Edición
12
ISSN: 2953-769X

FUTURO INNOVADOR
UNA MIRADA TRANSFORMADORA

REVISTA SEMESTRAL

Somos esencial® COSTA RICA

RAI | Universidad San Marcos
Revista Académica Institucional

San Marcos

ACADEMIA

En esta sección podrás encontrar artículos académicos y artículos científicos de la comunidad universitaria en general, los cuales son originales, y describe resultados experimentales, nuevos conocimientos o experiencias basadas en hechos conocidos de sus autores.

Universidad San Marcos
Revista Académica Institucional
Edición 12, Volumen 7 ISSN: 2953-769X pp. 29- 46 Enero - Junio, 2025

CRITICAL ANALYSIS OF THE MEP CYBERSECURITY POLICY: CHALLENGES AND OPPORTUNITIES FOR ITS OPTIMIZATION

[1] ***Mtr. Ricardo Aguirre Morice,*** *ricardoaguirremorice@hotmail.com*
Ministry of Public Education, Costa Rica. Computer Science Engineering Information Security. Cybersecurity
Código ORCID: *https://orcid.org/0009-0002-5309-9297*

DOI: *https://doi.org/10.64183/facx2f86*

Received: ***October 2024***
Accepted: ***January 2025***

Abstract. This article evaluates the Cybersecurity Policy of Costa Rica's Ministry of Public Education (MEP) in relation to international standards such as ISO 27001 and NIST SF. Strengths were identified in its alignment with national regulations, but also gaps in critical areas such as training, incident management, and business continuity. Through a comparative and methodological approach, an improvement plan is proposed to ensure the confidentiality, integrity, and availability of institutional information.

Keywords. Cybersecurity, Educational Policies, ISO 27001.

ANÁLISIS CRÍTICO DE LA POLÍTICA DE CIBERSEGURIDAD DEL MEP: RETOS Y OPORTUNIDADES PARA SU OPTIMIZACIÓN

[1] ***Mtr. Ricardo Aguirre Morice,*** *ricardoaguirremorice@hotmail.com*

Recibido: ***Octubre 2024***
Aceptado: ***Enero 2025***

Resumen. Este artículo evalúa la Política de Ciberseguridad del Ministerio de Educación Pública de Costa Rica (MEP) en relación con estándares internacionales como ISO 27001 y NIST CSF. Se identificaron fortalezas en su alineación con normativas nacionales, pero también brechas en áreas críticas como capacitación, gestión de incidentes y continuidad del negocio. A través de un enfoque comparativo y metodológico, se propone un plan de mejoras para garantizar la confidencialidad, integridad y disponibilidad de la información institucional.

Palabras Clave. Ciberseguridad, Políticas Educativas, ISO 27001.

1. INTRODUCTION

The Ministry of Public Education (MEP) of Costa Rica covers a substantial area when accounted for, employing around 88,000 public servants, which includes the entire MEP staff.

These employees are distributed across central offices, including the Minister's office, twenty-seven separate regional offices throughout the national territory, approximately 206 school circuits, and about 4,825 educational centers (MEP, 2019). From this, it can be inferred that it is an organization with a significant exposure surface and a large volume of data handling.

This is without even considering the student population; once this data is incorporated, according to Sibaja in 2023, the population was 1,123,964 (2024). With this information, it can be extrapolated that the MEP holds 24.03% of the country's total personal data, encompassing both officials and students, almost a quarter of the country's total population, stored in the services offered by this institution.

This does not even account for the historical records it possesses, which is a vast amount of information for a single organization, equivalent to a gold mine of data waiting to be exploited by someone who knows how to leverage this information.

Based on the data presented previously, the quantification of the potential held by the Ministry of Public Education (MEP) is justified, as is, simultaneously, the analysis of the inherent risk it faces from a strategic perspective.

Costa Rica, as a country with a public and compulsory education system at primary and secondary levels, ensures that all citizens, at some point in their lives, pass through this institution via its various decentralized units. These characteristic positions national education as a critical infrastructure, given its fundamental role in citizen formation and its exposure to security risks.

The MEP, by managing sensitive personal information of both minors and public fund administrators, as well as officials working in the institution, faces significant risks in terms of data breaches. This scenario makes the organization a potential target of interest for malicious actors.

Therefore, it is considered imperative to integrate elements of cybersecurity, cyber intelligence, and information security into the primary structure of the MEP, not only as a protective measure but also as a strategic approach that strengthens the institution's resilience against potential threats. This integration seeks to mitigate risks and ensure operational continuity, highlighting the relevance of including these elements as part of national critical infrastructure protection policies and strategies.

Objective

To evaluate the Cybersecurity Policy of the Ministry of Public Education (MEP) and propose a structured modification that optimizes data protection and strengthens its capacity against cyber threats.

Background

According to Moreno, "education is a right of individuals throughout their lives, and it is the state's responsibility to ensure digital literacy and the use of information and communication technologies in the educational process" (2019). As the author comments, education is the cornerstone of many nations, and the main element that generates this education is security. But what security does the government provide to institutions? Clearly, legal and physical security, by installing fences, perimeter fences, and trained personnel to safeguard the integrity of attendees.

This can be defined as security, which can be indicated as "the set of methods that promote a safe and protected environment that allows people to carry out their daily activities" (Purpura, 2006, p. 20). From the description mentioned above, it can be understood that one of the fundamental pillars for a society that tries to develop a daily life requires a level or degree of security.

This is corroborated by the humanist philosopher Maslow when he formulated his theory of human motivation, in which he places the need for safety and security in the second position (Figure 1, Maslow's Hierarchy of Needs, self-made).

He states that human beings must build from the base of the pyramid until they reach a point of full growth or enlightenment. Therefore, if we focus on dealing with an educational institution that houses people in training within its programs, and hundreds of people who strive for that objective, everyone must ensure their safety, and not only in the traditional way. This security must also extend to the digital world, which has been massively adopted since the end of the last century thanks to the use and penetration of the internet, accelerating even more in ten-year intervals.

Now, after the global COVID-19 pandemic, the world is immersed in a greater interconnectedness and dependence on the technological world, which creates a greater exposure to its inherent dangers.

2. MATERIALS AND METHODS

Technology in modern life has significantly increased information security risks. Cyberattacks, such as data theft, ransomware, and phishing, have become constant threats that seek to exploit vulnerabilities in systems and networks to gain unauthorized access to sensitive information.

The expansion of the Internet of Things (IoT) has exacerbated this problem, as connected devices, often unprotected or poorly configured, offer new access points for attackers. Furthermore, the increasing reliance on cloud services and digital storage has exposed companies and individuals to security failures derived from unauthorized access and incorrect configurations.

Information security also faces a critical challenge related to the human factor, which remains one of the main vulnerabilities. Lack of awareness about secure practices, use of weak passwords, and susceptibility to social engineering techniques are recurring problems that facilitate the exploitation of sensitive data.

On the other hand, the massive amount of personal information stored on digital platforms has generated growing concerns about privacy, including the risk of unauthorized tracking, data misuse, and its sale without consent. Together, these problems have exposed both individuals and organizations to increasingly complex scenarios in the field of digital security.

For all the above reasons, an additional layer of protection or security must be added to existing ones, and Maslow's pyramid must be updated, by providing the critical infrastructure of the educational system with a layer of protection for the data of citizens who use this service. This security is essential to train the nation's future citizens, but why is it necessary to protect data in the current world?

The creation of an information security culture in society and educational environments is essential due to the central role technology plays in daily life and the emerging risks in catastrophic or futuristic scenarios.

In a context where personal information is digitized and identity can be manipulated or even stolen, threats arise such as the improper granting of one person's identity to another or to a digital human, which could lead to unauthorized access to critical resources, erroneous legal decisions, or even the total impersonation of a digital existence. In the educational field, where student and teacher data represent a vulnerable target, the lack of security measures amplifies the risk of these threats, leaving open the possibility that an educational identity could be cloned or reused for malicious purposes, such as academic fraud or access to restricted resources.

An information security culture is also vital to prevent the misuse of digital identities and ensure the integrity of data in an increasingly technology-dependent society. Without solid training in secure practices, people are more susceptible to becoming victims of sophisticated attacks that could usurp their identity not only on social networks or financial systems, but also in advanced digital environments where digital humans could

simulate behaviors, voices, or decisions of a real individual.

This risk raises profound ethical and legal implications, as a compromised identity in a hyperconnected digital world can be used to manipulate systems, commit crimes, or alter personal and social realities. Therefore, integrating cybersecurity education from an early age not only fosters a more conscious and prepared society but also strengthens the ability to anticipate and respond to critical scenarios where the consequences of a compromised identity can be irreversible.

It is at this point that the process of understanding some terms should begin to establish the context in which work should be carried out beforehand. Purpura indicates that prevention is "methods of reducing the chances of a loss occurring and also the associated expenses" (2006, p. 21). From the foregoing, it can be inferred that prevention is a strategy that helps to reduce the possible adverse effects of an unwanted event, and at the same time, the concept of loss prevention is introduced. Purpura himself indicates that it is "a broader range of methods to protect people and property" (2006, p. 20). This range of possibilities brings together essential elements such as strategy, which can be replicated methodically to obtain the same result regardless of where it is applied, since the purpose is to safeguard the assets or people that are to be protected. It is at this juncture that international information security frameworks emerge.

3. DISCUSSION

ISO 27001 and 27002 ISO/IEC 27001 and ISO/IEC 27002 standards represent fundamental pillars in enterprise information security management. ISO 27001 establishes a comprehensive framework for implementing an Information Security Management System (ISMS), being a certifiable standard that defines the essential requirements for effectively managing IT security in any organization. Its counterpart, ISO 27002, acts as a detailed complementary guide, providing specific guidelines and best practices for the effective implementation of security controls.

The importance of these standards is manifested in multiple critical aspects for organizations. First, they provide robust protection against data breaches and cyberattacks through a systematic approach to risk management. Furthermore, they facilitate compliance with various legal regulations such as GDPR, HIPAA, and PCI-DSS, which is fundamental in the current regulatory environment.

Organizations that obtain ISO 27001 certification not only demonstrate a serious commitment to information security but also gain a significant competitive advantage by generating greater trust among customers and

business partners.

The structure of these standards is meticulously organized into four main categories of controls. Organizational controls, comprising 37 elements, cover crucial aspects such as establishing security policies, defining roles and responsibilities, systematically assessing risks, and ensuring legal compliance. People controls, with 8 elements, focus on fundamental aspects such as security awareness, staff training, and implementing access management based on clearly defined roles. Physical controls, totaling 14 elements, focus on the tangible protection of infrastructure, including security in facility access, protection of equipment and assets, and proper management of waste and storage media.

For their part, technological controls, with 34 elements, constitute a crucial layer covering malware protection, implementation of network and communications security, data encryption, and effective vulnerability management.

The implementation of these standards follows a structured and methodical process based on the ISMS lifecycle, which begins with a clear definition of scope and objectives. This initial phase involves the precise identification of the processes, assets, and systems that will be under the protection of the ISMS, as well as the establishment of measurable and achievable objectives. The next crucial phase involves an exhaustive risk assessment, where information assets are identified and classified, potential threats and vulnerabilities are evaluated, and specific controls are implemented to mitigate the identified risks. The security control implementation phase requires the development of detailed policies and procedures, the establishment of a competent incident response team, and the application of technical protection measures such as advanced encryption, backup systems, and robust access controls. This entire process is complemented by a rigorous regime of internal audits and a commitment to continuous improvement, which includes conducting periodic evaluations to verify compliance and implementing corrective actions when necessary. Among the specific implementation measures, access control based on the principle of least privilege, multifactor authentication, the implementation of firewalls and intrusion detection systems, and data protection using AES-256 encryption stand out.

Furthermore, the importance of maintaining continuous information security training programs for employees and implementing specific security measures for cloud environments, including protection on platforms such as AWS, Azure, and Google Cloud, is emphasized.

Application of ISO/IEC 27001 and ISO/IEC 27002 in Educational Centers and Central

Offices of an Educational Organization The adoption of ISO/IEC 27001 and ISO/IEC 27002 standards in educational environments and central offices of an educational organization establishes a structured security framework for the protection of academic, administrative, and personal information of students, teachers, and administrative staff. This implementation responds to the need to guarantee the integrity, confidentiality, and availability of information, especially in a context where educational digitalization and the use of cloud platforms are predominant.

Implementation in Educational Centers In educational centers, the application of an Information Security Management System (ISMS) based on ISO/IEC 27001 focuses on protecting student and teacher data, as well as the security of digital educational systems. The main measures to be implemented include:

Organizational Controls: Define security policies for handling sensitive information such as grades, medical records, and students' personal data. Establish protocols for cybersecurity incident management, defining roles and responsibilities within teaching and administrative staff. Implement a cybersecurity training program for teachers and students, fostering a data protection culture from an early age.

People Controls: Regularly train teachers and students on phishing, social engineering, and good digital security practices. Manage access to educational platforms and databases using multifactor authentication (MFA) and role-based privileges.

Physical Controls: Ensure that devices in computer labs and virtual classrooms have restricted access measures to prevent unauthorized use. Implement security measures in institutional Wi-Fi networks to prevent unauthorized access and man-in-the-middle (MITM) attacks.

Technological Controls: Apply encryption mechanisms in academic databases to protect sensitive information. Implement firewalls and intrusion detection systems to prevent unauthorized access to the institutional network. Ensure that devices connected to the educational network are protected against malware and vulnerabilities.

Implementation in Central Offices of the Educational Organization Central offices have a more administrative and strategic focus, requiring stricter controls for the protection of institutional information. The application of the ISMS in this environment includes:

Organizational Controls: Implement security policies for data management on platforms such as ERP, LMS, and payroll systems. Comply with data protection laws such as GDPR or local regulations to avoid legal penalties. Establish a security committee to oversee ISMS compliance and continuous

system improvement.

People Controls: Apply cybersecurity awareness programs for administrative staff, focused on protection against fraud and information leaks. Define access policies for sensitive administrative documents, ensuring that only authorized personnel can consult them.

Physical Controls: Implement security measures in servers and data centers to prevent unauthorized access. Use video surveillance systems and access control with biometric credentials.

Technological Controls: Apply AES-256 encryption to critical documents such as contracts, financial records, and strategic plans. Conduct periodic security audits to identify and correct vulnerabilities in the digital infrastructure.

NIST National Institute of Standards and Technology. This is an organization belonging to the United States Department of Commerce that is responsible for developing standards, guidelines, and best practices. In this specific case, NIST 800-53, which explains security controls for information systems, and NIST 800-30 should be applied.

The analysis will first focus on NIST 800-53. The adapted application of the elements of this standard for a robust security policy requires a detailed approach. We begin with Risk Management, where the implementation of the Risk Management Framework (RMF) is recommended, promoting a systematic approach to evaluating and mitigating threats. This framework includes Risk Assessment (RA), focused on identifying critical assets and analyzing associated vulnerabilities.

Regarding Key Security Controls, NIST 800-53 proposes 20 control families, highlighting some for an effective security policy: **Access Control (AC):** Multi-factor authentication (MFA) must be implemented wherever the organization requires authentication, and its use must be mandatory.

Privileges and role-based access must be controlled, and access to critical information must be supervised and audited to ensure that only authorized users have the necessary access. **Identity and Authentication Management (IA):** Here, the use of strong passwords and robust authentication is essential, as is the implementation of a public key infrastructure (PKI) and the restriction of access to unauthorized users, especially in central or regional offices.

Monitoring, Auditing, and Accountability (AU): It is crucial to log and audit critical security events, implement a security information and event management (SIEM) system for immediate incident response, and ensure timely notification and mitigation.

The institution's structure necessitates segmentation by region, allowing for

auditable control and simultaneous event control. This requires establishing regional surveillance positions or a national network of regional offices to enable centralized surveillance.

System and Information Integrity Protection (SI): The use of anti-malware solutions, prevention of malicious code execution, monitoring the integrity of critical files, and network segmentation to reduce the potential impact of attacks are recommended.

This section clearly demonstrates the urgent need for organizational homogenization through a software usage policy that allows for standardization of its use and coordination for the prevention or eradication of possible threats. Incident Response (IR): It is fundamental to develop an Incident Response Plan, conduct regular tests through simulations, and ensure effective communication and rapid recovery of affected systems.

This point is crucial for training and capacitating officials nationwide on how to react and communicate appropriately in the face of an adverse event. This is especially critical since a large part of cybersecurity events must be handled by MICITT. Supply Chain Security (SR): Evaluating providers and third parties from a security perspective, implementing controls for data protection in the supply chain, and verifying software and hardware to avoid backdoor attacks are essential steps. At this point, the application processes of Law 8968 must be strengthened to improve the protection of internal and external clients, thus preventing additional information leakage.

Additionally, the supply chain must be protected, especially given that the MEP acquires multiple services from providers. The first thing that must be done is for all administrative boards or public fund managers to comply with Law 9986 on Public Procurement. Data and Privacy Protection (PT): Applying encryption for data both at rest and in transit, using controls to minimize the exposure of personal data, and implementing privacy measures by design protect the confidentiality and integrity of information.

A very deep awareness of the importance of Law 8968 and the processing of personal data must be generated, especially in the management of personnel files, appropriate use of financial information to provide students with school meals, medical information, curricular adaptations, high endowment. In addition, it must be standardized through a unanimous agreement that every device acquired must have encryption by default from the moment of purchase, as well as models that allow native encryption and biometrics from the moment of acquisition.

For Implementation in a Security Policy, access rules must be established by defining

roles and permissions according to security levels, an incident response plan with clear procedures must be developed, cybersecurity training must be offered to raise awareness and train personnel, and continuous monitoring and auditing must be maintained to review logs, data access, and detect anomalies. Finally, supplier management must ensure that all third parties comply with established security standards.

The other important element is risk analysis, which is where NIST 800-30 comes into play. However, Costa Rica has National Emergency and Risk Prevention Law No. 8488, but there is a series of additional regulations that will be taken into account to homogenize the criteria to generate a single line of thought regarding a secure environment in the digital age.

Information security in educational centers and administrative offices constitutes a fundamental pillar to guarantee the integrity, confidentiality, and availability of data. The NIST 800-30 document establishes a solid framework for risk assessment in information systems, allowing for the implementation of effective controls to prevent cybersecurity incidents. Furthermore, key documents such as the National Risk Management Policy 2016-2030, the National Risk Management Plan 2021-2025, and the Disaster Risk Management Strategy in the Education Sector 2022-2026 highlight the importance of strengthening digital resilience in educational institutions and administrative offices. The main elements to be applied in information security and cybersecurity in educational environments are presented, guaranteeing data protection, service continuity, and the formation of a digital security culture.

a) Risk Management in Information Security NIST 800-30 emphasizes the importance of risk management as the starting point for any cybersecurity strategy. In the educational and administrative sphere, this implies: Identification of critical assets: Learning Management Systems (LMS), student and teacher databases, internal and external communication platforms, document servers, and institutional networks. Threat analysis: From phishing and malware attacks to identity theft and unauthorized access to sensitive data. Vulnerability assessment: Outdated infrastructures, weak passwords, lack of network segmentation, and absence of multifactor authentication. Determination of potential impact: A cyberattack can compromise academic records, expose personal data, and paralyze essential administrative systems. Mitigation strategies: Implementation of encryption, regular backups, and real-time threat monitoring.

b) Critical Infrastructure Protection in Educational Environments Educational centers and administrative offices handle

large volumes of sensitive information, making a secure and resilient technological infrastructure essential. To this end, it is recommended to: Network segmentation: Separate academic, administrative, and public access networks to prevent unauthorized intrusions. Data encryption: Protect databases with robust encryption algorithms to safeguard confidential information. Use of firewalls and intrusion prevention/detection systems (IPS/IDS): Control and monitor network traffic to detect and block suspicious activities. Multifactor authentication (MFA): Reinforce access to digital platforms through additional credentials. System updates and patching: Keep software and hardware updated to prevent the exploitation of vulnerabilities.

c) Cybersecurity Awareness and Training One of the weakest links in information security is the human factor. It is fundamental to foster a cybersecurity culture in the educational and administrative community through: Regular training: Raise awareness among teachers, students, and administrative staff about threats such as phishing, social engineering, and malware. Responsible device and network use policies: Establish regulations for the appropriate use of personal devices in institutional environments. Attack simulation exercises: Conduct phishing tests and incident response exercises to evaluate user preparedness. Access and permission management: Apply the principle of least privilege, limiting access to sensitive information only to authorized users.

d) Business Continuity and Incident Response Plans Risk management documents in Costa Rica, such as the National Risk Management Plan 2021-2025, emphasize the need for response and recovery strategies for information security incidents. To this end, the following must be established: Incident response plans: Clear procedures to identify, contain, eradicate, and recover systems affected by cyberattacks. Periodic backups: Implementation of backups on physical and cloud servers with well-defined recovery policies. Security Operations Centers (SOC): Real-time monitoring of cybersecurity events to proactively detect and mitigate attacks. Cyberattack and technological disaster drills: Evaluate the institution's response capacity to critical events.

Analysis: MEP Cybersecurity Policy

This process aims to generate debate and awareness of weak or missing elements in the MEP's cybersecurity and information security policy. To make it easier to understand and gather information, the information was condensed as follows:

Table 1. *MEP Cybersecurity Policy.*

Category	Weakness or Inconsistency	Potential Impact
Technical Inconsistencies	Lack of specificity in the implementation of technical measures	Ineffective implementations that leave open vulnerabilities
Technical Inconsistencies	Absence of a risk-based approach	No clear method for evaluating and mitigating threats
Technical Inconsistencies	Does not integrate with international standards such as ISO 27001 or NIST	Lack of alignment with global standards, reducing effectiveness
Technical Inconsistencies	Optional multifactor authentication (MFA) instead of mandatory	Increased risk of unauthorized access to critical systems
Technical Inconsistencies	End-to-end encryption for communications and storage is not mentioned	Greater exposure to interception and data theft attacks
Management and Compliance	No clear sanctions specified in case of non-compliance	Lack of deterrence and deficient policy compliance
Management and Compliance	Lack of continuous monitoring and real-time incident response	Threats may not be detected in time, increasing damage
Management and Compliance	No mechanisms for auditing and compliance control are detailed	Lack of effective supervision to verify compliance
Management and Compliance	No business continuity or disaster recovery plan	Institution vulnerable to prolonged interruptions due to attacks
Management and Compliance	Lack of strict security requirements in third-party contracting	Providers can represent an entry point for attacks
Operational and Educational	Insufficient cybersecurity training for officials	Poorly prepared users can be the weak link in security
Operational and Educational	No concrete strategies against social engineering attacks (phishing)	Greater exposure to fraud and deception aimed at officials
Operational and Educational	No clear controls established for the use of personal devices (BYOD)	Risk of data leakage due to lack of control over external devices
Operational and Educational	Ambiguous definition of responsibilities among different MEP departments	Difficulty in applying the policy due to lack of clarity in roles
Operational and Educational	No process for periodic policy updates is established	Risk of the policy becoming obsolete in the face of new threats

Source of own elaboration (2025)

Based on the above, it can be stated that the policy presents significant gaps in the technical implementation of security. Although it mentions fundamental tools such as firewalls and IDS/IPS, it does not establish specific parameters for their effective implementation. The absence of minimum standards and update protocols compromises the robustness of the security system.

This lack of technical specificity can result in inconsistent implementations across departments, difficulty in evaluating security measure compliance, potential vulnerabilities due to lack of clear standards. A technical annex needs to be developed that specifies: Minimum standards for security configurations, Detailed implementation and maintenance protocols, Integration with international frameworks such as ISO/IEC 27001 and NIST

The policy lacks a structured methodology for risk management and does not establish clear mechanisms for compliance and accountability. The absence of specific sanctions and audit processes weakens its enforcement capability.

Table 2. *Risk Management and Compliance Identified Deficiencies.*

Impact	Improvement Recommendations
These shortcomings generate: Difficulty in prioritizing security resources and efforts. Lack of clarity on consequences for non-compliance. Inability to effectively measure the security level.	**It is necessary to incorporate:** A detailed methodology for risk assessment and management A specific and gradual sanctioning regime Audit procedures with defined deadlines and metrics. Incident Response and Operational Continuity Identified Deficiencies The policy does not adequately cover incident management or operational continuity. A complete framework for crisis management and disaster recovery is missing.
This omission can result in: Disorganized responses to security incidents. Extended recovery times. Potential loss of critical data	A detailed incident response plan Business continuity protocols with specific roles Disaster recovery procedures with objective timelines Human Factor and Training Identified Deficiencies The policy underestimates the importance of the human factor in information security. The lack of structured training and awareness programs represents a significant risk.
These deficiencies can lead to: Increased vulnerability to social engineering attacks. Insecure behaviors by staff. Security incidents due to human error	It is essential to implement: a) Mandatory training programs with periodic evaluations. b) Regular phishing attack simulations. c) Clear policies on the use of personal devices. d) Lack of Personal Data Control

Source of own elaboration (2025)

In previous years, some incidents related to personal data occurred within the MEP institution. Part of this is reflected in the policy in question.

Table 3. *Problems related to personal data occurred within the MEP institution.*

Identified Problem	Potential Impact
Lack of application of Law 8968 in the cybersecurity policy	Legal risk and possible sanctions for non-compliance with data protection legislation
No clear mechanisms are established for the collection, processing, and storage of personal data	Vulnerability to leaks and misuse of personal information
The right to informational self-determination in accordance with Law 8968 is not guaranteed	Lack of transparency and trust in the handling of student and staff information
Informed consent processes for data processing are not defined	Risk of lawsuits or complaints for improper use of personal data
Security measures for the protection of personal data are not specified	Greater exposure to attacks and sensitive information leaks
The right to access, rectify, and delete personal data is not addressed	Users without tools to correct or delete their data from MEP systems
Guidelines on data transfer to third parties are not established	Risk of inappropriate data transfer to companies or third parties without control
Data anonymization is not mentioned as a mandatory practice	Unnecessary exposure of sensitive information that could be used maliciously
No sanctions or disciplinary measures are foreseen for non-compliance in data protection	Absence of consequences fosters non-compliance with good data protection practices
No responsible entity is specified to ensure compliance with Law 8968 within the MEP	No specific team or department guarantees the correct application of the regulations

Source of own elaboration (2025)

The current policy presents serious omissions regarding compliance with Law 8968 on Personal Data Protection. It does not establish the fundamental mechanisms to guarantee the protection of personal data, nor does it designate clear responsibilities for its implementation.

Legal Impact

The lack of alignment with Law 8968 exposes the MEP to:

a) Legal and administrative sanctions.

b) Vulnerability to lawsuits for data mishandling.

c) Non-compliance with constitutional obligations regarding informational self-determination.

Regulatory Recommendations It is necessary to implement:

a) specific framework for compliance with Law 8968.

b) Designation of a data protection officer.

c) Clear procedures for exercising ARCO rights

The policy lacks specific procedures for collection and processing of personal data Informed consent processes Mechanisms for anonymization of sensitive information.

These shortcomings result in:

a) Risk of personal information leaks.

b) Lack of transparency in data handling.

c) Vulnerability to unauthorized uses of information.

It must be established detailed protocols for data collection and processing Informed consent systems Mandatory anonymization procedures.

Rights of Data Subjects Identified Deficiencies The policy does not adequately address: Mechanisms for exercising ARCO rights Data rectification procedures Protocols for the deletion of personal information. This omission affects:

a) Users' ability to control their data.

b) Transparency in personal information handling.

c) Trust in MEP systems.

Implementation. Recommendations It is necessary to develop:

a) Personal data access platforms.

b) Rectification and update procedures.

c) Information deletion systems.

d) Data Transfer and Security Identified Deficiencies The policy does not establish: Guidelines for data transfer to third parties Security requirements for

personal information Controls over access to sensitive data

These deficiencies generate:

a) Risk of inappropriate data transfers.

b) Vulnerability to unauthorized access.

c) Unnecessary exposure of sensitive information.

d) Secure data transfer protocols.

e) Granular access controls.

f) Monitoring and auditing systems.

g) Responsibility and Compliance Identified Deficiencies The policy lacks: Clear assignment of responsibilities Specific sanctions for non-compliance Supervision and control mechanisms.

h) Lack of clear responsibility.

i) Difficulty in implementing corrective measures.

j) Risk of systematic non-compliance.

k) A data protection committee.

l) Specific sanctions regime.

m) Regular auditing and control system.

4. CONCLUSIONS

The cybersecurity policy of the Ministry of Public Education (MEP) is presented as a document lacking practical sense, whose structure reflects a deep disconnection between its stated purpose and the reality of information security management. Although its wording includes general principles and technical terms widely used in the discipline, the absence of concrete guidelines, control mechanisms, and effective implementation strategies turns it into an empty instrument, intended more to fulfill a bureaucratic requirement than to offer a true guide for the protection of the institution's information and technological infrastructure.

From a critical perspective, it is evident that this document not only lacks internal coherence but also demonstrates a negligent omission in the application of fundamental regulatory frameworks, such as Law 8968 for the Protection of Individuals against the Processing of their Personal Data. The collection, processing, storage, and deletion of personal data are not adequately regulated within the document, which leaves students and officials exposed to arbitrary and potentially risky handling of their information. The lack of concrete anonymization measures, transparency in data management, and effective control mechanisms opens the possibility for violations of fundamental rights without a clear prevention or mitigation protocol.

A Cybersecurity Policy without Cybersecurity The document fails to fulfill its central

purpose: to protect information and guarantee the technological resilience of the MEP. Its structure does not identify concrete mechanisms for the detection, response, and recovery from security incidents. No continuous monitoring system or clear auditing strategy is established, which leaves the institution in a state of latent vulnerability. Beyond a simple statement of intentions, the lack of detailed processes and true operationalization turns this policy into a text with no real impact on the prevention of cyberattacks.

Recent experiences of attacks on government institutions in Costa Rica have demonstrated the fragility of the country's technological infrastructures and the urgent need for robust and well-defined strategies. However, this document ignores past lessons and fails to establish clear mechanisms to prevent catastrophic events such as those that occurred in the Ministry of Finance, the Costa Rican Social Security Fund (CCSS), and other public entities from happening again. The omission of strict controls on system access, the lack of a detailed business continuity plan, and the absence of protocols for action in the event of cyberattacks reinforce the perception that this policy does not represent a serious effort to strengthen institutional security.

The Danger of Becoming a Bureaucratic Document Beyond its technical deficiencies, the greatest threat of this policy lies in its ultimate fate: to become a reference document that no one consults or applies, another file in institutional bureaucracy, incapable of generating real changes in the cybersecurity culture. By lacking well-defined sanctions for non-compliance and failing to establish accountability mechanisms, a culture of indifference and complacency is fostered, where information security is seen as a simple formality rather than a strategic priority.

The document also ignores a fundamental element: the real awareness and training of users. Without a clear cybersecurity education strategy, the policy loses its purpose, as information security does not depend solely on technological tools but on the behavior of those who use them. The absence of robust and continuous training programs demonstrates a lack of long-term vision, leaving officials and students without the necessary preparation to identify and mitigate threats.

Towards an Urgent Review and Real Transformation, The lack of substance and applicability of this policy not only represents an institutional risk but also evidences a worrying lack of commitment to the protection of information and the digital security of the educational community. It is imperative to rethink this document from a perspective that prioritizes action, effectiveness, and adaptability to emerging threats. To achieve this, the following fundamental aspects must be considered:

Effective application of Law 8968: Clear compliance mechanisms for the protection of personal data must be established, guaranteeing the right to informational self-determination of students and officials. Implementation of mandatory security measures: Multi-factor authentication must be a requirement in all critical systems, and end-to-end encryption must be a minimum standard. Continuous monitoring and incident response: It is necessary to establish a Security Operations Center (SOC) that allows for early detection and mitigation of threats. Clear sanctions for non-compliance: The document must include penalties for those who do not follow the established regulations, thus avoiding impunity and negligence in security management. Education and cybersecurity culture: Without a real training strategy, the policy will remain ineffective. It is necessary to invest in continuous training for the entire educational community. Audits and periodic reviews: Internal and external audit mechanisms must be established to ensure that security measures are effective and updated against new threats.

Information security is not an optional or secondary issue; it is an urgent need in an increasingly digitized world exposed to high-impact technological risks. Inaction in this field not only compromises the integrity of institutional data but also endangers trust in the educational system and the security of thousands of students and officials. It is time for the MEP to set aside empty policies and adopt a serious, technical, and applicable approach to cybersecurity management.

5. REFERENCES

Ministry of Public Education. (2019). About the MEP. MEP website. *https://dgth.mep.go.cr/sobre-el-mep/*

Moreno Guerra Carlos Bladimir (2019) "Information security for third-level educational institutions based on ISO/IE27001", Caribbean Journal of Social Sciences *https://www.eumed.net/rev/caribe/2019/07/seguridad-informacion.html*

Purpura (2006, p 20) "Security Personnel Training Manual"

Purpura (2006, p 21) "Security Personnel Training Manual"

Sibaja David (2024) MEP closed 180 schools in the last 10 years *https://www.teletica.com/calle-7/mep-cerro-180-escuelas-en-los-ultimos-10-anos_352595*