FLASH REPORT

Aug.26

AI Application

Business Management and Governance Risks

Artificial Intelligence is no longer a technological promise; it has become an unavoidable operational and corporate reality. For senior leadership, the immediate challenge is no longer just innovation; it now includes establishing a governance architecture that protects trade secrets and ensures perfect alignment between People, Processes, and Technology.

H7 ADVISORS

The context

The use of Artificial Intelligence has advanced continuously in the personal and professional lives of executives and companies worldwide. Access to this technology, previously restricted and high-cost, has become democratic and affordable in recent years.

It has become common to see professionals using Large Language Model (LLM) chatbots to automate research, analysis, and writing tasks. However, this reach and the speed of adoption have reinforced "Shadow IT"—a concept defining the use of software and hardware by employees without formal evaluation or approval from IT or cybersecurity teams.

The indiscriminate use of these tools in the production environment raises critical debates regarding information security and the accuracy of deliverables, posing a challenge for digital governance, especially in companies managing complex operations and integrated supply chains.

What Has Changed in Pratice?

Implementing AI in corporate operations has become the new differentiator for leaders who wish to position their corporations at the market's forefront. However, the speed of adoption cannot overlook precision and security.

The first point of attention is avoiding the illusion of certainty. Although AI excels at processing large volumes of data and modeling multiple scenarios rapidly, its results depend intrinsically on the refinement of prompts and the data used in its analysis context.

Secondly, negligence regarding information security is a liability often assumed by omission. When employees use public AI tools outside the company’s controlled infrastructure to process corporate data, confidential information may be used to train the tool’s algorithm. In practice, the company assumes the unmanaged risk of leaking industrial secrets, financial data, and legally protected information, losing control over its own data security.

Finally, managers must discard the illusion that AI entirely replaces human judgment. H7 Advisors firmly believes in the balanced conjunction of people, processes, and technology, where technology should be applied to empower teams, not to replace them.

Companies that rushed into the AI boom, laying off entire teams for the sake of absolute automation, have already backtracked due to quality losses. What effectively changes is the need for a surgical diagnosis: the technology is available, but it requires rigorous alignment between personnel training, the redesign of process flows, and an adjusted technology architecture.

Why This Matters for Operations in Brazil?

Brazil has a market with over 25 million active companies, where the endless search for operational cost reduction and margin optimization leads to the rapid adoption of new technologies. Naturally, AI is a powerful tool in this context.

However, Brazil has an extremely complex regulatory and compliance framework, with rigorous oversight on issues such as the LGPD (General Data Protection Law). Implementing productivity tools without adapting them to local bureaucratic and legal rigidity is a shortcut to litigation.

There is a dangerous gap between acquiring the technology and orchestrating its secure integration, requiring business management to consider the reality of the Brazilian landscape in its risk matrix.

Key Question for Companies

In this scenario, boards and executive leadership must confront their operational reality with the following management reflections:

- Does your company have a clear and active governance policy regarding the use of AI in the organization?
- Is your operation evaluating AI implementation as a technology project, or have you already mapped the need for re-aligning people and processes?

- If a data security incident occurs or an incorrect decision is made based on an AI hallucination, does your board have a mapped responsibility matrix and a crisis protocol?

Recommended Immediate Actions

To ensure business continuity and corporate resilience, H7 Advisors recommends that management execute three immediate tactical moves:

1. **Shadow IT and LGPD Audit:** Engage the IT and Legal departments to audit the unofficial use of Artificial Intelligence by employees, aiming to stop any input of unanonymized corporate data into public LLMs.
2. **Creation of an AI and Governance Committee:** Establish a multidisciplinary working group to design a "Safe Use Playbook," defining the transition to closed (Enterprise) AI environments that ensure absolute confidentiality of business information.
3. **Adoption of organizational optimization:** Perform internally, or seek an external partner to perform an organizational reorganization of operations. The secure integration of disruptive technologies requires excellent professionals with experience who can perfectly structure the "People, Processes, and Technology" triad, mitigating risks before they even materialize.

Conclusion

Artificial Intelligence does not replace strategic leadership, but it can lead management to unprecedented levels. However, technology, no matter how brilliant, is merely the means.

Adopting AI impulsively, while neglecting the necessary engineering in personnel training and process architecture, is the fastest way to put company equity at risk through compliance failures, biased decisions, and regulatory shutdowns.

Extreme efficiency is within the market's reach, but survival in the current scenario requires that innovation be guided by analytical intelligence, rigorous risk management, and absolute operational orchestration.

To navigate this landscape of rapid AI adoption without exposing your corporation to severe data and compliance vulnerabilities, your business needs a rigorous governance architecture. Connect with H7 Advisors to map your digital exposure and seamlessly integrate People, Processes, and Technology, ensuring your operations remain secure under any circumstances.

ABOUT H7 ADVISORS

H7 Advisors is a strategic advisory firm specializing in protecting critical infrastructure and complex operations across Latin America. We architect secure corporate frameworks, enabling global capital to operate safely in highly volatile jurisdictions.

H7 ADVISORS

Navigating Complexity.
Safeguarding Assets.

www.h7advisors.com