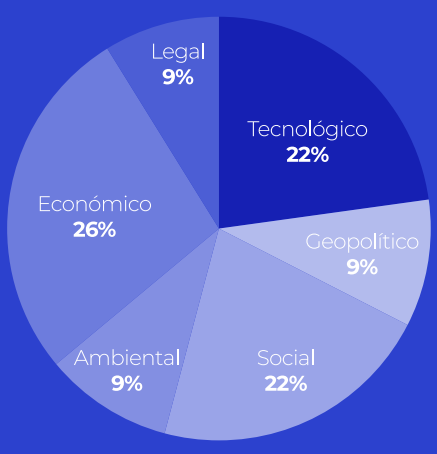
RIESGOS EMERGENTES 2026

Como parte del ejercicio de Riesgos Emergentes 2026 se incorporaron cuatro nuevas compañías del conglomerado financiero, con actividades estratégicas que amplían el enfoque del análisis y la identificación de riesgos que podrían afectar la operación de Grupo Aval y sus Entidades. Para este año se integraron diversas fuentes de información, ampliando el alcance y fortaleciendo el proceso de identificación.

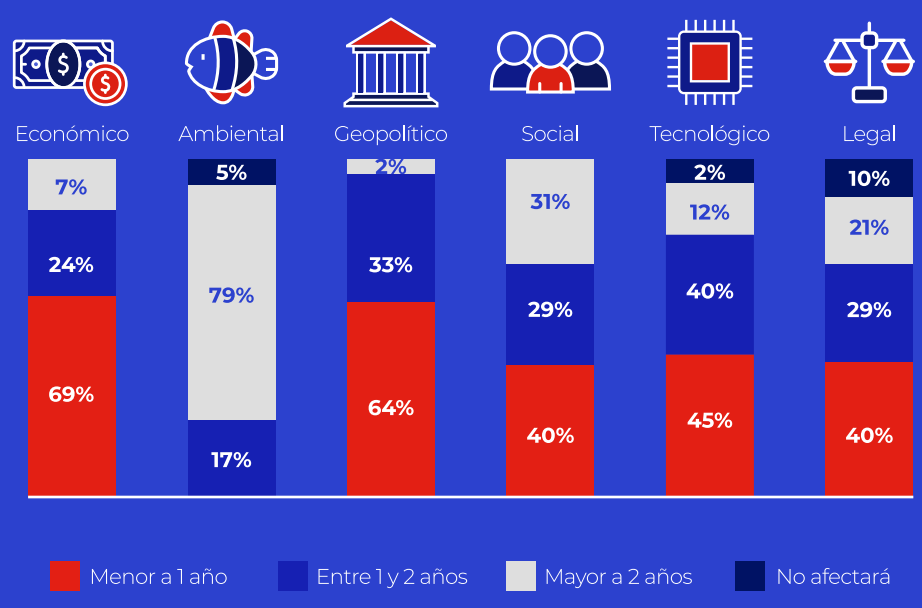
La metodología se basa en el análisis de factores (PESTAL): Político, Económico, Social, Tecnológico, Ambiental y Legal, los cuales pueden combinarse en algunos riesgos. Para complementar este análisis realizamos una encuesta liderada por las áreas de riesgo de las entidades.

Como resultado de la encuesta se obtuvieron los siguientes hallazgos:

Presencia de los Riesgos Emergentes clasificados por categorías (PESTAL)



Horizonte de impacto por categoría (PESTEL)



Realizada la evaluación de los riesgos identificados se estableció que los riesgos emergentes que podrían impactar de manera transversal las líneas de negocio en el corto plazo son los siguientes:

1 CIBER INSEGURIDAD (TECNOLÓGICO): UNA AMENAZA QUE PUEDE CRECER RÁPIDAMENTE

La ciber inseguridad se ha convertido en uno de los riesgos globales más altos. El aumento de la dependencia digital ha incrementado las vulnerabilidades frente a ciberdelincuentes, incluyendo robo de datos, fraudes, ransomware y espionaje, tanto en entidades públicas como privadas. Aunque el avance tecnológico aporta beneficios, también genera amenazas más complejas, especialmente con herramientas avanzadas como inteligencia artificial y agentes. Estos factores han posicionado la ciber inseguridad entre los riesgos emergentes más relevantes para Grupo Aval.

Estas situaciones pueden generar impactos graves en la operación, marca y reputación de Grupo Aval y sus entidades, especialmente en el sector financiero, así como efectos económicos derivados de posibles reclamaciones de clientes afectados por vulneraciones.

Algunas acciones implementadas para mitigar estos riesgos incluyen:

CAMPAÑAS DE EDUCACIÓN financiera para el adecuado uso de los canales.

PRUEBAS DE SEGURIDAD sobre los portales y aplicaciones de las entidades desde diferentes escenarios.

INCREMENTO DEL MONITOREO de señales de alerta, que puedan derivar en posibles incidentes de ciberseguridad.

MONITOREO de la marca en redes.

MADURACIÓN de un sistema de gestión de riesgo de fraude externo transaccional.

2 INFORMACIÓN ERRÓNEA Y DESINFORMACIÓN (TECNOLÓGICO): UN RIESGO CRECIENTE Y MÁS "FACIL" DE CREER

La información errónea y la desinformación se han convertido en amenazas relevantes para la estabilidad social, económica y empresarial. La rápida difusión de contenido falso mediante redes sociales, algoritmos y tecnologías como los deepfakes dificulta distinguir la realidad, afecta la confianza pública, incrementa la polarización y deteriora la reputación de las marcas.

En el sector financiero, este riesgo es crítico, ya que noticias falsas o rumores malintencionados pueden generar volatilidad, afectar el valor de activos, provocar corridas bancarias y deteriorar la reputación. La desinformación puede manipular percepciones sobre ciberataques, liquidez o solvencia, facilitar fraudes y alimentar campañas coordinadas de desprestigio. Grupo Aval y sus entidades también están expuestos a estos impactos.

Las acciones para mitigar este riesgo incluyen el fortalecimiento del monitoreo digital, protocolos de comunicación en crisis, capacitación digital interna y detección temprana de contenido manipulado. Una gestión activa de la reputación, apoyada en tecnología y análisis de datos, es esencial para proteger la confianza en Grupo Aval y sus Entidades.

Grupo AVAL