

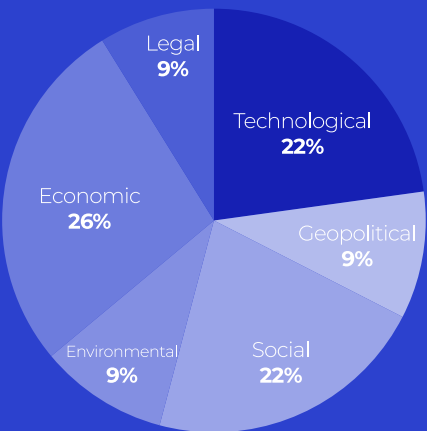
EMERGING RISKS 2026

As part of the Emerging Risks 2026 exercise, four new companies from the financial conglomerate were incorporated. These companies, with strategic activities, broaden the scope of the analysis and the identification of risks that could affect the operation of Grupo Aval and its Entities. For this year, various information sources were integrated, expanding the scope and strengthening the identification process.

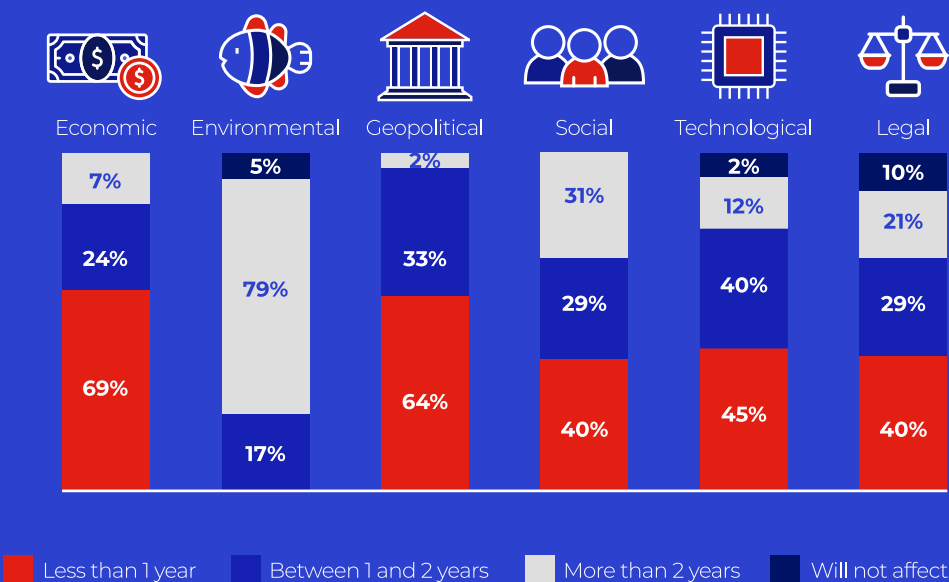
The methodology is based on the analysis of PESTAL factors (Political, Economic, Social, Technological, Environmental, and Legal), which may combine in certain risks. To complement this analysis, a survey was conducted, led by the risk areas of the entities.

As a result of the survey, the following findings were obtained:

Emerging Risks Classified by categories (PESTAL)



Impact horizon by category (PESTEL)



Having evaluated the identified risks, it was determined that the emerging risks with the potential to impact business lines transversally in the short term are the following:

1 CYBER INSECURITY (TECHNOLOGICAL): A THREAT THAT CAN GROW RAPIDLY

Cyber insecurity has become one of the highest global risks. The increased dependence on digital systems has heightened vulnerabilities to cybercriminals, including data theft, fraud, ransomware, and espionage, affecting both public and private entities. Although technological advances bring significant benefits, they also create more complex threats, especially with advanced tools such as artificial intelligence and agents. These factors have positioned cyber insecurity as one of the most relevant emerging risks for Grupo Aval.

These situations can generate severe impacts on the operation, brand, and reputation of Grupo Aval and its entities, especially in the financial sector, as well as economic effects derived from possible claims submitted by customers affected by breaches.

Some actions implemented to mitigate these risks include:



FINANCIAL EDUCATION
campaigns for the proper use of channels.



SECURITY TESTING
on the entities' portals and applications from different scenarios.



INCREASED MONITORING
of warning signs that may lead to potential cybersecurity incidents.



BRAND MONITORING
on social networks.



MATURATION
of a management system for transactional external fraud risk.

2 MISINFORMATION AND DISINFORMATION (TECHNOLOGICAL): A GROWING AND EASIER TO BELIEVE RISK

Misinformation and disinformation have become significant threats to social, economic, and business stability. The rapid spread of false content through social media, algorithms, and technologies such as deepfakes makes it difficult to distinguish reality, undermines public trust, increases polarization, and damages brand reputation.

In the financial sector, this risk is critical, as false news or malicious rumors can generate market volatility, affect asset values, trigger bank runs, and deteriorate an entity's reputation. Disinformation can manipulate perceptions regarding cyberattacks, liquidity, or solvency, facilitate fraud, and fuel coordinated smear campaigns. Grupo Aval and its entities are also exposed to these impacts.

Actions to mitigate this risk include strengthening digital monitoring, crisis communication protocols, internal digital training, and early detection of manipulated content. Active reputation management, supported by technology and data analysis, is essential to protect trust, a fundamental asset for Grupo Aval and its Entities.