó estragos en la ciudad portuaria con un saldo que supera 200 personas muertas y un sinnúmero de daños materiales. Expertos en meteorología han recordado que la DANA es un fenómeno habitual que puede producirse en cualquier estación del año; no obstante, es más peligroso en verano y en otoño, cuando la temperatura superficial del mar es alta y hay mayor evaporación. Si bien, la formación de este fenómeno no obedece al cambio climático, algunos estudios apuntan a que el progresivo aumento de la temperatura del mar Mediterráneo genera una DANA más potente[5].

Finalmente, un problema que está afectando el comercio mundial son los bajos niveles de agua del lago Gatún, el principal cuerpo de agua que surte al Canal de Panamá. En un escenario normal, un promedio de 38 buques transita diario por el Canal de Panamá; empero, la autoridad del canal tuvo que restringir el paso a 20 embarcaciones debido a los bajos niveles de agua. Al respecto, citamos una nota periodística publicada en El País en febrero de 2024: El impacto inflacionario por la situación en Panamá ya lo ha sentido el consumidor desde mediados del año pasado. El 40% del tráfico de contenedores de mercancías que tienen como destino EE. UU. cruzan por el Canal, que se utiliza como alternativa a la red de carreteras y líneas férreas que conectan las dos costas del país, por lo que el precio final de las mercancías ha aumentado. El transporte de cada contenedor les cuesta a las navieras cerca de 8,000 dólares, según LaRocco, y cada retraso es una presión adicional sobre el precio de las mercancías[6].

La atención que requiere el cambio climático no es una tarea que corresponde únicamente a los gobiernos, a las empresas o a ciertos sectores de la sociedad. El cambio climático podría llegar a un punto en el que no hay vuelta atrás, por lo que es fundamental seguir creando consciencia y acciones específicas que, dentro de lo posible, mitiguen el riesgo que indudablemente sea prioridad tanto para gobiernos, como para empresas y la sociedad civil.

Hoy en día, la materialización de riesgos no solo afecta el presente y el futuro de una empresa, también tiene un efecto en las sociedades y en las personas en lo individual.

Ciberseguridad

Son diversos y muy interesantes los datos que arroja el análisis de la evolución de los riesgos a través de los años. En relación con la ciberseguridad, el tema apareció por primera vez entre los cinco principales riesgos en el reporte del *World Economic Forum* de 2012.

A poco más de una década, los temas relacionados con la seguridad de la información se mantienen como foco de atención, según *The Global Risks Report 2024*:

Nuevas herramientas y capacidades abrirán nuevos mercados para las redes criminales, con el cibercrimen, una fuente de ingresos de bajo riesgo y bajo costo para el crimen organizado. Los ataques de *phishing*, por ejemplo, ahora pueden ser mucho más precisos usando inteligencia artificial generativa. En los próximos años, las defensas cibernéticas más sofisticadas desviarán la atención del crimen organizado a objetivos e individuos menos alfabetizados digitalmente o infraestructuras y sistemas menos seguros. Ya prevalente en América Latina, el cibercrimen continuará extendiéndose a partes de Asia y África Occidental y Meridional, a medida que la riqueza crezca y la conectividad a internet traiga grandes segmentos de la población mundial en línea[7].

El mapa de ciberamenazas de Kaspersky[8], consultado el 3 de enero de 2025, establece el lugar que ocupan los países latinoamericanos en la lista de ciberataques:

- Brasil #4
- México #12
- Colombia #20
- Argentina #34
- Perú #36
- Chile #54
- Panamá #63
- Bolivia #76
- Venezuela #77
- Paraguay #104
- República Dominicana #105
- Uruguay #110
- Costa Rica #111
- Honduras #112
- Guatemala #124
- El Salvador #140

Y en el panorama global, los más atacados son: Rusia, China, Kazajistán, Estados Unidos y Alemania.

Los ciberataques son ahora más avanzados, ejemplo de ello es el *ransomware*, un tipo de *malware* o *software* malicioso que los ciberdelincuentes utilizan para extorsionar a sus víctimas. Una vez que el *ransomware* infecta un sistema, cifra los archivos o bloquea el acceso al sistema completo, impidiendo que el usuario acceda a sus datos. Después, los atacantes exigen un pago, generalmente en criptomonedas, a cambio de proporcionar una clave de descifrado o restaurar el acceso.

El *ransomware* puede propagarse a través de correos electrónicos de *phishing*, descargas maliciosas, vulnerabilidades en el *software* o a través de redes comprometidas. Se trata de una violación de datos que puede comprometer la información sensible y las operaciones críticas.

Las inversiones que llevan a cabo las empresas para prevenir ciberataques deben ser revisadas recurrentemente dada la sofisticación y el incremento de las amenazas tecnológicas. Es de suma importancia la transparencia en este aspecto, brindar claridad a los órganos de gobierno respecto del nivel de confianza en la defensa, medidas de mitigación y amenazas ante las que está expuesta una empresa, son la base para tomar decisiones estratégicas relacionadas con la seguridad de la información.

Si bien, las ciberamenazas no son algo nuevo en el espectro de riesgos, llevan años encabezando la preocupación y la atención por parte de gobiernos, empresas y personas; sin embargo, el tema nuevamente cobra protagonismo con la incorporación de la inteligencia artificial y el crecimiento de la digitalización.

La Encuesta mundial sobre el futuro de la cibernética 2023[9], elaborada por Deloitte, afirma:

Los días en que "la ciberseguridad era una idea de último momento" han quedado atrás. Y para cualquier negocio, las nuevas capacidades tecnológicas serán más efectivas cuando se incluyan estrategias de ciberseguridad sólidas. Las tecnologías emergentes traerán consigo soluciones innovadoras que pueden apoyar los modelos de negocio futuros y también presentar desafíos imprevistos en el ámbito de la ciberseguridad. ¿Cómo se aprovecharán estas tecnologías para generar valor empresarial mientras se asegura que las estrategias e inversiones en ciberseguridad estén a la par?

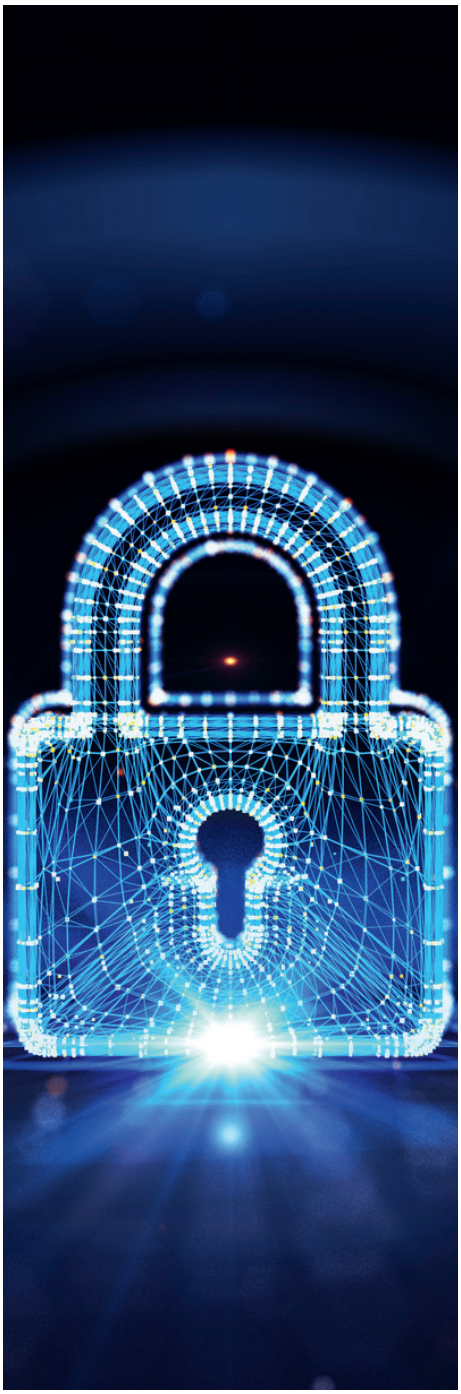
Finalmente, un punto de vista elaborado por Deloitte en 2024, titulado *Safeguarding Generative Artificial Intelligence (AI) with cybersecurity measures*[10], concluye lo siguiente:

La IA generativa tiene inmensas posibilidades en cuanto a contenido, lo que puede ayudar a reducir esfuerzos y aumentar las eficiencias. La IA generativa tiene aplicaciones en todo el ecosistema, afectando por igual a individuos, gobiernos, organizaciones y en general la sociedad civil.

Si bien celebramos este avance cuantitativo en el progreso tecnológico, al igual que con cualquier tecnología, la ciberseguridad debe ser una consideración primaria. Los riesgos se encuentran en modelos de IA generativa, aplicaciones, infraestructura, personas, datos y las metodologías de entrenamiento y prueba.

Ya que el potencial de la IA generativa es innegable, lo que la convertirá en una fuerza transformadora es el equilibrio entre riesgos y controles para su adopción.

La IA generativa creará inmensas oportunidades de crecimiento en áreas clave, como TI inteligente, productos y operaciones. La próxima década será cuando la IA se convierta en la palanca para mejorar el potencial y crecimiento humano.



Información

Un riesgo que debuta entre los cinco más relevantes, con base en *The Global Risks Report 2024*, es la desinformación y la información falsa generada por humanos o por la Inteligencia Artificial (IA):

La desinformación y la información falsa pueden interrumpir radicalmente los procesos electorales en varias economías durante los próximos dos años.

Una creciente desconfianza en la información, así como en los medios de comunicación y los gobiernos como fuentes, profundizará la polarización de opiniones -un ciclo vicioso que podría desencadenar disturbios civiles y posiblemente confrontación-.

Existe el riesgo de represión y erosión de derechos si las autoridades no reprimen la proliferación de información falsa.

Siempre han existido las noticias falsas, estas que no se originan con el auge de las redes sociales. Son noticias que se han creado para engañar o generar una falsa percepción respecto de alguien o de algún suceso. Asimismo, pervive el sesgo informativo o las noticias "a modo" con el fin de manipular a ciertos sectores de la opinión pública. El manejo perverso de noticias es también un riesgo, pues quien recurre a esta práctica generalmente es para obtener un beneficio particular.

Es a Joseph Goebbels, ministro para la Ilustración Pública y Propaganda del Tercer Reich, a quien se le atribuye la frase "Una mentira repetida mil veces se convierte en verdad".

Hoy en día, las noticias falsas, *fake news* o bulos, han cobrado mayor relevancia en parte por el mal uso de herramientas tecnológicas y en parte por su propagación en redes sociales. Son muchas las personas que han recibido mensajes de texto, imágenes o videos sacados de contexto a través de correo electrónico o redes sociales.

La Procuraduría Federal del Consumidor (Profeco) en México, por su parte, define así a las noticias falsas[11]:

Las noticias falsas o infodemia consisten en publicar o difundir de forma masiva información falsa de interés público, a sabiendas de su falsedad, con la intención de engañar o confundir, desinformar, crear pánico en las personas, implantar angustia y promover conductas incorrectas.

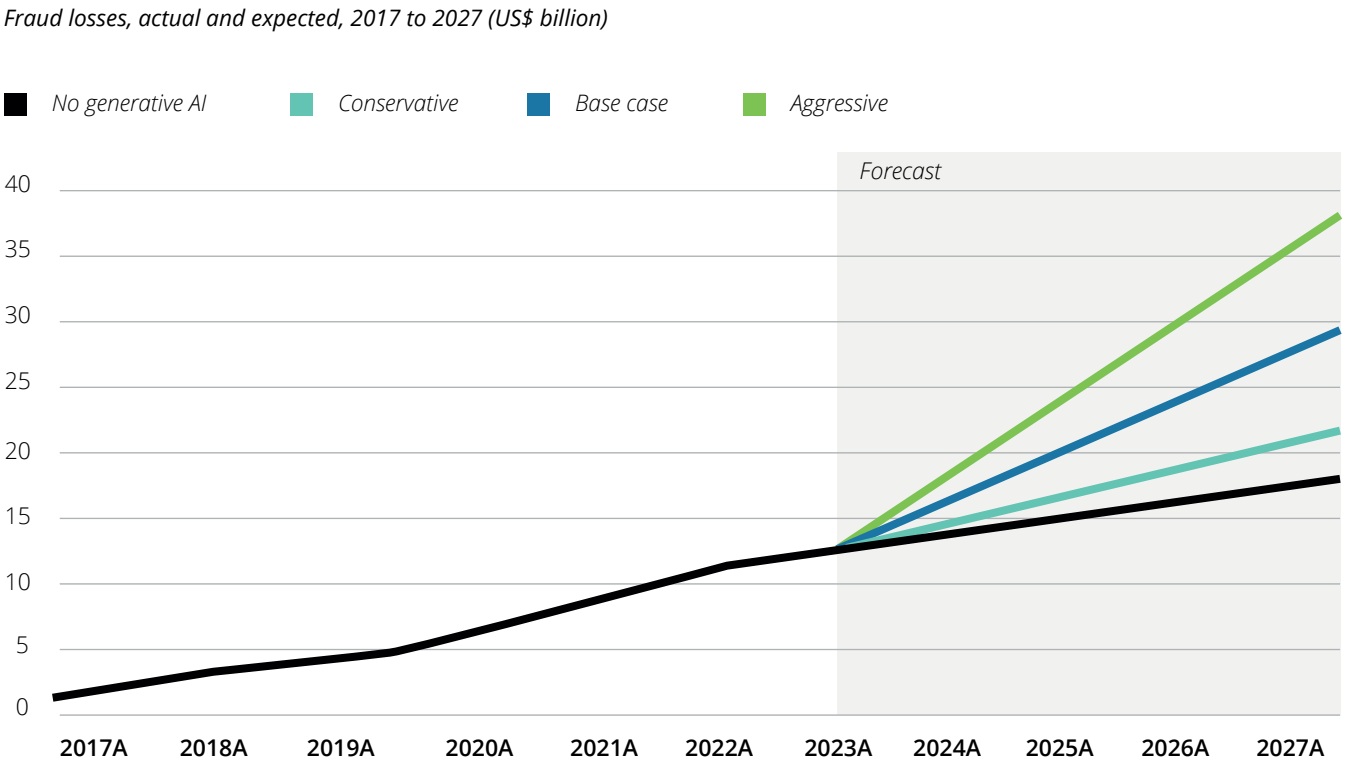
Son percibidas por los usuarios como ciertas y en muchas ocasiones se van modificando mientras se difunden. Tienen una gran capacidad de propagación, principalmente por medio de las redes sociales y en las aplicaciones de mensajería instantánea.

El concepto *fake news* ganó popularidad durante la campaña presidencial de 2016 en Estados Unidos, cuando el candidato en ese entonces, Donald Trump, lo utilizó pública y repetidamente.

En México, de acuerdo con una publicación de El Financiero[12], las tres personas que aspiraban a la presidencia de la República en 2024 fueron víctimas del *deep fake*, pues circularon videos con declaraciones falsas. Según el mismo artículo, ocho de cada diez personas que leen o ven este tipo de contenido no son capaces de distinguir entre un video real y uno creado por inteligencia artificial.

De igual manera, distintos medios de comunicación han recopilado una serie de publicaciones cuya finalidad es la desinformación a través de imágenes generadas por IA durante la última campaña electoral en la Unión Americana[13]. Finalmente, de acuerdo con un estudio realizado por Deloitte, se prevé que la Inteligencia Artificial generativa incremente rápidamente las pérdidas por fraudes en los siguientes años[14]:

Figura 2. IA generativa podría aumentar rápidamente las pérdidas por fraude en los próximos años



Sources: The FBI's Internet Crime Complaint Center; Deloitte Center for Financial Services.

Conclusión

"Quien tiene la información, tiene el poder". Probablemente la frase deriva de "Scientia potentia est" (el conocimiento es poder) atribuida al filósofo inglés Francis Bacon. Si bien, quien posee la información o el conocimiento tiene el poder, también quien distorsiona el conocimiento o la información, lo ostenta.

La identificación de riesgos en una empresa debe considerar múltiples aspectos. Situaciones que antes parecerían irreales o sumamente lejanas, hoy en día están ocurriendo o están por ocurrir.

Observar la evolución o la conversión de los riesgos históricos, así como su proyección a mediano y largo plazo, son factores fundamentales para prevenir -dentro de lo posible- su materialización o para tener elementos que resuelvan las complicaciones derivadas del riesgo materializado.

Habiendo explorado algunos aspectos del esquema global de riesgos, ¿considera su ejercicio de riesgos completo y útil?

Referencias

1. World Economic Forum. (2006). Global Risks 2006. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2006.pdf
2. World Economic Forum. (2020). The Global Risks Report 2020. https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
3. Comisión Nacional del Agua. (2024). Monitor de Sequía de México. Conagua. https://smn.conagua.gob.mx/tools/DATA/Climatolog%C3%ADa/Sequ%C3%ADa/Monitor%20de%20sequ%C3%ADa%20en%20M%C3%A9xico/Seguimiento%20de%20Sequ%C3%ADa/MSM20241031.pdf
4. Guillén, B. (2024). El balance final del huracán "John" en Guerrero: 270,000 afectados y 23 fallecidos. El País México. https://elpais.com/mexico/2024-10-04/el-balance-final-del-huracan-john-en-guerrero-270000-afectados-y-23-fallecidos.html
5. BBC News Mundo. (2024). Qué es una DANA, el fenómeno meteorológico que provocó las lluvias torrenciales que han dejado decenas de muertos en el sureste de España. https://www.bbc.com/mundo/articles/cj6k5xk648zo
6. Cota, I. (2024). El Canal de Panamá sufre una crisis hídrica y mete en problemas al comercio mundial. El País Negocios. https://elpais.com/economia/negocios/2024-02-19/la-crisis-hidrica-ahoga-al-canal-de-panama.html?event_log=oklogin
7. World Economic Forum. (2024). The Global Risks Report 2024. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf
8. AO Kaspersky Lab. (2025). Ciberamenazas Live-map. https://cybermap.kaspersky.com/es
9. Deloitte. (2022). 2023 Global Future of Cyber Survey. Building long-term value by putting cyber at the heart of the business. https://www.deloitte.com/content/dam/assets-shared/docs/services/risk-advisory/2023/gx-deloitte_future_of_cyber_2023.pdf
10. Deloitte. (2024). Safeguarding Generative Artificial Intelligence (AI) with cybersecurity measures. Risk insights and building blocks for secure Generative AI solutions. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-deloitte-pov-safeguarding-gen-ai%20-with-cybersecurity-measures-noexp.pdf
11. Procuraduría Federal del Consumidor. (2021). *Noticias falsas la otra pandemia*. Profeco. https://www.gob.mx/profeco/es/articulos/noticias-falsas-la-otra-pandemia
12. Calderón, C. (2024). Elecciones México 2024: *Deep fakes y fake news ganan en las votaciones*. El Financiero. https://www.elfinanciero.com.mx/elecciones-mexico-2024/2024/06/04/deep-fakes-y-fake-news-marcaron-el-escenario-electoral/
13. Harbour, B. y Lafuente, J. (2024). El poder de las noticias falsas en la campaña electoral de Estados Unidos. El País Elecciones. https://elpais.com/internacional/elecciones-usa/2024-10-28/ruta-5n-el-poder-de-las-noticias-falsas-en-la-campana-electoral-de-estados-unidos.html

    Bayo, B. (2024). El uso de la IA como herramienta de desinformación en la campaña. Corporación de Radio y Televisión Española. https://www.rtve.es/noticias/20241103/elecciones-eeuu-2024-ia-herramienta-desinformacion-campana/16307898.shtml

    Cohen, M. (2024). El apoyo "fake" de celebridades creado con inteligencia artificial, un arma en "la guerra" de desinformación antes de las elecciones de 2024. CNN. https://cnnespanol.cnn.com/2024/08/22/fake-news-inteligencia-artificial-politicos-trump-desinformacion-elecciones-ee-uu-trax

    Grippo, M. (2024). Trump vs. Harris: así ha operado la desinformación durante la campaña electoral en Estados Unidos. France 24. https://www.france24.com/es/programas/des-informando/20241102-trump-vs-harris-as%C3%AD-ha-operado-la-desinformaci%C3%B3n-durante-la-campa%C3%B1a-electoral-en-estados-unidos
14. Deloitte Insights. (2024). Generative AI is expected to magnify the risk of deepfakes and other fraud in banking. https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-predictions/2024/deepfake-banking-fraud-risk-on-the-rise.html

Contactos

Israel Zagal
Socio en Estrategia, Riesgos y Transacciones
Deloitte México
izagal@deloittemx.com

René Nájera
Socio en Estrategia, Riesgos y Transacciones
Deloitte México
rnajera@deloittemx.com

Fabiola Juscamaita
Socio en Estrategia, Riesgos y Transacciones
Deloitte Spanish Latin America
fjuscamaita@deloitte.com

Deloitte.