55

Presentation date: January, 2024
Date of acceptance: April , 2024
Publication date: May, 2024

SYSTEM

OF MEASURES RELATED TO ENSURING INFORMATION SECURITY IN THE MANAGEMENT OF EDUCATIONAL INSTITUTIONS

SISTEMA DE MEDIDAS RELACIONADAS CON GARANTIZAR LA SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LAS INSTITUCIONES EDUCATIVAS

Ulviyya Hajiyeva Davud [1*]
E-mail: ulviyyehaciyeva13@mail.ru
ORCID: https://orcid.org/0000-0002-9612-6702
Mirvari Gasimova Mammad [1]
E-mail: qasimovamirvari@gmail.com
ORCID: https://orcid.org/0000-0001-5404-9799
Gunay Aliyeva Dilgam gizi [1]
E-mail: aliyevagunay79@yahoo.com
ORCID: https://orcid.org/0000-0001-5780-039X
Yegana Iskenderova Khaleddin [1]
E-mail: i.yegana90@hotmail.com
ORCID: https://orcid.org/0000-0002-8467-1543
* Author for correspondence
[1] Azerbaijan State Pedagogical University.

Suggested citation (APA, seventh ed.)

Hajiyeva, U., Gasimova, M., Dilgam, G. A., & Iskenderova, Y. (2024). System of measures related to ensuring information security in the management of educational institutions. ***Universidad y Sociedad, 16***(3),523-528.

ABSTRACT

Establishing an effective system of measures to uphold information security within the management framework of educational institutions hinges on a clearly defined purpose and vision. The core mission underlying information security measures implemented by an institution's leadership stems from the need to safeguard informational resources, so once this foundational objective is established, a holistic system of security measures can be methodically constructed and deployed in service of the organization's mission and long-term vision. However, ensuring the successful execution of this system is a responsibility that transcends just institution management, it requires accountability and buy-in from all stakeholders. Administrators, faculty, staff, and students alike must collectively embrace their respective roles in upholding the information security protocols. Then, fostering an ingrained culture of information security awareness, coupled with judicious risk assessment, deployment of technical safeguards, end-user training, and continual process evaluation are all vital components. Considering the above, this research discussed the most important elements of the system of measures related to ensuring information security in the management of educational institutions.

Keywords: Information security, Effective control, Measures system.

RESUMEN

Establecer un sistema eficaz de medidas para mantener la seguridad de la información dentro del marco de gestión de las instituciones educativas depende de un propósito y una visión claramente definidos. La misión central que subyace a las medidas de seguridad de la información implementadas por el liderazgo de una institución surge de la necesidad de salvaguardar los recursos de información, por lo que una vez que se establece este objetivo fundamental, se puede construir e implementar metódicamente un sistema holístico de medidas de seguridad al servicio de la misión de la organización y su largo plazo. visión del término. Sin embargo, garantizar la ejecución exitosa de este sistema es una responsabilidad que trasciende la mera gestión institucional: requiere rendición de cuentas y aceptación de todas las partes interesadas. Tanto los administradores, profesores, personal y estudiantes deben asumir colectivamente sus respectivos roles en el mantenimiento de los protocolos de seguridad de la información. Luego,

fomentar una cultura arraigada de concientización sobre la seguridad de la información, junto con una evaluación juiciosa de los riesgos, el despliegue de salvaguardias técnicas, la capacitación del usuario final y la evaluación continua de los procesos, son todos componentes vitales. Considerando lo anterior, en esta investigación se discuten los elementos más importantes del sistema de medidas relacionadas con garantizar la seguridad de la información en la gestión de las instituciones educativas.

Palabras claves: seguridad de la información, control efectivo, sistema de medidas.

INTRODUCTION

Information security (IS) refers to the tools, processes, and protocols used to protect all forms of information types from unauthorized access, usage, disclosure, disruption, alteration, or deletion. Information security is a broad domain encompassing diverse facets such as policy establishment, network and infrastructure security, testing, auditing, and more (Cardenas-Solano et al., 2016; Lundgren & Möller, 2019). In general, the fundamental components of information security encompass: (1) ensuring that information remains accessible solely to authorized individuals (confidentiality); (2) preserving the accuracy and dependability of information and systems (integrity); and (3) guaranteeing that information and systems are usable and accessible as required (availability). Frequently, the terms "information security" and "cybersecurity" are used interchangeably, although they bear distinct meanings. IS represents a pivotal aspect of cybersecurity, focusing primarily on data security, whereas cybersecurity encompasses a broader spectrum of security measures, including IS. Therefore, IS constitutes an essential component of cybersecurity, concentrating specifically on the security of data (Taherdoost, 2022; von Solms & van Niekerk, 2013). In general, information security plays an outstanding role in safeguarding an organization's critical information, which includes digital files, physical documents, media, and even verbal communications. Considering the escalating reliance on digital information, companies are making significant investments in information security technologies, as well as skilled personnel, to mitigate security risks and safeguard sensitive enterprise information against misuse, unauthorized entry, disruption, or deletion (Corallo et al., 2022; Kritzinger & Smith, 2008).

Educational institutions are not the exception, since IS holds significant relevance across various critical aspects of their operations. For example, these institutions accumulate a lot of sensitive data concerning their students, including personal details, academic records, and sometimes financial information. Robust information security measures are then necessary to safeguard this data from unauthorized access, misuse, or theft, thereby upholding the privacy and rights of students within the institution's care. Moreover, maintaining the integrity of academic records and assessments is pivotal in educational settings. Information security is necessary to preserve the accuracy and credibility of these records. This ensures that academic achievements remain unaltered and trustworthy, fostering an environment of academic honesty and fairness. In addition, information security becomes even more critical for institutions engaged in research activities. Research often involves handling sensitive data, intellectual property, and confidential findings. Therefore, ensuring robust information security protects these assets, creating an adequate environment for innovative research without the fear of data compromise or intellectual property theft (Hina & Dominic, 2020; Siponen et al., 2014).

It is important to highlight that information security is indispensable in the growing adoption of online learning platforms and digital resources. Safeguarding these platforms from cyber threats ensures the confidentiality and availability of educational materials. This, in turn, guarantees uninterrupted learning experiences for students and faculty, fostering a seamless transition to digital learning environments. Beyond regulatory requirements, maintaining a strong security posture significantly contributes to preserving the institutional reputation. Information security breaches can have far-reaching effects on public trust and perception. Demonstrating a commitment to protecting student interests, faculty research, and institutional integrity through robust security measures helps uphold the institution's standing within the community (Hui et al., 2023).

The topic of Information Security and its relation/application with educational institutions has been well addressed. For example, Cheung (2014) and Rehman et al. (2013) both emphasize the need for a comprehensive information security management system, with Cheung identifying eight key control areas and Rehman providing a general framework for implementation. Custer (2010) underscores the necessity of an institutional security program based on risk assessment and clear governance. Various studies have explored compliance with information security policies in higher education institutions, emphasizing the influence of institutional governance on protection motivation and information security policy compliance (Hina & Dominic, 2020). Additionally, research has shown that organizational information security climate and social bonding play a significant role in enhancing information

security policy compliance among healthcare professionals, such as nurses (Dong et al., 2021). Effective information security management frameworks and strategies are essential for higher education institutions to safeguard their information assets from security threats (Merchan-Lima et al., 2021). These frameworks are based on standards such as ISO 27000, COBIT, ITIL, NIST, and EDUCAUSE, providing a strategic reference for the development and implementation of information security management practices.

Furthermore, the use of blockchain technology and IoT-edge frameworks has been proposed to enhance the sharing of healthcare services while addressing concerns about data privacy and security (ElRahman & Alluhaidan, 2021; Zhang & Lin, 2018). In the context of digitalization and the increasing vulnerability of individuals in the information field, there is a need for a systematic approach to personal information security to protect individuals in the digital economy and digital management (Puinko & Tolkacheva, 2021). Additionally, the development of post-quantum public-key searchable encryption schemes on a blockchain has been suggested to ensure the security of information and prevent key leakage (Xu et al., 2022).

Overall, research in the field of information security for educational institutions highlights the importance of implementing robust information security policies, frameworks, and technologies to mitigate security risks and protect sensitive data in academic settings. Collaboration between academia, industry, and government institutions is crucial to address evolving security threats and ensure the confidentiality, integrity, and availability of information systems in educational environments. Considering the above, the objective of this work is to briefly discuss the most important elements of the system of measures related to ensuring information security in the management of educational institutions.

DEVELOPMENT

Thanks to information technologies, which have reached the highest level of development thanks to scientific and technical progress, the world is almost located in the palm of our hands, and any information circulates in a matter of seconds due to these technologies. It has entered our lives and enchanted us in such a way that we can hardly imagine that such high development is working against us at such a critical moment. Perhaps, most of us are so addicted to IT that we either cannot see its consequences or we are unable to understand the danger of any applied innovation for humanity. If we go back for a moment and think about the people who are still suffering from the tragedy that the atomic test brought to humanity, we will witness that after the tragedy, it is either impossible to eliminate the consequences, or it has left deep traces in our lives. From this point of view, the high development of information technologies has already created a similar situation along with its benefits:

...maintained as a result of the rapid development and wide spread of personal computers, geographically distributed computer systems and networks, information and network resources intended for general use, in all fields of activity, ensuring the security of processed and transmitted information has become a very serious issue. (von Solms & von Solms, 2004).

This requires the implementation of a system of measures to ensure information security, especially in educational institutions. Information security has made it necessary to establish good management practices consisting of policies and controls for the effective application of information security to protect the educational institution's information and protect it from any unauthorized access to the system, disclosure, and destruction. The Internet provides equal service to any user, even hackers, criminals, and people with negative intentions, and today hacker attacks, interceptions, information warfare, viruses, etc. are threats that can delete and destroy all the data of the educational institution at once.

When building a system of measures to ensure the information security of the educational institution, the heads of the educational institution should first understand the concepts of information security, the characteristics of computer systems and networks in terms of security, the places and weaknesses of information leaks from the systems, and the main directions for ensuring information security. The important elements for building a system of measures in this direction should be determined. Determining the area of control in the system of measures should not escape the manager's attention. Dana DesPlanques proposed an information security policy framework and noted its two directions. He suggested first reviewing the institution's existing policies and conducting a risk assessment. Then, after analyzing the initial stage, he proposed a comprehensive information security policy, procedures, and guidelines for preventing threats (Gasimov, 2009). The study notes that eight areas of information security control have been identified. These include areas such as information asset control, personnel control, physical control, access control, communication control, operational control, information system control, incident management, and business continuity. Developing a governance framework for establishing policies and implementing information security controls is also an important element. Experts

recommend maintaining the right balance between technical capabilities, flexibility, and management efficiency.

We consider it important to determine the purpose and vision of the process by examining the procedures for establishing a system of measures related to ensuring information security. The system of measures to be implemented by the management of the educational institution to ensure information security depends first on the goal and vision, and then on the implementation of the mission, i.e., tasks. As a rule, the goal of information security in all educational institutions, both higher and general education, is the protection of information resources, and the development of an algorithm for the prevention of threats and illegal actions against these resources. When taking security measures, the focus should be on the prevention of the main threats, such as disclosure, dissemination, leakage of information, illegal and unauthorized access to confidential information sources, and the implementation of copyright protection procedures. After that, organizational-technical actions and other measures of information security can be planned.

Before planning, it is necessary to classify mechanisms taking into account the nature and types of protection objects. This classification takes into account the educational institution's scope, territory, object type, methods of combating threats, and legal, organizational, engineering, and technical types of measures used. This series also includes separate elements of the territorial circle of the educational building, equipment, and technical systems, personnel, material and technical base, financial and information resources, and measures to eliminate threats. The research shows that the protection of information security and the creation of a system involves the systematic planning and implementation of measures. This system includes:

- Preventive measures and preventive works aimed at preempting the possibility of dangers and threats.
- Measures to limit or prevent the occurrence of hazards.
- Detection measures to prevent threats and criminal attacks or dirty acts.
- Measures related to the localization of threats and dangers.
- Measures to eliminate threats, dangers, or criminal acts.

Taking these directions into account, we believe that all businesses using the Internet, and all institutions, especially educational institutions, face more threats than groups using IT. Academic educational institutions use digital data to perform educational functions (DesPlanques, 2005). Therefore, they face unique information security threats such as data theft, malware infections, computer hacking, infiltration by other entities through their networks, website defacement, unauthorized use of internet bandwidth, etc. With the number of viruses, worms, trojans, hackers, phishers, and social engineers increasing day by day, it is almost impossible to stay safe on the Internet. Sangkyun and Choon proposed a framework for information systems security that emphasizes the design of information security controls, provides steps and tools for planning, and aligns security strategy with other strategies (Nizami et al., 2023).

Experiences show that it is impossible to prevent threats that are increasing like moths with only one institution, and the list of measures should be increased, and new models of anti-measures against threats should be developed. The head of each educational institution should first hire specialists in the field of information security, realizing their responsibility and accountability. Otherwise, IT provision is not possible: "For this purpose, important new roles are proposed, because the normal hierarchical system of the academic institution is not enough for the effective and efficient management of exceptions (in terms of information security)" (Bhilare et al., 2008). It is true that if the educational institution has limited financial resources, it can create IT security by training the existing staff and supporting personal and professional development. However, this does not seem to be very useful in ensuring a sustainable process. Every manager who understands the responsibility of their work and assesses the risk should work with good specialists share the responsibility with them and implement important measures. These measures include:

- Provide tactical and strategic planning, development, evaluation, and coordination of IT systems.
- Facilitate communication between staff, management, and other technology resources within the enterprise.
- Design, implement, and evaluate systems that support end users in the productive use of computer hardware and software.
- Develop information security policies, procedures, and guidelines for the educational institution.
- Organize monitoring to detect security violations related to the educational institution's information security policies.
- Manage response to information security incidents.

- Develop appropriate security solutions.

Every manager who understands the responsibility of their work and assesses the risk should work with good specialists and share the responsibility with them and implement these important measures.

Then, as part of our revision on the topic, we would like to note that threats to information security can never be eliminated, but it is possible to provide comprehensive protection to prevent security breaches. It is possible to prevent threats by developing and implementing a system of measures related to ensuring information security in the management of educational institutions using local and international experiences, and this depends very much on the responsibility and accountability of each person.

CONCLUSIONS

Ensuring robust information security for educational institutions necessitates a comprehensive approach integrating scientific innovations with practical measures. From a theoretical perspective, a holistic information security framework requires thoroughly analyzing threats and risks, determining optimal protection measures, utilizing automated monitoring to detect incursions, regulating encryption/decryption of sensitive data, and defining user access controls. Implementing technical solutions like anti-virus/malware programs, training personnel and students on security principles, and ensuring compliance with relevant policies and legislation are moreover essential underpinnings. Practically speaking, effective information security serves to protect confidential institutional data on students, academic records, curricula, and more through robust encryption and access management. A secure information infrastructure enhances the efficacy of core educational processes, affording administrators the ability to independently and securely manage critical data assets. Ultimately, fortifying information security demands a strategic, multi-layered approach synergizing pioneering technologies, rigorous theory, and pragmatic protective applications tailored to the needs of schools and universities.

Proactive investment in these innovations and best practices is crucial for educational institutions to remain resilient against the perpetually evolving landscape of cyber threats. In this regard, a key innovative frontier involves leveraging artificial intelligence and machine learning applications to analyze and identify threats, implement additional protective safeguards, and more effectively manage potential risks. Intelligent monitoring systems with advanced filtering, analysis, and automated adjustment of countermeasures represent another critical innovation.

REFERENCES

Bhilare, D. S., Ramani, A. K., & Tanwani, S. (2008). Information Protection in Academic Campuses: A Scalable Framework. ***Journal of Computer Science***, ***4***(10). https://doi.org/10.3844/jcssp.2008.864.870

Cardenas-Solano, L.-J., Martinez-Ardila, H., & Becerra-Ardila, L.-E. (2016). Information security management: A bibliographic review. ***Profesional de La Informacion***, ***25***(6), 931–948. https://doi.org/10.3145/epi.2016.nov.10

Cheung, S. K. S. (2014). Information Security Management for Higher Education Institutions. In J.-S. Pan, V. Snasel, E. S. Corchado, A. Abraham, & S.-L. Wang (Eds.), ***Intelligent Data Analysis and its Applications, Volume I*** (pp. 11–19). Springer International Publishing. https://doi.org/10.1007/978-3-319-07776-5_2

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. ***Computers in Industry***, ***137***, 103614. https://doi.org/10.1016/j.compind.2022.103614

Custer, W. L. (2010). Information security issues in higher education and institutional research. ***New Directions for Institutional Research***, ***2010***(146), 23–49. https://doi.org/10.1002/ir.341

DesPlanques, D. (2005). ***Information Security Policy Development for Institutions of Higher Education*** [School for Professional Studies MSCIS Program, Regis University]. https://vdocuments.mx/information-security-policy-development-for-institutions-of-higher-.html?page=2

Dong, K., Ali, R. F., Dominic, P. D. D., & Ali, S. E. A. (2021). The Effect of Organizational Information Security Climate on Information Security Policy Compliance: The Mediating Effect of Social Bonding towards Healthcare Nurses. ***Sustainability***, ***13***(5), Article 5. https://doi.org/10.3390/su13052800

ElRahman, S. A., & Alluhaidan, A. S. (2021). Blockchain technology and IoT-edge framework for sharing healthcare services. ***Soft Computing***, ***25***(21), 13753–13777. https://doi.org/10.1007/s00500-021-06041-4

Gasimov, V. (2009). ***Basics of information security***. Elm Publishing House.

Hina, S., & Dominic, P. D. D. (2020). Information security policies' compliance: A perspective for higher education institutions. ***Journal of Computer Information Systems***, ***60***(3), 201–211. https://doi.org/10.1080/08874417.2018.1432996

Hui, S. C., Kwok, M. Y., Kong, E. W. S., & Chiu, D. K. W. (2023). Information security and technical issues of cloud storage services: A qualitative study on university students in Hong Kong. ***Library Hi Tech***, ***ahead-of-print***(ahead-of-print). https://doi.org/10.1108/LHT-11-2022-0533

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. ***Computers & Security***, ***27***(5), 224–231. https://doi.org/10.1016/j.cose.2008.05.006

Lundgren, B., & Möller, N. (2019). Defining Information Security. ***Science and Engineering Ethics***, ***25***(2), 419–441. https://doi.org/10.1007/s11948-017-9992-1

Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sanchez, F., Lopez-Fonseca, G., & Quiroz, D. (2021). Information security management frameworks and strategies in higher education institutions: A systematic review. ***Annals of Telecommunications***, ***76***(3), 255–270. https://doi.org/10.1007/s12243-020-00783-2

Nizami, L. H., Tahir, G. E., Nazim, S. N., Farrukh, A. K., & Maharram, V. K. (2023). Development of inclusive education in Azerbaijan. ***Revista Conrado***, ***19***(S2), Article S2. https://conrado.ucf.edu.cu/index.php/conrado/article/view/3263

Puinko, L. E., & Tolkacheva, E. V. (2021). A systematic approach to personal information security in the context of digitalization of the economy and management. ***SHS Web of Conferences***, ***110***, 04012. https://doi.org/10.1051/shsconf/202111004012

Rehman, H., Masood, A., & Cheema, A. R. (2013). Information Security Management in Academic Institutes of Pakistan. ***2013 2nd National Conference on Information Assurance (NCIA)***, 47–51. https://doi.org/10.1109/NCIA.2013.6725323

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. ***Information & Management***, ***51***(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006

Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. ***Electronics***, ***11***(14), Article 14. https://doi.org/10.3390/electronics11142181

von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management. ***Computers & Security***, ***23***(5), 371–376. https://doi.org/10.1016/j.cose.2004.05.002

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. ***Computers & Security***, ***38***, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Xu, G., Xu, S., Cao, Y., Yun, F., Cui, Y., Yu, Y., & Xiao, K. (2022). PPSEB: A Postquantum Public-Key Searchable Encryption Scheme on Blockchain for E-Healthcare Scenarios. ***Security and Communication Networks***, ***2022***, e3368819. https://doi.org/10.1155/2022/3368819

Zhang, A., & Lin, X. (2018). Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. ***Journal of Medical Systems***, ***42***(8), 140. https://doi.org/10.1007/s10916-018-0995-5