Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2024 | Submission: 02/16/2024 | Accepted: 02/19/2024 | Publication: 02/22/2024

Corporate information governance: security, data privacy, and executive management in the age of artificial intelligence.

Corporate information governance: security, data privacy and executive management in the age of artificial intelligence

Corporate Information Governance: Security, Data Privacy and Executive Management in the Artificial Intelligence Era

Ricardo Saddi Becker holds

a Bachelor's degree in Computer Science from the Federal University of Mato Grosso (2009).

DRII Certified Business Continuity Specialist

SUMMARY

Information has become one of the main strategic assets of contemporary organizations, playing a key role in generating value, innovation, and competitiveness.

Alongside the exponential growth in data volume and the incorporation of Artificial Intelligence (AI)-based technologies, challenges related to information security, data subject privacy, and corporate governance have expanded. In this context, this study analyzes the integration between information governance, data protection, executive management, and cybersecurity, discussing how these elements contribute to building more resilient, transparent, and data-driven organizations. The research was developed through an exploratory and descriptive literature review, based on scientific literature, international standards, and governance frameworks widely adopted in the corporate environment. The results show that information protection has ceased to represent merely an operational responsibility of Information Technology areas and has become a strategic responsibility shared among executives, boards of directors, and organizational leaders. It is concluded that integrated governance models, combined with the adoption of structured security, privacy, and risk management practices, are essential factors for ensuring regulatory compliance, business sustainability, and institutional trust in a scenario characterized by the increasing digitalization of economic and social relations.

KEYWORDS: Information Governance; Information Security; Data Privacy; Artificial Intelligence; Executive Management.

ABSTRACT

Information has become one of the most valuable strategic assets of contemporary organizations, playing a decisive role in value creation, innovation and competitiveness. Simultaneously with the exponential growth of data volumes and the incorporation of Artificial Intelligence (AI) technologies, challenges related to information security, data privacy and corporate governance have intensified.

This study examines the relationship between information governance, data protection, executive management and cybersecurity, discussing how these elements contribute to the development of resilient, transparent and data-driven organizations. The research was conducted through an exploratory and descriptive literature review based on scientific publications, international standards and recognized governance frameworks. The findings demonstrate that information protection is no longer solely an operational responsibility of Information Technology departments, becoming instead a strategic concern shared by executives, boards of directors and organizational leadership. The study concludes that integrated governance models, combined with structured practices in security, privacy and risk management, are fundamental to ensuring regulatory compliance, business sustainability and institutional trust in an increasingly digital economy.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2024 | Submission: 02/16/2024 | Accepted: 02/19/2024 | Publication: 02/22/2024

KEYWORDS: Information Governance; Information Security; Data Privacy; Artificial Intelligence; Executive Management.

INTRODUCTION

The digital economy has profoundly transformed the way organizations produce.
Knowledge allows them to make decisions and establish competitive advantages. The expansion of environments
Connected technologies, cloud computing, digital platforms, and Artificial Intelligence have expanded...
significantly increasing the strategic value of data, making information an indispensable resource.
for innovation, the development of new business models and the strengthening of
business competitiveness.

However, the same scenario that fosters opportunities also increases the complexity of management.
Corporate. The exponential growth in the volume of information, the continuous circulation of data.
personal, the integration between different technological ecosystems and the growing dependence on
Digital services have increased risks related to privacy, cybersecurity, and...
Regulatory compliance and governance of information assets. As a consequence, the
The management of these resources has ceased to be an exclusively technical task.
to assume a strategic dimension in organizations.

In recent years, legislation aimed at protecting personal data, such as the General Data Protection Law, has been enacted.
The Brazilian General Data Protection Law (LGPD) and the European General Data Protection Regulation (GDPR) in the European Union.
Europeans reinforced the need for mechanisms capable of ensuring transparency,
responsibility and control over the handling of information. In parallel, the rapid evolution of
AI-based solutions have introduced new challenges related to their ethical use.
From data, to the transparency of algorithms and accountability for automated decisions. In this
In this context, information governance emerges as a discipline responsible for establishing policies,
Processes and responsibilities that ensure the safe, ethical, and strategic use of assets.
informational. More than ensuring regulatory compliance, its purpose is to promote
Data quality, strengthen decision-making, reduce corporate risks, and expand...
The ability to generate value from information.

The participation of executive leaders is becoming increasingly important in this process. Councils of
administration, executive directors, technology managers, and those responsible for data protection.
They will share responsibilities related to defining governance strategies, and...

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2024 | Submission: 02/16/2024 | Accepted: 02/19/2024 | Publication: 02/22/2024

digital risk management and the establishment of an organizational culture oriented towards information protection and the responsible use of Artificial Intelligence.

Given this scenario, this study aims to analyze the relationship between governance and... Information, information security, data privacy, and executive management, discussing how These elements complement each other in building organizations capable of reconciling innovation. technological, regulatory compliance and business sustainability in an environment characterized due to increasing digital complexity.

METHODOLOGY

This research is characterized as an exploratory and descriptive study. developed through a literature review. According to Gil (2019), this procedure The methodological approach allows for gathering, organizing, and critically analyzing different theoretical perspectives on... a given phenomenon, facilitating the understanding of conceptual and practical transformations. observed in contemporary organizational contexts.

The literature review included books, scientific articles, international standards, Institutional publications and governance guidelines related to information security. personal data protection, corporate governance, Artificial Intelligence, risk management and digital transformation. Priority was given to projects recognized by the academic and technical community. as well as documents produced by international organizations dedicated to the development of best practices in information governance.

The selected sources were subjected to qualitative analysis, seeking to identify convergences. conceptual frameworks, widely adopted management models, and trends observed in the evolution of Corporate information governance practices. To promote a systematic approach, the The content was organized into five thematic areas: fundamentals of information governance; Data privacy and regulatory compliance; Artificial Intelligence and risk management; Security Information from an executive perspective; and data-driven strategic leadership.

In addition to the classic literature on governance and information management, the following were considered as benchmarks. recent developments related to the regulation of Artificial Intelligence, and to international principles of digital ethics and standards aimed at protecting the privacy and security of information assets. This approach makes it possible to integrate established principles from the literature with the challenges.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2024 | Submission: 02/16/2024 | Accepted: 02/19/2024 | Publication: 02/22/2024

emerging factors resulting from rapid technological evolution and new regulatory requirements.
to organizations.

1. FUNDAMENTALS OF INFORMATION GOVERNANCE

Digital transformation has substantially changed the way organizations create value.
making information one of the main strategic assets in the corporate environment. Data generated
operations, customers, suppliers, connected devices, and digital platforms have become
to support business decisions, drive innovation initiatives, and guide strategies.
growth. In this context, information governance ceases to be a restricted activity.
Information Technology is taking on a cross-cutting role, involving different areas of
Organization and levels of leadership.

Information governance can be understood as the set of policies, processes,
responsibilities and control mechanisms designed to ensure that information assets
They should be managed consistently throughout their entire life cycle. Their purpose is not...
It is limited to data protection, but seeks to ensure that the information is reliable, complete,
accessible, used ethically, and aligned with the institution's strategic objectives.
Form, quality, safety, compliance, and value creation become inseparable dimensions.
of information management.

The consolidation of this discipline stems from the understanding that organizational decisions are
directly influenced by the quality of the available data. Incomplete information,
Inconsistent or outdated data compromises management analyses and hinders compliance with...
regulatory requirements can have financial, operational, and reputational impacts.
relevant. From this perspective, information governance establishes criteria for standardization,
classification, retention, sharing and disposal of information assets, reducing
Removing ambiguities and strengthening the reliability of corporate decisions.

Among the most relevant pillars of this model, the clear definition of roles and...
responsibilities. Organizations with a higher degree of maturity tend to distinguish between assignments.
among sponsoring executives, data owners , *and* managers responsible for
quality of information *(Data Stewards)* and technical teams in charge of managing the
technological environments. This segregation fosters greater institutional accountability, expands the
Transparency in processes and reduces conflicts related to data usage.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2024 | Submission: 02/16/2024 | Accepted: 02/19/2024 | Publication: 02/22/2024

Another essential element relates to the management of the information lifecycle. From its creation or From collection to archiving and final disposal, data goes through different stages that require... Specific controls. The absence of policies for retention, document classification, or disposal. Insurance increases exposure to regulatory risks and compromises the efficiency of document management. For this reason, modern governance models establish objective criteria for each phase of this process. cycle, reconciling legal requirements, operational needs and strategic interests of organization.

Data quality also occupies a central position in governance practices. Dimensions such as Accuracy, consistency, completeness, timeliness, and uniqueness directly influence reliability. from analyses performed by business areas. The expansion of Business Intelligence initiatives, Analytics and Artificial Intelligence have made it even more evident that analytical models produce Results are only achieved insofar as they utilize reliable databases. Thus, investments in Advanced technologies tend to exhibit limited performance when not accompanied by... structured information quality programs.

Beyond operational aspects, information governance strengthens the adaptability of Organizations facing regulatory and technological changes. The existence of policies. Institutionalized, formally defined responsibilities and documented processes facilitate the Incorporating new legal requirements reduces the impacts resulting from transformations. organizational and increases predictability in the management of informational assets.

In this scenario, an important conceptual evolution is observed: information ceases to be treated... merely as an operational resource to consolidate itself as a strategic asset of the organization. Its Proper governance directly influences the ability to innovate, compete, and meet demands. regulatory compliance and establishing trusting relationships with clients, partners, investors, and regulatory bodies. oversight. In data-driven organizations, the maturity of information governance It has become a relevant indicator of the institution's own capacity to generate value in a sustainable way.

2. DATA PRIVACY AND REGULATORY COMPLIANCE

The intensification of the collection, sharing, and processing of personal information. This has transformed privacy into one of the main challenges of contemporary corporate governance. The growth of digital services, cloud computing, collaborative platforms, and... Applications based on Artificial Intelligence have significantly expanded the flow of data between

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2024 | Submission: 02/16/2024 | Accepted: 02/19/2024 | Publication: 02/22/2024

organizations, suppliers and users, requiring mechanisms capable of ensuring treatment
Responsible for the information and respect for the rights of data subjects.

The evolution of this scenario has driven the strengthening of regulatory frameworks aimed at protection.
of personal data. The entry into force of the General Data Protection Law (LGPD) in Brazil, and of
The General Data Protection Regulation (GDPR) in the European Union has consolidated a change.
This paradigm shift establishes that the use of personal data must adhere to related principles.
to purpose, necessity, transparency, security, accountability, and reporting. These
Legislation represents not only legal instruments for oversight, but also benchmarks capable of...
to guide more mature models of information governance.

From this perspective, regulatory compliance should not be understood as a limited activity.
In compliance with legal requirements. Organizations that handle data protection exclusively.
As a regulatory obligation, they tend to adopt specific and reactive measures. In contrast,
Institutions that incorporate privacy into their organizational strategy develop policies.
Permanent data management measures, strengthening the trust of data subjects and reducing associated risks.
due to the misuse of information.

One of the most relevant principles in this context is the concept of *Privacy by Design,* according to which
Privacy requirements should be considered from the early stages of product design.
Organizational services and processes. Instead of implementing controls only after identification.
To address these problems, this approach encourages the proactive integration of data protection into
Developing technological solutions, reducing adaptation costs and increasing effectiveness.
of the security mechanisms.

Additionally, the *Privacy by Default* principle establishes that the default settings of
Systems should prioritize the least possible processing of personal data, limiting the collection and processing of personal data.
Sharing only the information strictly necessary for each purpose. This guideline reinforces
the idea that privacy protection does not depend exclusively on user behavior,
but also the architectural decisions adopted during the development and operation of
systems.

The implementation of structured privacy programs also requires permanent mechanisms for
Governance. Data inventories, mapping of information flows, activity records.
treatment, data protection impact assessments, and formal processes for addressing
Data subjects' rights are fundamental instruments for ensuring ongoing compliance.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2024 | Submission: 02/16/2024 | Accepted: 02/19/2024 | Publication: 02/22/2024

These practices also promote greater transparency with regulatory authorities and reduce the time required to respond to incidents involving personal information.

Another aspect of increasing relevance relates to the management of risks arising from sharing. Data sharing with third parties. Complex supply chains, outsourced services, platforms in Cloud computing and digital ecosystems increase the need for ongoing evaluation of adopted practices. by business partners. Organizational compliance, therefore, no longer depends solely on Internal controls are being implemented, and due diligence mechanisms and contractual clauses are being incorporated. specific, periodic audits and objective criteria for the selection and monitoring of operators data.

The figure of the Data Protection Officer, known internationally as *The Data Protection Officer* (DPO) reinforces this governance model by acting as an element of Integration between the organization, stakeholders, and oversight authorities. More than just performing a function. In an advisory role, this professional contributes to disseminating a data protection culture and supporting decision-making. Strategic planning and guiding compliance programs aligned with regulatory requirements and best practices. international practices.

As the digital economy evolves, privacy is no longer perceived merely as a requirement. legal to consolidate itself as a competitive differentiator and an essential element of institutional reputation. Organizations capable of demonstrating transparency, accountability, and commitment to protection. Data strengthens trust relationships with clients, partners, and investors, transforming the... Regulatory compliance as a strategic component of sustainability and governance. corporate.

3. ARTIFICIAL INTELLIGENCE, ALGORITHMIC GOVERNANCE AND MANAGEMENT OF RISKS

The incorporation of Artificial Intelligence (AI) into organizational processes represents one of the The most significant transformations of today. Systems capable of analyzing large volumes of Data analysis, identifying complex patterns, and supporting real-time decisions have been employed in sectors such as health, finance, industry, logistics, education, and public administration. Although these Technologies that enhance the operational efficiency and analytical capabilities of organizations, their adoption It also introduces challenges related to governance, the transparency of automated decisions, and... Managing the risks associated with algorithmic models.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2024 | Submission: 02/16/2024 | Accepted: 02/19/2024 | Publication: 02/22/2024

Unlike traditional systems, machine learning-based applications
They exhibit dynamic behavior, conditioned by the quality of the data used in the training.
to the characteristics of the algorithms used and the changes that have occurred in the operating environment.
As a consequence, decisions produced by these models may suffer degradation.
performance over time, reproducing statistical biases present in databases, or generating
results whose logic is not fully understood by the users themselves. This characteristic
This reinforces the need for specific governance mechanisms to ensure reliability.
Traceability and human supervision.

In this context, algorithmic governance emerges as a discipline focused on establishing
Policies, responsibilities, and controls applicable to the lifecycle of Intelligence models.
Artificial intelligence. Its goal is to ensure that automated systems are developed.
implemented and monitored in a manner consistent with ethical principles, legal requirements and objectives
Strategic goals of the organization. Governance does not seek to limit technological innovation, but to ensure
that its use occurs in a transparent, responsible manner and is aligned with the institutional interest.

Among the main challenges is the quality of the databases used for training and
Validation of the models. Incomplete, outdated, or statistically unbalanced information.
They compromise the predictive capacity of algorithms and increase the risk of inconsistent decisions.
In applications related to granting credit, recruiting people, medical diagnosis or
Risk analysis: small distortions in the data can have significant impacts on individuals.
and organizations. Therefore, AI governance programs depend directly on maturity.
of the information governance discussed in previous chapters.

Another aspect of increasing relevance refers to the explainability of the models *(Explainable Artificial Intelligence).*
Intelligence – XAI). In critical applications, automated decisions should not be evaluated solely
for statistical accuracy, but also for the ability to provide understandable justifications for

Transparency promotes independent audits and strengthens user confidence. Its results are enhanced by transparency, which facilitates independent audits and strengthens user trust.

and makes it possible to identify factors that influence the behavior of algorithms, especially in
sectors subject to high regulation.

Human supervision remains equally indispensable. Although advanced models are
capable of automating complex activities, the responsibility for organizational decisions
The right to participate remains with the people and institutions that use these technologies.
experts in validating results, periodically reviewing models, and defining limits.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2024 | Submission: 02/16/2024 | Accepted: 02/19/2024 | Publication: 02/22/2024

Automation reduces the likelihood of inappropriate decisions and preserves principles related to corporate responsibility.

The rapid evolution of AI solutions has also increased the importance of continuous management of Technological risks. Mature organizations establish ongoing processes to monitor them. model performance, identifying statistical drift *(model drift),* reviewing parameters of training and evaluating the impacts of changes to datasets. This approach It allows for the detection of degradations before they produce significant consequences for the processes of business.

In recent years, international organizations have begun to structure specific frameworks for Governance of Artificial Intelligence. Initiatives focused on risk management and principles stand out. Ethical principles for the responsible use of AI and guidelines for algorithmic transparency, reflecting a global trend towards strengthening regulatory mechanisms applicable to technologies emerging trends. These initiatives reinforce that innovation and responsibility must evolve in a way that... integrated, preventing efficiency gains from being achieved at the expense of reduced trust. institutional.

From this perspective, Artificial Intelligence ceases to represent merely a tool of Automation is becoming a permanent part of corporate governance. Its responsible use. It depends on the integration between data quality, human oversight, continuous risk assessment, and... mechanisms capable of ensuring transparency, regulatory compliance and accountability in automated decisions.

4. Information Security as a Tool of Governance and Organizational Value

For many years, information security was predominantly treated as a function. technique, focused on the administration of computer controls designed to protect the technological environments. The evolution of digital business models, however, has expanded significantly its strategic relevance. Currently, incidents involving leaks of information, data integrity compromise, or service interruption produce impacts that extend beyond the technological sphere, affecting institutional reputation and performance. Financial security, regulatory compliance, and the trust of clients, investors, and business partners.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2024 | Submission: 02/16/2024 | Accepted: 02/19/2024 | Publication: 02/22/2024

This transformation has changed the way organizations structure their security programs.
The responsibility for protecting information is no longer limited to technical teams and has become shared.
to be integrated into the agenda of boards of directors and senior leadership. Risk management
Cybersecurity has come to be understood as a component of corporate governance, influencing
decisions related to business expansion, technological innovation, third-party management, and
organizational sustainability.

In this context, organizational culture plays a crucial role. The effectiveness of controls...
Security depends not only on the adoption of specialized technologies, but also on...
The behavior of people who produce, share, and use information daily.
Ongoing programs for awareness, training, and skills development.
They strengthen the perception of the risks associated with the improper handling of data and reduce the...
The occurrence of incidents resulting from human error, still responsible for a significant portion.
of security incidents recorded in public and private organizations.

Another relevant aspect concerns the integration between information security and risk management.
Corporate security programs, instead of operating in isolation, should participate in...
strategic planning processes, evaluating potential impacts on institutional objectives,
Continuity of operations, regulatory compliance, and organizational reputation. This integration
It favors more balanced decisions regarding investment prioritization and risk acceptance.
residual controls and the definition of controls compatible with the context of each organization.

The growing reliance on specialized suppliers has also increased the importance of management.
of the risks associated with digital supply chains. Cloud services, platforms
outsourced companies, software providers, technology partners, and companies responsible for
Data processing has become integrated into highly connected ecosystems, in which
External vulnerabilities can have a significant impact on the contracting organization.
Therefore, structured supplier evaluation processes, periodic audits and
Continuous monitoring has become an essential element of security governance.

From an executive perspective, performance indicators take on a strategic role. Metrics
related to the maturity of controls, incident response time, and adherence to policies.
Corporate data, audit results, regulatory compliance, and risk level evolution.
They provide relevant information to support decisions by senior management. Unlike
operational indicators traditionally used by technical teams, these instruments

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2024 | Submission: 02/16/2024 | Accepted: 02/19/2024 | Publication: 02/22/2024

They allow technological risks to be translated into understandable information for responsible managers.
through the organization's strategic direction.
The evolution of digital environments has also reinforced the need for approaches based on
Continuous improvement. Periodic maturity assessments, reviews of institutional policies,
crisis management exercises, independent audits, and systematic learning processes.
Organizational improvements contribute to the continuous improvement of security programs, making them...
more adaptable to technological and regulatory changes.
Finally, it is observed that information security has come to play a relevant role in the generation of
Institutional value. Organizations capable of demonstrating a high degree of maturity in protecting...
Their informational assets tend to strengthen trust relationships with clients, investors, and...
strategic partners, expanding their competitive capacity in increasingly market-oriented markets
by data. In this scenario, security ceases to represent exclusively a cost center for
to consolidate itself as a strategic investment capable of supporting innovation, compliance and
sustainable growth.

5. Executive Leadership and Data-Driven Decision Making

The consolidation of the digital economy has significantly altered the role of leadership in organizations.
The increasing availability of information, coupled with the advancement of analytical platforms and...
Artificial intelligence has expanded companies' ability to understand their business environment.
and respond more quickly to market changes. In this context, decision-making
Data- driven *decision making* no longer represents a competitive advantage.
circumstantial, but becoming an essential component of corporate strategy.
This transformation requires executives to develop skills that go beyond basic expertise.
traditional management. Understanding the principles related to governance of
Information, data protection, cybersecurity, and Artificial Intelligence are now integrated into...
a set of skills needed to guide investments, assess risks, and establish
Organizational priorities. The role of leadership is no longer focused exclusively on management.
financial and operational, incorporating responsibilities related to ethical, safe and effective use.
strategic management of informational assets.
The digital maturity of organizations is directly associated with their ability to integrate data.
Information originating from different business areas in consistent decision-making processes.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2024 | Submission: 02/16/2024 | Accepted: 02/19/2024 | Publication: 02/22/2024

produced by corporate systems, customer relationship platforms, indicators
Financial technologies, industrial sensors, and digital environments allow for a more comprehensive view.
of institutional performance. However, the mere availability of this data does not guarantee
better decisions. Their effectiveness depends on the existence of governance mechanisms capable of
To ensure quality, reliability, and context for the interpretation of information.
In this scenario, Business Intelligence, Analytics, and Artificial Intelligence play key roles.
Complementary. While analytical platforms offer support for identifying trends.
and behavioral patterns, AI models expand the predictive capacity of organizations and
They help in simulating complex scenarios. However, the use of these technologies must
to remain subordinate to the strategic objectives defined by leadership, preventing decisions from being made indiscriminately.
Automated processes replace the critical analysis necessary for organizational management.
Integrated action between the Board of Directors, Chief Executive Officer (CEO), Chief
Information Officer (CIO), Chief Information Security Officer (CISO) and Person in Charge of
Data Protection Officer (DPO) has become one of the main indicators of maturity in
Corporate governance. The coordination between these functions fosters greater alignment with innovation.
technological, risk management, regulatory compliance and institutional objectives, reducing the
Fragmentation of decisions related to digital transformation.
Another relevant element refers to the establishment of indicators capable of translating
Technical information in metrics understandable to senior management. Key performance indicators of
Performance indicators (KPIs) and key risk indicators (KRIs) related to data quality,
regulatory compliance, governance maturity, privacy protection and efficiency
operational data provides objective support for monitoring institutional development and for
Defining strategic priorities.
The sustainability of digital organizations also depends on the consolidation of a culture.
driven by data. This transformation does not stem exclusively from the adoption of new technologies,
but also the institutional capacity to incorporate objective evidence into planning processes,
Innovation and decision-making. Organizational environments that encourage transparency.
Responsible sharing of information and continuous learning present greater
Ability to adapt to regulatory, technological, and market changes.
Finally, it is observed that contemporary leadership now plays an integrating role among
Technology, governance, and strategy. The ability to transform data into reliable knowledge.
Promoting innovation responsibly and balancing opportunities with risks has become a key factor.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2024 | Submission: 02/16/2024 | Accepted: 02/19/2024 | Publication: 02/22/2024

crucial for organizations seeking competitiveness in an environment characterized by
Rapid technological evolution and increasing dependence on informational assets.

CONCLUSION

The increasing centrality of information in economic and institutional activities has redefined the way
How organizations structure their management, innovation, and value creation processes. In a
an environment marked by the intensification of digital transformation and the expansion of Intelligence.
Artificial and through the strengthening of regulatory requirements related to data protection, the
Information governance is consolidating itself as a strategic element for sustainability.
organizational.

The analysis developed in this study shows that information security, data privacy,
Corporate governance and executive management are interdependent dimensions of the same entity.
management system. The effectiveness of these initiatives does not depend exclusively on the implementation of
specialized technologies, but also the construction of organizational structures capable of integrating
institutional policies, decision-making processes, clearly defined responsibilities and mechanisms
Permanent monitoring and continuous improvement strategies.

It was observed that the quality of information has a direct influence on the ability of
organizations develop reliable analytical models and implement solutions based on
Artificial Intelligence and meeting the growing demands related to transparency and
regulatory compliance. In this context, information governance programs cease to
to have a purely administrative character in order to assume a decisive role in value creation.
institutional and in reducing the risks associated with the use of digital assets.

The evolution of Artificial Intelligence technologies introduces new challenges related to
algorithmic transparency, bias mitigation, human oversight, and accountability for
Automated decisions. These aspects demonstrate that technological innovation needs to be...
accompanied by robust governance mechanisms capable of ensuring a balance between
Operational efficiency, protection of fundamental rights, and corporate responsibility.

Another aspect highlighted throughout this work refers to the importance of senior participation.
Management in the implementation of information governance strategies. Integration between boards.
administration, executives, technology areas, information security and data protection

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2024 | Submission: 02/16/2024 | Accepted: 02/19/2024 | Publication: 02/22/2024

It strengthens the institutional capacity to respond to the transformations of the digital environment, promoting Greater alignment between strategic objectives, innovation, and risk management.

Although this study was developed through a literature review, the references The analyses show convergence regarding the need to treat information as an asset. Strategic for organizations. The maturity of information governance begins to reflect not only the level of regulatory compliance achieved by the institution, but also its capacity to innovate, to preserve the trust of different audiences and support data-driven decisions. reliable.

As for perspectives for future research, it is recommended to further investigate related topics. Impacts of Generative Artificial Intelligence on corporate governance and regulation. international intelligent systems, to governance models for digital ecosystems. distributed and to the use of metrics capable of measuring the strategic return on investment. in information governance and privacy protection.

We understand, therefore, that corporate information governance represents one of the main pillars of data-driven organizations. By integrating information security, privacy, Artificial intelligence, risk management, and executive leadership make it possible to build environments. more transparent, resilient, innovative and prepared to face technological challenges, regulatory and competitive factors that characterize the contemporary digital economy.

REFERENCES

- GIL, AC *How to Develop Research Projects.* 6th ed. São Paulo: Atlas, 2019.

Information and Data Governance • DAMA INTERNATIONAL. *DAMA-DMBOK: Data Management Body of Knowledge.* 2nd ed. Bradley Beach: Technics Publications, 2017.

- WEILL, P.; ROSS, JW *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results.* Boston: Harvard Business School Press, 2004.
- DAVENPORT, TH *Competing on Analytics: The New Science of Winning.* Boston: Harvard Business School Press, 2007.
- REDMAN, TH *Data Driven: Profiting from Your Most Important Business Asset.* Boston: Harvard Business Review Press, 2008.

Information Security and Management

- WHITMAN, ME; MATTORD, HJ *Principles of Information Security.* 7. Ed. Boston: Cengage Learning, 2022.
- ISACA. *COBIT 2019 Framework: Governance and Management Objectives.* Schaumburg: ISACA, 2019.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year V, v.2 2024 | Submission: 02/16/2024 | Accepted: 02/19/2024 | Publication: 02/22/2024

- ISO/IEC 27001:2022. *Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements.*
- ISO/IEC 27701:2019. *Privacy Information Management.*
- ISO/IEC 38500:2015. *Governance of IT for the Organization.*

Privacy and Artificial Intelligence

- NIST. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. Gaithersburg: National Institute of Standards and Technology, 2023.
- NIST. *Cybersecurity Framework (CSF 2.0).* Gaithersburg: National Institute of Standards and Technology, 2024.
- OECD. *Recommendation of the Council on Artificial Intelligence.* Paris: Organization for Economic Co-operation and Development, 2019.
- BRAZIL. Law No. 13.709, of August 14, 2018. *General Law on the Protection of Personal Data (LGPD).* •

REGULATION (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. *General Data Protection Regulation (GDPR).*

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.