BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Confidentiality, Loyalty, and Responsibility: The Ethical Triad in Information Systems Management in the Field of National Security

Assoc. Prof. Florentina-Loredana DRAGOMIR, PhD*

*"Carol I" National Defence University, Bucharest
e-mail: Dragomir.Loredana@unap.ro

Abstract

With the intensification of hybrid threats, strategic organizations are faced with a fundamental challenge: ensuring a sustainable balance between process transparency, information confidentiality, and decision-making responsibility. This article analyzes the ethical triad of confidentiality, loyalty, and responsibility in the management of information systems in the field of national security, highlighting the need for information governance adapted to the current complexity. At the heart of the analysis is the role of intelligent information systems (IIS), which, by integrating artificial intelligence, machine learning, and behavioral analysis technologies, provide decisive support in modernizing security architectures and strengthening an ethical organizational culture. Intelligent information systems not only optimize threat detection and response processes but also actively contribute to the professionalization of strategic decisions by generating predictive assessments, automatic traceability, and alignment with legal regulations and ethical standards. They allow the transition from a reactive security model to a proactive one, oriented towards anticipation, compliance, and distributed responsibility. In this sense, the article argues that the integration of IIS is no longer an optional technological choice, but a strategic necessity for organizations that manage classified information and critical resources. Through its multidisciplinary approach and theoretically and normatively grounded arguments, the study contributes to the delimitation of a robust conceptual framework regarding the ethical governance of information in national security institutions.

Keywords:
Intelligent Information Systems; National Security; Ethical Governance; Strategic Decision-Making; Confidentiality.

Article info
Received: 30 April 2025; Revised: 28 May 2025; Accepted: 30 May 2025; Available online: 27 June 2025

Citation: Dragomir, F.L. 2025. "Confidentiality, Loyalty, and Responsibility: The Ethical Triad in Information Systems Management in the Field of National Security". *Bulletin of "Carol I" National Defence University*, 14(2): 296-310. https://doi.org/10.53477/2284-9378-25-31

The ethical management of information systems in the field of national security has become a major strategic challenge. Military and security institutions are faced with the need to balance the transparency of operational processes with the protection of sensitive information, in an environment where confidentiality, loyalty, and accountability are essential pillars of institutional trust. Military and security institutions are faced with the need to balance the transparency of operational processes with the protection of sensitive information, in an environment where confidentiality, loyalty, and accountability are essential pillars of institutional trust. In the current strategic climate, deeply marked by accelerated digitalization and geopolitical volatility, the protection of sensitive information is a priority objective for organizations in the field of national security. In parallel, the demands regarding the transparency of processes and institutional accountability are becoming increasingly significant, including in the military sector. Thus, a fundamental ethical dilemma emerges: how can a sustainable balance be ensured between the need for operational transparency and the imperatives of confidentiality?

Confidentiality is no longer just a technical issue, but a fundamental ethical dimension in the architecture of strategic information systems. Recent studies highlight that the effectiveness of information security is influenced by institutional and cultural factors, and the integration of these aspects into security strategies is essential for protecting sensitive data (Metin, et al. 2024). Research emphasizes that the performance of information security systems depends significantly on the institutional context and cultural values, and the incorporation of these factors into security policies is crucial for ensuring the protection of sensitive data (Xu, et al. 2025). The loyalty of personnel with access to classified information is another critical element. Deviant behaviors, such as violating security policies, can have serious consequences for the integrity of information systems. Behavioral analyses highlight the importance of a strong organizational culture and ethical leadership to prevent these risks (Metin, et al. 2024). At the same time, the loyalty of personnel with access to classified information is asserted as an essential link in the security chain. Ethical misconduct and human factor risks remain among the main vulnerabilities of information systems. Preventing these risks requires cultivating a strong organizational culture, rooted in values such as institutional commitment and professional discipline. Accountability, both at the individual and institutional levels, is essential in the governance of information systems. The implementation of clear policies and effective audit mechanisms contributes to ensuring the integrity and availability of information, crucial aspects for the optimal functioning of strategic organizations (Almomani, et al. 2023). On the other hand, responsibility in information governance involves both formal control mechanisms (audit, traceability, regulations) and the conscious assumption of the consequences of decisions taken at all structural levels. The implementation of a framework of distributed responsibility contributes to strengthening institutional resilience and public trust (Almomani, et al. 2023).

In this context, the present article aims to explore the ethical triad formed by confidentiality, loyalty, and accountability, analyzing how these values can be integrated into the management of information systems in the field of national security. Through a multidisciplinary approach, we will examine the ethical challenges and solutions that can contribute to strengthening information security in strategic organizations.

1. Confidentiality in Strategic Information Systems Architecture

1.1 Defining the Concept of Confidentiality in the Context of National Security

Confidentiality, along with integrity and availability, is one of the three essential dimensions of information security, known as the CIA triad. In an operational sense, confidentiality involves protecting data from unauthorized access, ensuring that only authorized individuals or entities can view, manipulate, or distribute sensitive information.

Within national security organizations, this component takes on critical importance. Protecting strategic, military, or diplomatic information from compromise is not just a technical requirement, but an institutional obligation that supports state sovereignty and the functioning of the defense system. Classified information, if disclosed or accessed in an unauthorized manner, can lead to operational vulnerabilities, damage to international relations, or even loss of life in theaters of operations.

One of the fundamental conceptual models for implementing confidentiality is the Bell–LaPadula model. It was designed for military environments, where classification levels are rigorous, and proposes two main rules: simple security property ("no read up") and property ("no write down"). These rules aim to prevent access to higher-level information by users with lower authorizations, respectively blocking the unauthorized transfer of information from higher to lower levels. The application of this model contributes to maintaining a rigorous security hierarchy, in which the information flow is strictly controlled and documented.

Thus, confidentiality in the architecture of strategic information systems must be understood not only as a technological protection measure but also as an ethical and institutional responsibility, anchored in the national and international regulatory framework on information security.

1.2. Technological and procedural tools for ensuring confidentiality

Protecting sensitive information within strategic information systems involves implementing a set of technological and procedural measures designed to prevent unauthorized access, interception, or compromise of data. These measures are integrated into a comprehensive security architecture that operates both at the level of the IT infrastructure and within organizational structures.

Data encryption is one of the most effective technological means of protecting confidentiality. Advanced cryptographic algorithms, such as the Advanced

Encryption Standard (AES), ensure the confidentiality of information both in transit and at rest, preventing access to its content in the absence of a valid key (NIST, 2001). In military environments, where data circulates through distributed and often vulnerable networks, encryption is accompanied by robust authentication protocols and digital signatures, which help validate the identity of users and the integrity of messages.

Another fundamental pillar of privacy protection is access control policies. These are governed by mechanisms such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), which ensure that access to information is granted according to the functional responsibilities and authorization level of each user. In strategic institutions, where the degree of classification of data is high, these mechanisms are complemented by Mandatory Access Control (MAC) policies, which impose rigid and hierarchical restrictions, in accordance with the legislation on classified information. In addition to technological components, procedural tools play an essential role in guaranteeing confidentiality. Systematic auditing of IT activities, real-time monitoring of data access, and analysis of user behavior contribute to the rapid identification of possible security breaches (Kent and Souppaya 2006). In parallel, continuous staff training, carried out through institutional awareness and training programs, aims to reduce the risks associated with human error, which remains one of the most frequent causes of compromising classified information.

Therefore, ensuring confidentiality is not limited to the implementation of high-performance technologies but requires integrated governance of information risk, in which processes, policies, and individual behaviors are in a relationship of strategic interdependence.

1.3. Risks associated with the disclosure or loss of classified data

Unauthorized disclosure or loss of classified information represents one of the most serious vulnerabilities in the architecture of strategic information systems, with direct implications for national security, geopolitical stability, and the operational capacity of military institutions. These incidents can compromise tactical plans, reveal technical capabilities, or affect strategic alliances and partnerships, generating a domino effect in decision-making and operational chains.

First of all, compromising classified information can lead to the loss of strategic advantage. In an operational environment where information asymmetry is decisive, adversaries' access to sensitive data can favor actions of anticipation, deterrence, or sabotage, which undermine the efficiency and safety of military missions. Cases documented in the specialized literature reveal that information leaks within defense institutions have repeatedly led to the reassessment of command structures, the temporary suspension of operations, and the diminution of inter-institutional trust.
Second, the loss of control over classified data severely affects international relations

and security cooperation. Strategic partners base their information exchange on the premise of mutual confidentiality and the existence of equivalent information protection measures. A breach in this system of trust can lead to the restriction of access to critical information, the suspension of collaborations, or the reassessment of the geopolitical position of the affected state.

From an institutional perspective, such incidents generate significant costs, both logistically and in terms of reputation. Reconfiguring the affected systems, initiating internal investigations, remedial measures, and additional investments in security involve the allocation of considerable budgetary resources. Moreover, in the context of public opinion, the loss of sensitive information can erode citizens' trust in the state's ability to protect its fundamental interests, fueling the perception of institutional vulnerability. To mitigate these risks, strategic organizations must adopt a proactive approach, based on ongoing risk assessments, penetration testing, incident simulations, and independent audits. These mechanisms must be supported by a coherent regulatory framework and an organizational culture oriented towards compliance, accountability, and information vigilance. Without these measures, the protection of classified data remains exposed to persistent, sophisticated, and systemic threats.

With the growth of strategic data and the rise of hybrid threats, protecting sensitive information can no longer be effectively achieved through traditional security and institutional control mechanisms. This article has argued that the ethical triad of confidentiality, loyalty, and accountability cannot be sustainably supported without the integration of emerging technologies, especially intelligent information systems (IIS).

These systems not only extend the technical capabilities of strategic organizations but also fundamentally transform the way information governance is understood and applied. With the ability to monitor user behavior in real time, generate predictive risk assessments, and support strategic decisions through recommendations that comply with ethical and legal standards, IISs become distributed accountability infrastructures. They provide additional guarantees for the integrity of processes and significantly reduce the risk of human error, abuse, or institutional negligence.

Another essential contribution of these technologies is to support an ethical organizational culture. Through traceability, impartiality in evaluation, and adaptability, SII contributes to strengthening the professional awareness of staff and to the internalization of institutional values. Thus, technology functions not only as a control tool, but as a mechanism for cultivating institutional ethics, in which responsibility is not imposed externally, but supported by infrastructure and decision-making process.

The integration of intelligent information systems into the architecture of strategic organizations must be seen not as a technological option, but as a strategic

necessity. They provide the premises for robust, compliant, proactive, and value-oriented governance. In an increasingly unstable information environment, where reaction time is critical and the costs of mistakes are irreversible, SII constitutes an indispensable support for ensuring security, legitimacy, and institutional resilience.

2. Institutional and individual responsibility in the governance of information systems

2.1. Normative frameworks and legal obligations regarding information protection (national laws, international treaties)

Responsibility in the field of information governance is closely correlated with compliance with a complex normative framework, which brings together national regulations, international directives, and multilateral treaties regarding the protection of classified data and critical infrastructures. In Romania, Law no. 182/2002 on the protection of classified information, together with the related methodological rules, establishes the obligations of public institutions and authorized personnel regarding the classification, handling, and storage of sensitive data. These provisions are harmonized with NATO and EU requirements regarding interoperability in the field of secured information.

At the international level, instruments such as the NATO Information Security Treaty and the General Data Protection Regulation (GDPR) – where the interaction also involves civilian or dual-use components – impose clear standards regarding confidentiality, traceability, and responsibility for information processing. Also, conventions such as the Budapest Convention on Cybercrime outline state obligations in preventing and combating illegal access to systems and data.

Compliance with these rules is not optional, but is part of the institutional responsibility to guarantee information security as an integral part of national security. This responsibility presupposes the existence of functional internal control structures, periodic auditing, and continuous updating of procedures in accordance with technological developments and emerging threats (Dragomir-Constantin 2025c).

2.2. Accountability mechanisms: traceability, auditing, criminal or disciplinary liability

In the context of information systems used by strategic organizations, responsibility cannot be reduced to a theoretical principle or an abstract value; it must be expressed concretely through a set of institutionalized mechanisms that allow both the prevention and remediation of incidents that affect the confidentiality of classified information. This responsibility is twofold: individual, in the sense of the assumption of decisions by each authorized user, and institutional, through the existence of structures and procedures that ensure the traceability of actions, the auditing of

systems, and the application of sanctions in case of misconduct. Traceability is the fundamental condition for any form of accountability. By implementing technical monitoring mechanisms, such as activity logging, cryptographic journaling systems, and behavioral analysis platforms, organizations can ensure continuous visibility of user interactions with critical systems. Thus, each access, modification, or transmission of data is recorded and associated with a digital identity, eliminating the premises of anonymity and reducing the risk of impunity (Dignum 2019). This system of tracking individual actions is indispensable for identifying the source of an incident, but also for establishing proportional responsibility.

Audit, as a formal tool for verifying compliance and efficiency, contributes to maintaining a transparent and predictable institutional climate. Periodic assessments of information security policies, carried out by internal or external entities, allow not only to correct deviations, but also to anticipate structural vulnerabilities. In military environments, audit has an additional strategic dimension: it validates the capacity of information systems to support operations under conditions of informational and cyber adversity (Kent and Souppaya 2006).

Disciplinary and legal sanctions complete this framework, ensuring a proportionate institutional response to violations of security norms. Without clear sanctioning mechanisms, responsibility becomes illusory, and the organization runs the risk of the norms being perceived as purely formal. The consistent application of measures – from withdrawal of access, to temporary or permanent suspension from office, to criminal prosecution in serious cases – contributes to the consolidation of an institutional culture based on compliance with regulations and awareness of the individual consequences of negligence or malicious intent (Metin, et al. 2024).

Thus, accountability in a strategic information ecosystem cannot function in the absence of a coherent framework of traceability, audit, and sanctioning. This institutional triad ensures not only operational resilience but also the internal and external legitimacy of the organization in the face of the challenges specific to the contemporary security environment.

Traceability is an essential functionality within the security architecture of strategic information systems, defining the system's ability to record, track, and correlate all actions carried out on information resources by authorized users. This function is not only a technical role, but also constitutes the foundation of individual and institutional accountability, providing evidentiary support for assessing user behavior and process compliance with policies and regulations in force. Operationally, traceability is achieved through a set of technologies and methods, such as detailed access logs, cryptographic journaling systems, and behavioral analysis modules, which allow the correlation of each action in the system with a unique digital identity. In high-security military and institutional environments, these systems are configured to operate in a non-repudiation regime, ensuring that

no relevant operation can be subsequently contested by the actor that generated it (Sulaiman, et al. 2022).

The importance of traceability is not limited to the post-incident investigative dimension, although this is vital for determining the causes and responsibilities in the event of information compromise. It plays a preventive and systemic role in the information risk governance process, allowing institutions to monitor user activity in real time, detect behavioral anomalies, and react promptly to violations or potential internal attacks. Thus, traceability contributes to strengthening operational response capacity and maintaining an organizational culture based on transparency and accountability. In addition, traceability is an essential condition for effective auditing of information systems. Especially in strategic organizations, logs must be protected against modification or deletion, as they can constitute legal evidence in disciplinary or criminal investigations. For this reason, military institutions implement solutions that ensure the integrity of logs through digital sealing mechanisms, temporal synchronization with external time sources, and replication in redundant systems, thus guaranteeing that any attempt to alter records is detectable and punishable.

Therefore, traceability is not only a technological component but a strategic dimension of the security architecture, integrated into the overall compliance, internal control, and information governance policies. Without a robust traceability mechanism, strategic institutions risk not only losing control over information resources but also diminishing the ability to react legitimately and effectively to internal misconduct or external attacks.

Auditing is one of the most important components of the institutional control mechanism in information security, with the role of assessing the compliance, efficiency, and robustness of processes, policies, and IT infrastructures. In strategic environments, auditing transcends the purely procedural dimension, becoming an essential tool for governance and risk anticipation, which contributes to strengthening organizational integrity and maintaining operational capacity in conditions of uncertainty or threat. Information security auditing is carried out on two interdependent levels: the technical and the procedural. The technical audit involves examining information systems from the perspective of security configurations, encryption levels, intrusion detection systems, as well as access and logging policies. The objective is to identify vulnerabilities that could be exploited by internal or external actors and assess the system's ability to withstand cyberattacks, including advanced persistent threats (APT). In military organizations, this type of audit is often complemented by penetration simulations ("red teaming"), in which specialized teams attempt to compromise systems in a controlled manner to highlight weaknesses in the defense.

On the other hand, procedural auditing focuses on how security policies and regulations are applied in practice. It analyzes the compatibility between operational

flows and regulatory requirements, the degree of compliance with protocols for accessing and handling classified information, and the level of training of personnel. Discrepancies between theoretical provisions and the actual behavior of institutional actors may signal communication deficiencies, the lack of an organizational culture focused on security, or even systemic risks generated by tolerance for deviations. An effective audit requires the independence of control structures, access to unfiltered data, and the ability to formulate operational recommendations, not just technical findings. It is also essential that the audit results are integrated into a continuous improvement cycle, in which recommendations are translated into concrete measures and their implementation is monitored with the same rigor.

In conclusion, auditing is not just a retrospective verification practice, but an active element of the information security system, designed to detect and correct vulnerabilities, validate measures, and strengthen individual and institutional responsibility. In the absence of a solid audit function anchored in the decision-making architecture of strategic organizations, control over information risks remains partial and reactive, which can compromise the resilience of the entire system.

Legal and disciplinary liability is the sanctioning dimension through which strategic organizations strengthen their control mechanisms and prevent non-compliant behaviors. In highly classified environments, such as military ones, individual responsibility for protecting classified information is not only a professional obligation but also a legal requirement, regulated by internal rules, national legislation, and international treaties on security and defense. Within military institutions, the sanctioning regime is complemented by internal regulations that include, in addition to temporary suspension or revocation of access to classified information, procedures for demotion or exclusion from the system. Criminal liability is activated when the compromise of information occurs through intentional acts, gross negligence, or culpable omissions. Such acts include the unauthorized transfer of data, unauthorized access to classified systems, loss of physical storage media, or failure to comply with operational procedures. In these cases, the competent authorities, including specialized structures of the Public Ministry or counterintelligence services, initiate investigations that may lead to the prosecution of the individuals involved (Metin, et al. 2024). Disciplinary liability, although distinct from criminal liability, plays a complementary role, with the objective of maintaining internal order and compliance with organizational norms. This can be applied even in situations where the act does not meet the constitutive elements of a crime, but reflects unacceptable conduct from the perspective of job obligations. Sanctions can range from written warnings and temporary salary reductions to dismissal from office or exclusion from security structures, depending on the seriousness of the violation and the position occupied by the person in question.

In strategic environments, the effectiveness of these forms of liability depends on three factors: the clarity of the rules, the consistency of application, and the

transparency of the procedures. The lack of a well-defined regulatory framework or the selective application of sanctions can lead to the erosion of the organizational culture based on ethics and responsibility. In contrast, a firm but fair liability regime contributes to strengthening internal trust, preventing information risks, and protecting the integrity of classified systems.

Thus, legal and disciplinary liability must be understood as an essential link in the information security ecosystem, through which individual behavior is correlated with institutional norms, and protecting sensitive information becomes an act of compliance, loyalty, and respect for the national interest.

3. Contributions of Intelligent Information Systems in Strengthening Organizational Responsibility and Ethics

In the era of accelerated digital transformation and intensification of hybrid threats, Intelligent Information Systems (IIS) have become essential elements in the architecture of strategic organizations, redefining the paradigms of governance, security, and decision-making. These systems, based on artificial intelligence (AI), machine learning (ML), predictive analytics, and cognitive automation processes, extend the functionalities of traditional information infrastructure, offering an increased capacity for adaptation and anticipation in volatile operational environments (Dignum 2019; Xu, et al. 2024).

In particular, IIS allows the modernization of decision-making processes by reducing uncertainty and increasing the speed of reaction to information threats. Machine learning algorithms can analyze massive volumes of data in real time, identifying relevant patterns, anomalies, and weak signals that could indicate a security breach or deviant behavior by an internal user. This early detection capability, combined with automated response mechanisms, directly contributes to strengthening information resilience and preventing incidents with systemic impact (Grigaliunas, et al. 2024). Furthermore, intelligent systems facilitate proactive governance of information risks by generating predictive models and decision-making recommendations based on probabilistic threat assessment. These tools not only support tactical security processes but also allow for the alignment of operational decisions with pre-established ethical and legal standards. Thus, SIIs become ethical support tools in environments where rapid decisions must be compatible with national and international regulations on data protection and fundamental rights (Dignum, 2019; Tounsi and Rais 2021).

A key element that differentiates intelligent information systems (IIS) from classic security infrastructures is their ability to facilitate proactive governance of information risks, based on anticipation, adaptation, and regulatory compliance. This proactive approach involves moving beyond the reactive paradigm, in which

security measures are implemented post-factum, and moving to a predictive model, in which threats are identified, assessed, and neutralized before they materialize. IIS integrates machine learning algorithms and artificial intelligence models that process large volumes of data from heterogeneous sources – including system logs, communication flows, behavioral profiles, and threat indicators – to generate probabilistic assessments of emerging risks. Through these capabilities, systems can detect weak signals and correlate seemingly isolated events, identifying patterns that indicate abnormal, potentially dangerous activities before they become manifest (Tounsi and Rais 2021). This type of predictive analysis gives decision-makers a significant time advantage, allowing them to adopt preventive, not just corrective, security measures.

In addition to the technical dimension, SII also contributes to supporting a coherent ethical and legal decision-making framework. In strategic organizations, where decisions often have to be made under pressure and uncertainty, intelligent tools provide objective analytical support, reducing the risk of arbitrary or non-compliant decisions. For example, by integrating ethical rules or data protection compliance criteria, systems can assess decision-making options not only from the point of view of operational efficiency, but also from the point of view of compliance with legal norms and principles of law (Dignum 2019).

This "automated ethical assistance" function becomes crucial in sensitive areas, such as national defense, cybersecurity, or the protection of critical infrastructures, where decisions can simultaneously involve technical, human, and political consequences. SII can recommend options that minimize collateral risks, protect personal data, or respect fundamental rights, even in operational contexts where such dimensions are easy to neglect. Thus, these systems not only optimize the response to threats but also institutionalize a framework of distributed ethical responsibility, in which normative principles are incorporated into the algorithmic logic of action. In this sense, the role of SII transcends the function of technological support, becoming an integral part of a responsible decision-making mechanism, capable of integrating security, legality, and ethical criteria in real time. In a complex and hyperconnected information ecosystem, in which the boundaries between the operational and the normative are increasingly fluid, this ability to support decisions compatible simultaneously with the imperative of efficiency and with moral and legal requirements represents a major strategic advantage.

Another essential benefit of SII consists of supporting an ethical organizational culture. By continuously and impartially monitoring user interactions with information systems, these technologies provide a framework of distributed responsibility, in which each actor is aware that their actions are subject to an objective regime of evaluation and traceability. In this sense, technology functions not only as a data guardian but also as a moral compliance mechanism, reducing the space for deviations or opportunistic behaviors (Xu, et al. 2024).

In conclusion, intelligent information systems contribute to the modernization of security architectures and the professionalization of strategic decisions, providing indispensable technological support for achieving a sustainable balance between operational efficiency, accountability, and institutional ethics. In an environment where reaction time is critical and human errors can have irreversible consequences, the integration of SII is no longer an option, but a strategic necessity for organizations that manage classified information and critical resources.

One of the most relevant benefits of intelligent information systems (SII) within strategic organizations lies in their ability to support and strengthen an ethical organizational culture, in which behavioral norms, institutional values, and individual responsibility are continuously promoted, verified, and reinforced through transparent and impartial technological mechanisms. Unlike traditional compliance models, which are predominantly based on hierarchical supervision and periodic audits, SII offers the possibility of constant, scalable, and neutral monitoring of interactions between users and critical information resources. By automatically collecting and analyzing data on user activity, including file access, configuration changes, communication through internal channels, or activity outside of work hours, these systems can build behavioral profiles that allow the detection of significant deviations from institutional norms. This form of monitoring does not aim at repressive control, but rather at cultivating an environment in which organizational actors become aware that each action is subject to a form of objective evaluation, unmediated by subjective perceptions or interests (Xu, et al. 2024).

In this configuration, technology becomes a catalyst for individual responsibility, contributing to the internalization of ethical norms by users. The awareness that professional activity is visible and traceable not only discourages opportunistic behaviors but also encourages the adoption of compliant practices, in which compliance with policies is no longer perceived as an external obligation but as a norm integrated into the individual's professional identity. This distributed responsibility, supported by impartial and automated systems, has the advantage of reducing the room for maneuver for destructive actions, while strengthening trust in institutional control mechanisms.

Furthermore, SII can contribute to the development of an organizational climate in which moral compliance is not just a result of fear of sanction, but of understanding and assimilation of institutional values. By analyzing collective and individual behaviors, systems can generate useful information about dominant patterns, the organization's ethical vulnerabilities, and the need for training or cultural adjustment interventions. This type of analytical feedback allows decision-makers to adopt proactive organizational ethics policies, based on data, and not just on assumptions or reactive incidents (Tounsi and Rais 2018).
Through advanced capabilities for predictive analysis, anomaly detection, reaction automation, and decision assistance, SII provides operational support that goes

beyond the technical sphere and penetrates the normative and organizational dimensions of security. Thus, decisions are no longer made solely based on intuition or individual experience, but are supported by data, correlated with scenarios, assessed according to risks, and filtered through ethical and legal constraints. This recalibration of the decision-making process allows not only to minimize human errors, but also to strengthen legitimacy and transparency within strategic institutions (Dignum 2019).

In the contemporary operational context, in which reaction time is compressed and the pressure on institutional leaders is constant, rapid but compliant decisions become an imperative. In this equation, SII offers a competitive advantage through its ability to provide information in real time, learn from previous incidents, and generate adaptive solutions in the face of dynamic threats (Tounsi and Rais 2018). Moreover, by promoting an organizational culture based on transparency, traceability, and distributed ethics, these systems support the development of an agile institution, capable of operating in volatile environments without compromising its fundamental values. In this sense, the role of SII is not limited to a security tool, but extends to the status of critical infrastructure for responsible decision-making, strategic governance, and organizational resilience.

Therefore, in institutional environments that manage classified information, critical infrastructures, or national strategic stakes, the implementation of intelligent information systems can no longer be considered a luxury or an optional choice. It represents an imperative necessity for strengthening security, optimizing decisions, and ensuring institutional conduct in line with international standards of ethics, legality, and performance.

Conclusions

With the growth of strategic data and the rise of hybrid threats, protecting sensitive information can no longer be effectively achieved through traditional security and institutional control mechanisms. This article has argued that the ethical triad of confidentiality, loyalty, and accountability cannot be sustainably supported without the integration of emerging technologies, especially intelligent information systems (IIS).

These systems not only extend the technical capabilities of strategic organizations but also fundamentally transform the way information governance is understood and applied. With the ability to monitor user behavior in real time, generate predictive risk assessments, and support strategic decisions through recommendations that comply with ethical and legal standards, IISs become distributed accountability infrastructures. They provide additional guarantees for the integrity of processes and significantly reduce the risk of human error, abuse, or institutional negligence.

Another essential contribution of these technologies is to support an ethical organizational culture. Through traceability, impartiality in evaluation, and adaptability, SII contributes to strengthening the professional awareness of staff and the internalization of institutional values. Thus, technology functions not only as a control tool, but as a mechanism for cultivating institutional ethics, in which responsibility is not imposed externally, but supported by infrastructure and decision-making process.

The integration of intelligent information systems into the architecture of strategic organizations must be seen not as a technological option, but as a strategic necessity. They provide the premises for robust, compliant, proactive, and value-oriented governance. In an increasingly unstable information environment, where reaction time is critical and the costs of mistakes are irreversible, SII constitutes an indispensable support for ensuring security, legitimacy, and institutional resilience.

References

Almomani, Iman, Aala Alkhayer, and Walid El-Shafai. 2023. "E2E-RDS: Efficient End-to-End Ransomware Detection System Based on Static-Based ML and Vision-Based DL Approaches" Sensors 23 (9): 4467. https://doi.org/10.3390/s23094467

Bell, David Elliott, and Leonard LaPadula. 1973. "Secure Computer Systems: Mathematical Foundations. Technical Report MTR-2547", Vol. I. Bedford, MA: The MITRE Corporation. https://websites.umich.edu/~cja/LPS12b/refs/belllapadula1.pdf

Dignum, Virginia. 2019. "Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way". Springer. https://link.springer.com/book/10.1007/978-3-030-30371-6

Dragomir, Florentina-Loredana, and Gelu Alexandrescu. 2017a. "Applications of Artificial Intelligence in Decision-Making Process". Bulletin of Carol I National Defense University 4(2): 56–61. https://cssas.unap.ro/en/pdf_periodicals/si63.pdf

___. 2017b. "The Axiomatic Character of Decision". Bulletin of "Carol I" National Defense University 6 (1): 16–22. https://www.ceeol.com/search/article-detail?id=548274

Dragomir, Florentina-Loredana., Gelu Alexandrescu, and Florin Postolache. 2018" Tools for hierarchical security ". The 14 the International Scientific Conference "eLearning and Software for Education", Bucharest, Carol I" National Defence University, April 19 - 20, Advanced Distributed Learning Association, vol. 4, pp. 34–38.

Dragomir-Constantin, Florentina-Loredana. 2025a. "Information System for Macroprudential Policies. "Acta Universitatis Danubius. Œconomica 21 (1): 48–57. https://dj.univ-danubius.ro/index.php/AUDOE/article/view/3254

___. 2025b. "Thinking Patterns in Decision-Making in Information Systems". New Trends in Psychology 7 (1): 89–98. https://dj.univ-danubius.ro/index.php/NTP/article/view/3255

___. 2025c. "Thinking Traps: How High-Performance Information Systems Correct Cognitive Biases in Decision-Making". New Trends in Psychology 7 (1) 99–108. https://dj.univ-danubius.ro/index.php/NTP/article/view/3257.

Grigaliūnas, Šarūnas, Michael Schmidt, Rita Brūzgienė, and Smyrli Panagiota. 2024. "Holistic Information Security Management and Compliance Framework". Kaunas University of Technology. https://epubl.ktu.edu/object/elaba:209322117/

Kent, Karen, and Murugiah Souppaya. 2006. "Guide to Computer Security Log Management. NIST Special Publication 800-92. National Institute of Standards and Technology". https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-92.pdf

Metin, Bilgin, Fatma Gözde Özhan, and Martin Wynn. 2024. "Digitalisation and Cybersecurity: Towards an Operational Framework." Electronics 13 (21): 4226. https://www.mdpi.com/2079-9292/13/21/4226

Sulaiman, Nur Shafinas, Mohd Azlan Fauzi, Wendy Wider, and Jasmine Rajadurai. 2022. "Cyber–Information Security Compliance and Violation Behaviour in Organisations: A Systematic Review." Social Sciences 11 (9): 386. https://www.mdpi.com/2076-0760/11/9/386

Tache, Florentina-Loredana, Postolache Florin, Nachila Cătălin, and Ivan Maria Alexandra. 2010." Consulting in Electronic Commerce." Acta Universitatis Danubius. Œconomica 6 (3): 162–169. https://journals.univ-danubius.ro/index.php/oeconomica/article/view/707

Tounsi, Wassim, and Hassen Rais. 2018. "A Survey on Technical Threat Intelligence in the Age of Sophisticated Cyber Attack". Computers & Security 72. https://www.sciencedirect.com/science/article/abs/pii/S0167404817301839?via%3Dihub

Xu, Yao, Jixin Wei, Ting Mi, and Zhihua Chen. 2024 "Data Security in Autonomous Driving: Multifaceted Challenges of Technology, Law, and Social Ethics." World Electric Vehicle Journal 16 (1): 6. https://doi.org/10.3390/wevj16010006