

Top 7 Riesgos para Directores y Administradores, Salud y Seguridad, el Riesgo Emergente



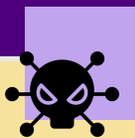
Si hablamos de riesgos, la SALUD y la SEGURIDAD asaltan literalmente el primer lugar de la lista en la encuesta de WTW, Global Directors' and Officers Survey Report 2024. Muy probablemente por el coletazo de la pandemia, el tema desbanca al de ciberseguridad, advirtiendo quizá sobre nuevas prioridades...

Más allá de los preocupantes ataques cibernéticos y la temida pérdida de datos -que hoy ocupan las posiciones número dos y tres entre los riesgos más sentidos entre Directores y Administradores- el aspecto humano destaca. Entre otras razones porque todo indica que la pandemia dejó tras de sí pérdidas económicas y problemas prácticos que cambiaron esquemas de trabajo. Si esto persiste, el tiempo lo dirá...

Top 7 riesgos 2024 según Directores & Administradores

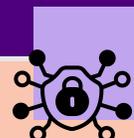
2023

- Ataques Cibernético
- Pérdida de datos
- Extorsión cibernética
- Incumplimiento de regulaciones
- Salud y Seguridad / Acusaciones de incumplimiento ambiental
- Sobornos y corrupción
- La organización como víctima de un crimen



2024

- Salud y seguridad
- Ataques cibernéticos
- Pérdidas de datos
- Incumplimiento de regulaciones
- Sistemas y controles
- Sobornos y corrupción
- Incumplimiento de sanciones



En la Encuesta hay temas a destacar:

1. El riesgo **Salud y Seguridad** ya figuraba en la lista de la encuesta de WTW desde el 2018, pero lo cierto es que nunca se había colado en los primeros tres sitios de la lista, ni conquistado a un 84% de los encuestados de poco más de medio centenar de países participantes, frente a un promedio de 45% que se decantaban por este tema en los tres años anteriores.

En Europa, Asia, Norteamérica, Latinoamérica (que representa el 14% de los encuestados), Australasia, África y Medio Oriente los D&O colocan Salud y Seguridad como su preocupación más importante, y solo en el caso de Gran Bretaña el tema se desplaza al segundo lugar, después de la Pérdida de Datos.

2. Los **Ataques Cibernéticos** que habían venido apareciendo en el primer sitio de la lista durante los últimos tres años, se desplaza a la segunda posición, pero, no hay que equivocarse, los temas relacionados con ciberseguridad siguen siendo riesgos prioritarios. De hecho, la mayor disponibilidad de herramientas y la integración de la inteligencia artificial a sus operaciones brinda a los autores de amenazas cibernéticas la oportunidad de realizar ataques más potentes y difíciles de detectar en el futuro. Esto reduce también las barreras de entrada para delincuentes novatos, contribuyendo a elevar la amenaza global del ransomware.

3. El cuidado y la prevención de la **pérdida de datos** van de la mano con el tema cibernético. Esta preocupación pone a la orden del día muchas importantes por parte de las autoridades de protección de datos y autoridades financieras. Infracciones, fallas en sistemas y controles, y reclamaciones de datos prenden alarmas a las que se suman los altos riesgos para la reputación de las organizaciones infractoras.

De ahí que **sistemas y controles** tengan también un lugar permanente en la lista de los 7 riesgos más importantes, y lo más seguro es que se queden ahí por mucho tiempo. Todo esto suma presiones sobre Directores y Administradores, urgiéndoles a la implementación de controles de ciberseguridad que permitan reaccionar eficiente y efectivamente ante cualquier ataque.

4. **ESG, el gran ausente.** Si alguna presencia habría que destacar en los riesgos destacados por los encuestados de más de 50 países es el que se refiere a riesgos Environmental, Social and Governance (ESG, por sus siglas en inglés). Si bien estos temas parecen a todas luces importantes, lo cierto es que no penetran aún en los 7 riesgos prioritarios para los encuestados. No obstante, dos excepciones llaman la atención: en Asia el asunto se cuelga hasta la posición número cuatro, y en Oriente Medio aparece en la posición número seis.

En Latinoamérica...las prioridades cambian

Como en el resto del mundo, la pandemia y la crisis económica cambió perspectivas y desveló fragilidades en los países latinoamericanos. Necesariamente, también modificó la lista de riesgos percibidos por Directores y Administradores.

Este año, los 7 riesgos percibidos poco tienen que ver con los registrados en 2023, revelando temas sociales, políticos y económicos urgentes y, en general, un fuerte reacomodo de prioridades (ver gráfico comparativo 7 Riesgos para Directores y Administradores 2023-2024).

Comparación de los Top 7 Riesgos 2023 – 2024 para Directores y Administradores en Latinoamérica

2023	2024
▪ Pérdida de datos 87%	▪ Salud y seguridad 87%
▪ Ciberataques 87%	▪ Ataques cibernéticos 86%
▪ Cibercrímenes 83%	▪ Pérdidas de datos 83%
▪ Insolvencia/bancarrota y problemas financieros 78%	▪ Incumplimiento de regulaciones 83%
▪ Crimen entre los empleados 78%	▪ Sistemas y controles 79%
▪ Ciberextorsión 78%	▪ Sobornos y corrupción 78%
▪ Incumplimiento de regulaciones 78%	▪ Incumplimiento de sanciones 78%

Fuente: Global Directors' and Officers' Survey Report 2024 – Global Finex. Clyde&Co/WTW

Al analizar ambas listas, vale la pena hacer las siguientes precisiones:



Salud y seguridad, que antes ni siquiera figuraban en la lista para Latinoamérica, desplaza de la posición número uno al cuarto lugar al tema de Ciberseguridad.



El **incumplimiento de sanciones, sobornos y corrupción** conquistan su lugar entre los 7 riesgos más destacados para ocupar la quinta y sexta posición respectivamente.



Los reajustes no significan que los temas de **Ciberseguridad, Protección y Manejo de Datos, y el Incumplimiento de la Normativa o la Legislación** dejen de ser relevantes en la región (de hecho, lo son desde hace tiempo). Entre otras razones, por el definición y crecimiento de normativas recientes; particularmente en el tema de manejo de datos.

Un mayor rigor en las regulaciones obliga, por ejemplo, a que todas las empresas que cotizan en bolsa revelen sus políticas de ciberseguridad. Además, cuando sufren

ciberataques deben informarlo en un plazo de cuatro días (Securities and Exchange Commission).

De hecho, cada gobierno latinoamericano se apresta o ya desarrolla leyes de ciberseguridad que tocan a sectores críticos. Y es que el ataque a una sola empresa o infraestructura esencial basta. El peligro radica en sus consecuencias en cascada, puesto que la economía de todo un país podría verse afectada.



El incumplimiento de la normativa y la legislación. Este tema destaca en la región debido a la multiplicación de leyes extraterritoriales -por ejemplo, las que se refieren a la protección de datos-. A un marco legal donde la inteligencia artificial y los negocios de plataformas rebasan fronteras, se suman nuevas preocupaciones como la sustentabilidad y el cambio climático, los planes de descarbonización que pueden aplicar al negocio no por las afectaciones directas al medio ambiente, sino porque así lo exigen los mismos usuarios.



Un futuro donde resistirse a la innovación, también es un riesgo

En Latinoamérica aún falta mucho para poder afirmar que los riesgos cibernéticos son gestionados y controlados en la medida que deben serlo. La inseguridad jurídica, las prácticas comerciales, los ciclos económicos y de inversión extranjera, y las prácticas comerciales ralentizan reacciones y acciones. Máxime cuando cada país de la región también comienza a enfrentar riesgos que hasta hace poco ni siquiera aparecían en el horizonte.

Hoy, por ejemplo, no innovar es asumir un riesgo. No cambiar, un peligro latente que tiene que ver con lo que cada empresa latinoamericana debería estar haciendo a partir del análisis de las señales que hoy emiten las economías de la región y sus mercados.

A medida que el mundo cambia, para cada nación de Latinoamérica las preocupaciones y los riesgos percibidos se modifican y exigen nuevas fórmulas de gestión de la operación y del riesgo. Las preguntas y las respuestas también se renuevan, e incluso traen al escenario coberturas y seguros distintos.

Un ejemplo:



En casos de ataques cibernéticos como el sufrido por IFX en Colombia, el seguro paramétrico fue la respuesta para una agresión que entró vía un tercer participante en la cadena de valor de la organización.

En ambientes tan volátiles como inciertos, las preguntas se multiplican:

- ¿Cómo protegerse contra los mayores riesgos percibidos o riesgos emergentes?
- ¿Es posible acceder a productos o respuestas innovadoras?
- ¿Qué ventajas o beneficios aportan nuevas fórmulas como los seguros paramétricos, cuándo y cómo conviene contratarlos?
- ¿Cuál es la cobertura correcta en renglones percibidos como de alto o muy alto riesgo?
- ¿Entendemos realmente el alcance de nuestras coberturas?
- ¿Estamos sobreprotegidos o nos hemos quedado cortos en renglones de importancia vital para el negocio?
- ¿Persisten dudas esenciales sobre las coberturas contratadas y los riesgos cubiertos?

WTW analiza riesgos y define nuevas soluciones para impulsar las acciones correctas. El objetivo, entender verdaderamente a fondo los peligros y las preocupaciones en materia de riesgos, diseñar diagnósticos y respuestas que conformen marcos de protección a la medida de cada organización, de acuerdo con su sector, circunstancia y naturaleza.

Acerca de WTW

En WTW (NASDAQ: WTW), proporcionamos soluciones analíticas basadas en datos en las áreas de personas, riesgo y capital. Potenciando la visión global y la experiencia local de nuestros profesionales presentes en más de 140 países y mercados, te ayudamos a perfilar tu estrategia, a mejorar tu resiliencia organizacional, a motivar a tu personal y maximizar tu rendimiento y aportamos la perspectiva que te impulsa.

Aviso Legal (Disclaimer)

WTW ofrece intermediación de seguros, y servicios de consultoría a través de entidades legales debidamente registradas ante los reguladores de cada país donde WTW opera. Para más detalles sobre las licencias y regulaciones de las entidades legales de WTW que operan en su país por favor referirse al sitio web de WTW: <https://www.wtwco.com/en-GB/Notices/global-regulatory-disclosures>.

Es un requisito normativo para nosotros considerar nuestros requerimientos de licencias locales antes de establecer cualquier acuerdo comercial. y/o contractual con nuestros clientes.

Las informaciones compartidas en esta publicación son consideradas precisas en la fecha de su comunicación, indicada en este documento. Estas informaciones pueden haber sido cambiadas o reemplazadas posteriormente y no se deben clasificar como precisas o adecuadas después de esta fecha. La presente publicación ofrece un resumen general sobre el tema al que se refiere. No aborda necesariamente todos sus aspectos ni todos los productos disponibles en el mercado. No es la intención que se la utilice (ni debe utilizarse) en reemplazo de asesoramiento específico referido a situaciones individuales.

WTW no ofrece (y no debe suponerse que la presente constituye) asesoramiento en materia contable, jurídica, regulatoria o tributaria. Si tiene previsto adoptar medidas o tomar decisiones sobre la base de los contenidos de esta publicación, le recomendamos consultar primero a un profesional apropiado para recibir asesoramiento específico en la materia. Es probable que parte de la información contenida en la presente se haya obtenido de fuentes externas que consideramos confiables, no obstante, lo cual no garantizamos ni asumimos responsabilidad por la exactitud de dicha información. Las opiniones expresadas no necesariamente reflejan las de WTW.