Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue 1,* 2026
Website: https://ceapress.org

Information Systems Security and Data Protection in Public Administrations and Institutions under Presidential Decree No. 07-26

Raouf Mansouri
Lecturer B, Mohamed Lamine Debaghine University Sétif 2
Faculty of Law and Political Science
Laboratory for Human Rights Studies and Research
E-mail: r.mansouri@univ-setif2.dz

Received: 11/10/2025 **Accepted:25/04/2026** **Published: 08/06/2026**

Abstract:
The article addresses the issue of information systems security and data protection within Algerian public administrations under Presidential Decree No. 26/07, as a legal framework regulating data protection in the context of digital transformation. It highlights that the expansion of e-government has led to a significant increase in data volume and cyber security risks, necessitating an effective legal and regulatory framework. Information systems security is defined as a set of measures ensuring the confidentiality, integrity, and availability of information, with a distinction made from cyber security.
The article also emphasizes that data protection, particularly personal and sensitive data, is based on legal principles such as legality, proportionality, and confidentiality, within a coherent framework combining constitutional and legislative provisions, notably Law 18-07. It further explains that Decree 26/07 establishes organizational rules including the allocation of responsibilities, data classification, and the implementation of internal security policies.
Moreover, the article presents protection mechanisms combining technical and organizational measures, while stressing the importance of the human factor, as well as the various forms of legal liability in cases of information security breaches. It concludes by underscoring the need to update the legal framework and strengthen training and institutional coordination to address evolving digital challenges.
Keywords: Information Systems Security, Data Protection, Digital Transformation, Cyber security, Legal Liability.

Introduction

Modern administration relies heavily on information systems security and the protection of critical data as fundamental pillars of the contemporary state, particularly in light of the rapid digital transformations that have reshaped various sectors, most notably public administration. Information systems have become integral to the management of public services, as well as to the storage and processing of

administrative and personal data. Their adoption represents a strategic choice driven by the need to enhance the quality, efficiency, and effectiveness of public services.

In Algeria, Presidential Decree No. 07-26 was enacted to establish a legal framework governing information systems security and to introduce mechanisms for data protection within public administrations and institutions, in accordance with national security requirements and the imperative of ensuring the continuity of public services.

The growing volume of data exchanged through information networks has intensified with the transition toward e-government, encompassing both citizens' data and information of an administrative nature. Despite the numerous advantages associated with digital transformation, it also creates significant security challenges, including risks of unauthorized access, data breaches, cyber attacks, and disruptions to public services. Consequently, the need emerged for a comprehensive legal framework regulating the establishment, operation, and security of information systems within public administrations. Presidential Decree No. 07-26 seeks to fulfill this objective by defining the general principles governing information systems security, clarifying the responsibilities of relevant stakeholders, and establishing mechanisms for monitoring and oversight.

Research Problem

This study is based on the following central research question:

How does Presidential Decree No. 07-26 regulate information systems security and data protection within Algerian public administrations?

This primary question gives rise to several subsidiary inquiries, including: What is meant by information systems security under the provisions of this Decree? What organizational and technical measures have been established to protect data? How are the responsibilities of public administrations and institutions defined in this regard?

Significance of the Study

The importance of information systems security and data protection in public administrations stems from their direct relationship with Algeria's digital sovereignty and the protection of individual rights in an era characterized by increasing reliance on e-government applications and digital services. Data protection has become not only a legal issue but also a security and strategic concern, closely linked to citizens' trust in public institutions and the State's capacity to guarantee the confidentiality, integrity, and availability of information.

Furthermore, compliance by public institutions with the provisions of Presidential Decree No. 07-26 constitutes an essential safeguard for promoting good governance, optimizing the use of information resources, and reducing risks and threats associated with cyberspace.

Objectives of the Study

This study aims to:

Analyze the legal and regulatory framework established by Presidential Decree No. 07-26 concerning information systems security.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue 1,* 2026
Website: https://ceapress.org

Identify the mechanisms adopted for data protection within public administrations and institutions.

Determine the legal responsibilities of stakeholders involved in the management of information systems.

Assess the extent to which this legal and regulatory framework aligns with the requirements of digital transformation and contemporary cyber security threats.

Research Methodology

The study adopts a descriptive-analytical legal approach through an examination of the provisions of Presidential Decree No. 07-26 and an interpretative analysis of its legal rules, while relating them to the process of digital transformation within Algerian public administration.

In addition, legal analysis will be employed to identify the fundamental principles underlying the regulation of information systems security and data protection, as well as to evaluate their effectiveness in addressing cyber threats and security challenges.

Accordingly, this study seeks to contribute to the development of legal discourse concerning information systems security in the public sector and to highlight the essential role played by legal regulation in establishing a secure digital environment within Algerian public administrations.

First: The Conceptual and Legal Framework of Information Systems Security in Public Administrations

The conceptual and legal framework of information systems security in public administrations constitutes the foundation upon which all organizational and technical measures aimed at protecting data and ensuring the continuity of public services are built **(Presidential Decree No. 26-07, 2026, Arts. 2–4).**

From a conceptual perspective, information systems security refers to the set of preventive and corrective measures designed to protect the components of an information system—including hardware, software, databases, and communication networks—against any threat affecting the confidentiality, integrity, and availability of information. These three principles are commonly known in cyber security literature as the "Information Security Triad" **(ISO/IEC, 2013, pp. 01-05)** Within public administrations, this concept acquires a particular significance due to its direct connection with the protection of citizens' data, sensitive administrative information, and strategic information related to state security and the public interest **(Law No. 18-07, 2018, Arts. 3, 9).**

From a legal perspective, the regulation of information systems security in Algeria is based on a set of legislative and regulatory texts that establish an integrated legal framework. Foremost among these is Presidential Decree No. 26-07, which lays down the general rules governing information systems security within public bodies by defining security governance principles, allocating responsibilities, and establishing monitoring and oversight mechanisms **(Presidential Decree No. 26-07, 2026, Arts. 6–8).** This framework is complemented by Law No. 18-07 on the protection of natural

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue 1,* 2026
Website: https://ceapress.org

persons with regard to the processing of personal data, which enshrines the protection of personal information and requires public administrations to comply with lawful and secure data-processing standards **(Law No. 18-07, 2018, Arts. 5, 10, 34).** This complementarity reflects a legislative approach aimed at moving beyond purely technical protection toward a comprehensive framework integrating legal, organizational, and security dimensions **(Law No. 09-04, 2009, Arts. 2–3).**

Accordingly, while the conceptual framework defines the nature and objectives of information systems security, the legal framework translates these concepts into practical obligations imposed on public administrations. These obligations include the adoption of internal security policies, the classification of information according to its level of sensitivity, the implementation of physical and logical protection measures, and the provision of continuous training for users **(Presidential Decree No. 26-07, 2026, Art. 8)**. Furthermore, it establishes the principle of administrative accountability in cases of non-compliance with information security requirements, thereby strengthening a culture of compliance and prevention within public institutions **(Law No. 18-07, 2018, Arts. 49–50).** Consequently, understanding this dual framework—conceptual and legal—is a prerequisite for analyzing the effectiveness of information systems security within public administration and assessing its capacity to address the growing cyber threats associated with digital transformation.

1. General Concepts of Information Systems Security and Data Protection

Information systems security and data protection refer to the set of concepts and principles aimed at ensuring the security of the digital environment and safeguarding information processed within electronic systems against various risks and threats **(ISO/IEC, 2013, p. 01)**Information systems security is based on protecting the system's physical, software, and human components through technical and organizational measures that ensure the confidentiality of information by preventing unauthorized access, preserve its integrity against alteration or destruction, and guarantee its availability to authorized users whenever needed. These objectives are commonly known as the principles of confidentiality, integrity, and availability **(ISO/IEC, 2013, p. 05)**

The Algerian legislator has incorporated these principles through the regulation of information systems security within public administrations and institutions **(Presidential Decree No. 26-07, 2026, Arts. 2–4).** Data protection, on the other hand, concerns the regulation of the collection, processing, storage, and use of data in accordance with legal standards designed to safeguard rights and freedoms, particularly when dealing with personal or sensitive data **(Law No. 18-07, 2018, Arts. 3, 9, 10; Regulation (EU) 2016/679, 2016, Arts. 5–6).**

This field is also founded upon the principle of preventing information-related risks such as cyber attacks, unauthorized intrusions, and data breaches through the adoption of clear security policies, the allocation of responsibilities, and the implementation of effective monitoring and control mechanisms **(Law No. 09-04, 2009, Arts. 2–3;**

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue 1,* 2026
Website: https://ceapress.org

Presidential Decree No. 26-07, 2026, Art. 8). Such measures contribute to achieving a balance between the requirements of digital transformation, the need for information security, and the protection of privacy.

1.1 The Concept of Information Systems Security and Its Distinction from Cyber security

Information systems security refers to the set of technical, organizational, and legal measures implemented to protect the components of an information system—including hardware, software, databases, networks, and human resources—from various threats that may compromise the confidentiality, integrity, or availability of information **(ISO/IEC, 2013, pp. 01-05)**. This concept aims to ensure the continuity, reliability, and efficiency of information systems while preventing unauthorized access to, alteration of, or disruption of data through mechanisms such as access control, encryption, backup systems, and risk management practices **(ISO/IEC, 2013, pp. 08-10**). Information systems security is therefore a comprehensive concept that focuses on safeguarding the entire information environment of an organization, regardless of whether its components are connected to external networks or operate within a closed internal environment **(Whitman, 2018, pp. 15-18)**

This concept differs from cyber security in terms of the scope of protection and the nature of threats addressed. Information security primarily concerns the protection of data itself, irrespective of its format or storage medium, whether digital or physical, and is based on the principles of confidentiality, integrity, and availability **(ISO/IEC, 2013, p. 01)**. Cyber security, on the other hand, specifically relates to the protection of cyberspace, networks, and Internet-connected systems against cyber attacks, intrusions, and cross-border digital threats. It focuses particularly on combating cybercrime and network-based attacks **(Craigen, 2014, pp. 13-15)** Consequently, information systems security may be regarded as a broader concept than information security because it encompasses both technical and organizational components, whereas cyber security constitutes a specialized field dedicated to addressing threats associated with interconnected digital environments. These concepts are therefore complementary rather than contradictory, forming part of an integrated framework for information protection in the digital age.

2.1 The Concept of Personal and Administrative Data Protection

Data are defined as any information, regardless of its form or method of storage, that allows the identification of a natural person either directly or indirectly **(Law No. 18-07, 2018, Art. 3; Regulation (EU) 2016/679, 2016, Art. 4).** Data may be classified into several principal categories. The first category comprises personal data, which refers to information relating to an identified or identifiable natural person, such as a name, surname, identification number, address, telephone number, family status, or professional information **(Law No. 18-07, 2018, Art. 3).**

The second category consists of administrative data, which includes information related to the management of public services and administrative activities, such as official

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue 1,* 2026
Website: https://ceapress.org

correspondence, administrative decisions, personnel files, and regulatory documents. These data fall within the scope of documents produced, processed, or exchanged by public bodies in the exercise of their legal functions **(Presidential Decree No. 07-26, 2026, Arts. 2–4).**

The third category comprises sensitive data, which refers to a special class of information whose disclosure or processing without adequate safeguards may adversely affect fundamental rights and freedoms. This category includes health data, biometric information, political opinions, and religious or philosophical beliefs, all of which are subject to enhanced legal protection **(Law No. 18-07, 2018, Art. 7; Regulation (EU) 2016/679, 2016, Art. 9)**.

The legal protection of data within the administrative environment is founded upon several fundamental principles. The first is the principle of lawfulness, which requires that data processing be based on a legal provision or the explicit consent of the data subject **(Law No. 18-07, 2018, Art. 6; Regulation (EU) 2016/679, 2016, Art. 6).** The second is the principle of purpose limitation, which requires that data be collected for specific, explicit, and legitimate purposes and not subsequently used in a manner incompatible with those original objectives **(Law No. 18-07, 2018, Art. 4; Regulation (EU) 2016/679, 2016, Art. 5(1)(b)).**

Furthermore, the legal framework is based on the principles of proportionality and necessity, whereby only the data strictly required to achieve the administrative purpose may be collected **(Law No. 18-07, 2018, Art. 4).** It also incorporates the principle of accuracy and updating to ensure the correctness and reliability of information **(Regulation, 27 April 2016)**In addition, the principle of security and confidentiality obliges administrative authorities to adopt appropriate technical and organizational measures to protect data against loss, leakage, unauthorized access, or unlawful processing **(Law No. 18-07 of June 10)**

Taken together, these principles constitute the foundation for achieving a balance between the requirements of public administration and the protection of individuals' rights to privacy and personal data protection within the administrative environment.

1. The Constitutional, Legislative, and Regulatory Framework for Information Systems Security

The legal framework governing information systems security is based on an integrated hierarchy of legal norms, ranging from constitutional provisions to legislative and regulatory texts, thereby ensuring the protection of information and the safeguarding of rights and freedoms within the digital environment.

At the constitutional level, the 2020 Constitution of the People's Democratic Republic of Algeria enshrines a set of principles that constitute the legal foundation of information systems security, foremost among them the protection of privacy, the inviolability of correspondence, the confidentiality of communications, and the State's commitment to safeguarding personal data **(Constitution of the People's Democratic Republic of Algeria, 2020, Articles 46 and 47).** These constitutional guarantees serve

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue 1,* 2026
Website: https://ceapress.org

as supreme legal references that oblige both the legislature and public authorities to establish legal mechanisms ensuring information security and protecting individuals against any unlawful interference with their personal data.

At the legislative level, the legal framework has been reinforced through several laws regulating the digital sphere. Among the most significant is Law No. 18-07 on the Protection of Natural Persons with Regard to the Processing of Personal Data, which defines the conditions for collecting, processing, and storing personal data while guaranteeing individuals' rights of access, rectification, and objection **(Law No. 18-07, 2018, Articles 3, 6, and 32–34).** In addition, Law No. 09-04 on the Prevention and Combating of Crimes Related to Information and Communication Technologies criminalizes acts that undermine information systems, including unauthorized access, cyber sabotage, and the dissemination of malicious software **(Law No. 09-04, 2009, Articles 2, 3, and 6).** Together, these legal instruments provide both preventive and punitive mechanisms for protecting information systems against internal and external threats.

At the regulatory level, Presidential Decree No. 26-07 establishes the general rules governing information systems security within public administrations and institutions. It does so by defining standards for securing networks and information systems, regulating information classification, allocating responsibilities among the various stakeholders, and establishing mechanisms for monitoring and oversight (Presidential Decree No. 26-07, 2026, Articles 2–4 and 8). This decree serves as a link between constitutional principles and legislative provisions on the one hand and their practical implementation within public institutions on the other.

Accordingly, the constitutional, legislative, and regulatory framework for information systems security is based on a coherent legal hierarchy. It begins with the constitutional recognition of the right to privacy and data protection, proceeds through the establishment of general legal rules and sanctions, and culminates in the adoption of practical measures to ensure information systems security within public administration. This framework strengthens confidence in digital transformation and contributes to safeguarding the State's informational sovereignty.

1.2 The Constitutional Basis for Data Protection and the Inviolability of Digital Privacy

The constitutional basis for data protection and the inviolability of digital privacy constitutes the supreme foundation upon which the various legislative measures governing information systems security in Algeria are built. The 2020 Constitution of the People's Democratic Republic of Algeria recognizes the protection of private life as a constitutionally guaranteed right. Article 47 provides that every person has the right to the protection of his or her private life and honor, including personal data **(Constitution of the People's Democratic Republic of Algeria, 2020, Article 47).**

Furthermore, Article 48 guarantees the inviolability of private correspondence and communications in all their forms and stipulates that they may not be infringed upon

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue 1,* 2026
Website: https://ceapress.org

except pursuant to a reasoned judicial order (Constitution of the People's Democratic Republic of Algeria, 2020, Article 48). In the digital age, this protection extends to electronic communications and data transmitted through digital networks.

These constitutional provisions reflect the constitutional legislator's recognition that the concept of privacy has expanded into the digital sphere. Protection is no longer limited to traditional forms such as the home or paper correspondence; it now encompasses electronic data and information stored or processed through information systems. Consequently, the State is required to establish legal and regulatory mechanisms that ensure the protection of personal data against any unlawful processing and to oblige public administrations to comply with the principles of confidentiality, security, and proportionality when collecting or using data **(Law No. 18-07, 2018, Articles 4, 6, and 34).**

Therefore, data protection within the administrative environment is not merely a regulatory option but rather the implementation of a constitutional obligation aimed at preserving individual dignity and ensuring digital security in the face of rapid technological advancements.

1.2 Presidential Decree No. 26/07 as a Regulatory Framework for the Protection of Information Systems

Presidential Decree No. 26/07 constitutes the primary regulatory framework governing the protection of information systems within public administrations and institutions. It was enacted to establish general rules aimed at ensuring information security and safeguarding the State's vital interests in the digital environment **(Presidential Decree No. 26/07, 2026, Arts. 2–4)**. The Decree sets forth a series of provisions requiring public bodies to adopt organizational and technical measures to protect their information systems against risks of intrusion, destruction, or data leakage. It also emphasizes the necessity of implementing an information security policy within each institution and appointing an Information Systems Security Officer responsible for coordination, monitoring, and ensuring compliance with the prescribed standards **(Presidential Decree No. 26/07, 2026, Arts. 6–8).**

Among the most significant provisions of the Decree is the obligation imposed on public administrations to classify information and information systems according to their level of sensitivity, implement access control measures (including authorization management and password policies), secure networks and databases, and ensure data backup procedures as well as business continuity plans in cases of emergencies or cyber incidents **(Presidential Decree No. 26/07, 2026, Art. 8)**. Furthermore, the Decree requires sensitive systems to be subject to enhanced security measures and mandates the notification of the competent authorities whenever serious security incidents affecting the integrity of systems or data occur (Presidential Decree No. 26/07, 2026, Arts. 9–10).

With regard to its objectives, the Decree seeks to strengthen the State's digital security, ensure the continuity of public services, and protect administrative and strategic data

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue 1,* 2026
Website: https://ceapress.org

against both internal and external threats. It also aims to promote a culture of prevention and risk management within public administration **(Presidential Decree No. 26/07, 2026, Art. 2)**. Its scope of application extends to all central and decentralized administrations, as well as public institutions and bodies that rely on information systems in carrying out their functions **(Presidential Decree No. 26/07, 2026, Art. 3)**. Consequently, it serves as a binding regulatory instrument designed to standardize information system security requirements across the public sector and ensure their consistency with the demands of digital transformation.

Second: Mechanisms for Ensuring Information System Security and Data Protection in Public Institutions

The mechanisms for ensuring information system security and data protection within public institutions are achieved through an integrated framework that combines organizational, technical, and human measures, thereby ensuring the protection of information and the continuity of public services **(Presidential Decree No. 26/07, 2026, Arts. 2–4).** From an organizational perspective, public institutions are required to establish a written information security policy that defines objectives, responsibilities, and protective procedures, while appointing an Information Systems Security Officer responsible for supervising the implementation of security measures and monitoring risk assessment processes **(Presidential Decree No. 26/07, 2026, Arts. 6–8; ISO/IEC, 2013, Clauses 5–6)**. Public administrations also adopt the principle of information classification according to sensitivity levels and establish strict access control mechanisms by granting privileges in accordance with the "need-to-know" principle **(Presidential Decree No. 26/07, 2026, Art. 8; ISO/IEC, 2013, Annex A.9).** From a technical perspective, these mechanisms include the use of encryption systems to protect data during storage and transmission, the deployment of firewalls and intrusion detection and prevention systems, the securing of internal networks, and the regular updating of software to address security vulnerabilities **(ISO/IEC, 2013, Annexes A.10, A.12, and A.13)**. Regular data backup procedures, business continuity planning, and disaster recovery plans also constitute essential tools for ensuring data availability and preventing data loss in the event of incidents or cyberattacks **(ISO/IEC, 2013, Annex A.17; Presidential Decree No. 26/07, 2026, Art. 8).**

From a human perspective, awareness-raising and continuous staff training are regarded as fundamental components, given that human error remains one of the leading causes of security breaches **(ISO/IEC, ISO/IEC 27001:2013 Information Security Management Systems , 2013)** Consequently, training programs are implemented to strengthen information security awareness and foster a security-oriented culture, alongside the imposition of legal obligations concerning professional secrecy and data confidentiality **(Law No. 18-07 of 2018, Arts. 34 and 49).** These mechanisms are further reinforced through periodic monitoring and auditing systems designed to verify compliance with established standards, ensure the prompt reporting

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue 1,* 2026
Website: https://ceapress.org

of security incidents, and facilitate the implementation of appropriate corrective measures **(Presidential Decree No. 26/07, 2026, Arts. 9–10).**

Accordingly, the protection of information systems within public institutions is founded upon a comprehensive approach based on prevention, risk management, and the integration of legal, technical, and organizational dimensions.

1. Technical and Organizational Measures for Information Security

Technical and organizational information security measures consist of a set of integrated procedures and policies aimed at protecting information systems and data within public institutions against various risks and threats, while ensuring the continuity of public services in an efficient and reliable manner **(Presidential Decree No. 26/07, 2026, Arts. 2–4; ISO/IEC, 2013, Clauses 4–6).**

From a technical perspective, these measures include securing networks and communication systems through the use of firewalls and intrusion detection and prevention systems, as well as implementing encryption mechanisms to protect data during storage and transmission. They also encompass regular data backup procedures, the establishment of business continuity and disaster recovery plans, continuous system updates and maintenance to address security vulnerabilities, and the deployment of antivirus and anti-malware solutions **(ISO/IEC, 2013, Annexes A.10, A.12, A.13, A.17).**

Organizational measures, on the other hand, involve the development of clear policies defining responsibilities and authorities, the implementation of access control mechanisms based on the "need-to-know" principle, and the classification of information according to its level of sensitivity in order to ensure the protection of sensitive and strategic data **(Presidential Decree No. 26/07, 2026, Art. 8; ISO/IEC, 2013, Annex A.9).** These measures also include the organization of continuous training programs to strengthen information security awareness among employees and reduce human errors **(ISO/IEC, 2013, Annex A.7),** as well as conducting regular monitoring and auditing activities to verify compliance with security standards and identify any deficiencies **(Presidential Decree No. 26/07, 2026, Arts. 9–10).**

By integrating both technical and organizational measures, a secure information environment can be established within public institutions, enhancing data protection, mitigating cyber risks, and supporting sustainable and effective digital transformation while complying with the legal obligation to ensure data security and confidentiality as stipulated by law **(Law No. 18-07, 2018, Art. 34).**

1.1 Technical Measures for System Protection

Technical measures for the protection of information systems focus on safeguarding digital assets and ensuring the confidentiality, integrity, and availability of information, commonly referred to in information security literature as the CIA Triad (Confidentiality, Integrity, Availability) **(ISO/IEC, 2013, p. 01)**These measures include security systems designed to monitor network activities and detect suspicious behavior or intrusion attempts, such as intrusion detection and prevention systems

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue 1,* 2026
Website: https://ceapress.org

(ISO/IEC, 2013, Annexes A.12, A.13). They also involve the use of encryption technologies that protect data during storage and transmission and prevent unauthorized access **(ISO/IEC, 2013, Annex A.10).**

Firewalls constitute another essential security mechanism, acting as a barrier between internal and external networks to prevent unauthorized access **(ISO/IEC, 2013, Annex A.13).** Regular data backup procedures are also implemented to ensure data recovery in the event of system failures or cyber attacks, as part of broader business continuity and disaster recovery strategies **(ISO/IEC, 2013, Annex A.17).** Furthermore, protection mechanisms include access monitoring through strong password policies and multi-factor authentication systems to regulate user privileges and ensure that access is granted only to authorized individuals **(ISO/IEC, 2013, Annex A.9)**. These measures are aligned with the regulatory obligations imposed on public institutions under Presidential Decree No. 26/07 **(Presidential Decree No. 26/07, 2026, Art. 8)** and with the duty to ensure data security and confidentiality established by Law No. 18-07 **(Law No. 18-07, 2018, Art. 34).**

Collectively, these technical measures constitute the primary line of defense for maintaining the security of information systems and protecting sensitive data within public institutions.

The technical measures adopted for the protection of information systems in public institutions may be organized as follows:

2.1 Access Control and Protection Systems

These measures encompass all mechanisms aimed at monitoring user activities within networks and information systems, as well as detecting any unauthorized access attempts or suspicious behaviors **(ISO/IEC, 2013, Annex A.12, A.13)**. This is achieved through the implementation of access control policies, the use of strong passwords, and the deployment of multi-factor authentication systems to ensure that access to information systems is restricted solely to authorized individuals **(ISO/IEC, 2013, Annex A.9; Presidential Decree No. 26-07, 2026, Article 8).** Furthermore, these systems contribute to the monitoring and recording of security-related events, enabling analysis and auditing when necessary, in accordance with security auditing requirements and the supervision of sensitive data as stipulated in Law No. 18-07 **(Law No. 18-07, 2018, Article 34).**

3.1 Encryption and Firewalls

Encryption is considered one of the most important technical measures for protecting data during storage and transmission across systems and networks, as it prevents unauthorized access to or modification of information **(ISO/IEC, 2013, Annex A.10).** Firewalls, on the other hand, function as a security barrier between internal and external networks. They filter data traffic and prevent unauthorized access and cyber attacks originating from external sources, thereby ensuring the protection of information systems against various cyber security threats **(ISO/IEC, 2013, Annex A.13; Presidential Decree No. 26-07, 2026, Article 8).**

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue 1,* 2026
Website: https://ceapress.org

4.1 Backup and Business Continuity

Regular data backup is regarded as a fundamental mechanism for ensuring the recovery of information in the event of data loss caused by technical failures or cyber attacks **(ISO/IEC, 2013, Annex A.17).** This measure is complemented by the establishment of business continuity plans and disaster recovery plans, which ensure the uninterrupted operation of critical systems within public administrations and minimize the impact of security incidents on administrative processes **(ISO/IEC, 2013, Annex A.17; Presidential Decree No. 26-07, 2026, Article 8).**

In this way, these three technical measures—access monitoring and protection systems, encryption and firewalls, and backup and recovery plans—constitute an integrated framework that ensures the security of information systems and the protection of data within public institutions, in compliance with the legal obligations set forth in Law No. 18-07 concerning the protection of personal data **(Law No. 18-07, 2018, Article 34).**

2. Organizational and Administrative Measures

Organizational and administrative measures aimed at ensuring information systems security and protecting data within public institutions can be expanded as follows:

These committees or units constitute the backbone of security governance within public administrations, as they are composed of technical, legal, and administrative specialists to ensure comprehensive information security management **(ISO/IEC, 2013, Clauses 5–6).** Their responsibilities include conducting periodic risk assessments, monitoring potential threats, and developing rapid response plans for cyber security incidents **(ISO/IEC, 2013, Annex A.16, A.17).** They are also responsible for designing prevention and awareness strategies, organizing employee training programs on the secure use of information systems, and coordinating with supervisory and external bodies whenever necessary to safeguard critical data **(Presidential Decree No. 26/07 of 2026, Articles 6–8; Law No. 18-07 of 2018, Article 34).** The existence of such structures strengthens the culture of institutional security within public administrations by ensuring that employees are fully aware of their responsibilities and obligations regarding data protection.

2.1 Establishing Information Security Committees or Units

These committees or units represent the cornerstone of security governance within public institutions. They are composed of technical, legal, and administrative experts tasked with ensuring a comprehensive approach to information security management **(ISO/IEC, 2013, Clauses 5–6).** Their duties include regularly assessing risks, identifying potential threats, and preparing rapid response plans to address cyber security incidents **(ISO/IEC, 2013, Annex A.16, A.17).** Furthermore, these committees develop prevention and awareness strategies, organize staff training programs on the secure handling of information systems, and coordinate with regulatory and external authorities whenever necessary to ensure the protection of critical data **(Presidential Decree No. 26/07 of 2026, Articles 6–8; Law No. 18-07 of 2018, Article 34).** The establishment of such bodies enhances the institutional security culture within public

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue 1,* 2026
Website: https://ceapress.org

administrations, fostering greater awareness among employees regarding their data protection responsibilities and obligations.

2.2 Developing Internal Policies and Secure Operating Procedures

Internal policies constitute the reference framework governing the handling and protection of information within public institutions **(ISO/IEC, 2013, Clauses 5–6).** These policies define the responsibilities and authorities assigned to each employee and enforce the "need-to-know" principle, whereby access to information is granted solely to individuals directly involved in the relevant tasks **(ISO/IEC, 2013, Annex A.9; Presidential Decree No. 26/07 of 2026, Article 8).**

Secure operating procedures further include classifying data according to its level of sensitivity, ensuring that personal and sensitive information is stored and processed in accordance with established standards, issuing clear instructions regarding the handling of storage devices, and restricting the use of software to authorized applications only **(ISO/IEC, 2013, Annex A.8, A.12; Law No. 18-07 of 2018, Article 34).** These procedures also encompass internal control and auditing mechanisms through which operational activities are regularly reviewed to ensure compliance with security and legal requirements and to detect any irregularities or unauthorized access attempts **(ISO/IEC, 2013, Annex A.16; Presidential Decree No. 26/07 of 2026, Articles 9–10).**

2.3 Strengthening Training and Awareness Programs

Training and awareness programs constitute an integral component of organizational security measures. Through these programs, employees are trained on cyber security best practices, methods for identifying intrusion attempts and phishing attacks, and appropriate responses to security incidents **(Scholl, 2018)**This approach has been expressly endorsed by the Algerian legislator, as Presidential Decree No. 26/07 requires the newly established structure to undertake the mission of "raising awareness and providing training to users in the fields of information systems security and personal data protection" as an independent function within its organizational framework **(Presidential Decree No. 26/07 of 2026, Article 4).**

These programs also contribute to fostering a culture of prevention and both individual and collective responsibility **(Corradini, 2020)**Moreover, the same decree obliges the structure to "ensure continuous vigilance and permanent monitoring of information systems security" and to "immediately report any cyber incident to the competent authorities" **(Presidential Decree No. 26/07 of 2026, Article 4).** Such measures significantly reduce risks arising from human error, which remains one of the leading causes of security breaches. Recent studies indicate that human error is responsible for more than 95% of cyber security incidents **(Verizon, 2024)**

By combining the establishment of specialized committees, the implementation of internal security policies and secure operating procedures, and the strengthening of training and awareness initiatives, public administrations and institutions can develop a comprehensive information security framework **(Ubowska, 2022)**This approach is

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue 1,* 2026
Website: https://ceapress.org

reflected in Presidential Decree No. 26/07, which requires every public institution to establish an independent structure responsible for "developing the information systems security policy of the institution, administration, or body to which it belongs and ensuring its implementation" in accordance with the relevant national strategy **(Presidential Decree No. 26/07 of 2026, Article 4).** Such measures contribute to the effective protection of data, ensure the continuity of public services, and support digital transformation in a secure and sustainable manner **(Ikwuanusi, 2024)**

1. Legal Responsibility and Oversight in the Protection of Information Systems and Data

Legal responsibility and oversight constitute fundamental components for ensuring the protection of information systems and data within public institutions. Public administrations and employees responsible for managing these systems are required to comply with all applicable legal and regulatory measures. In particular, Presidential Decree No. 26-07 explicitly mandates that every public institution, administration, and public body establish an independent structure responsible for ensuring "compliance with legislation relating to the processing of personal data in coordination with the National Authority for Data Protection" **(Presidential Decree No. 26-07, 2026, Article 4),** as well as compliance with Law No. 18-07 on the Protection of Personal Data. Individuals who fail to comply with these obligations may incur legal consequences in cases of negligence, data leakage, or breaches of data confidentiality **(Baskerville, 2014)**

Oversight is exercised through two complementary mechanisms. The first is internal oversight, implemented through information security committees and audit teams responsible for monitoring the application of policies and procedures, assessing system integrity, and detecting intrusion attempts. This requirement is expressly stipulated in Presidential Decree No. 26-07, which obliges the designated structure to "conduct auditing and monitoring operations in the field of information systems security and personal data protection in cooperation with the competent authorities according to a predetermined program" **(Presidential Decree No. 26-07, 2026, Article 4).** The second mechanism is external oversight, carried out by supervisory authorities and general inspectorates that verify the extent to which public administrations comply with legal and security standards, issue recommendations, and adopt corrective measures when necessary **(ENISA, 2017)**

The objective of such responsibility and oversight is to foster a culture of compliance and both individual and institutional accountability **(Corradini, 2020)**, protect sensitive data against technical and human-related risks, and ensure a balance between digital transformation and the continuity of public services on the one hand, and the protection of individuals' rights to privacy and information confidentiality on the other **(Ikwuanusi, 2024)**This reflects the State's commitment to providing a secure and sustainable information environment within the public sector, as reaffirmed by Presidential Decree No. 26-07, which requires the designated structure to ensure

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue 1,* 2026
Website: https://ceapress.org

information systems security and data protection "permanently and under all circumstances" **(Presidential Decree No. 26-07, 2026, Article 3).**

1.2 Disciplinary, Civil, and Criminal Liability for Breaches of Information Systems Security

Disciplinary, civil, and criminal liability constitute essential mechanisms for deterring violations of information systems security and ensuring the protection of data within public institutions. Such liability may be imposed on individuals or public administrations whose negligence, misuse, or deliberate attacks on information systems result in damage or harm **(Baskerville, 2014)**Presidential Decree No. 26-07 established an integrated compliance framework by requiring the newly established structure to "ensure the implementation of legislation and regulatory provisions concerning the processing of personal data in coordination with the National Authority for Data Protection" **(Presidential Decree No. 26-07, Article 4).**

First: Disciplinary Liability

Disciplinary liability applies to employees of public institutions who violate information security instructions and internal policies. Such violations may result in sanctions including reprimands, denial of promotions, or dismissal from employment, in accordance with Ordinance No. 06-03 containing the General Civil Service Statute, which provides for a range of disciplinary sanctions against any public employee who fails to fulfill their professional obligations **(Ordinance No. 06-03, Article 163 et seq., 2006),** in addition to the provisions of the internal regulations of each administration.

Second: Civil Liability

Civil liability arises when a breach causes material or moral damage to an institution or to individuals, such as the loss of important data or the disclosure of personal information. Victims are entitled to seek compensation for damages under the provisions of the Civil Code, particularly the principle of fault-based liability established under Article 124 thereof **(Ordinance No. 75-58 containing the Civil Code, Article 124, as amended and supplemented).** Furthermore, Law No. 18-07 on the Protection of Personal Data recognizes the right of individuals to claim compensation for any infringement of their personal data rights **(Law No. 18-07, 2018).**

Third: Criminal Liability

Criminal liability applies in cases involving unauthorized access to information systems, system sabotage, dissemination of malicious software, or disclosure of sensitive information. Such acts are regulated by Law No. 09-04 establishing the specific rules for the prevention and combating of crimes related to information and communication technologies, which criminalizes attacks against information systems and prescribes penalties ranging from fines to imprisonment **(Law No. 09-04, Articles 2–10, 2009)**. In addition, the provisions of the Penal Code relating to breaches of professional secrecy and abuse of trust are applicable (Ordinance No. 66-156 containing the Penal Code, as amended and supplemented). The severity of penalties

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue 1,* 2026
Website: https://ceapress.org

varies according to the gravity of the offense and its impact on the State or on individuals **(Broadhurst, 2014)**

Collectively, these forms of liability contribute to strengthening discipline, safeguarding data, and promoting a culture of legal compliance within public institutions **(Corradini, 2020)** They ensure the security of information systems, the continuity of public services, and the protection of citizens' rights, which is precisely the objective reaffirmed by Presidential Decree No. 26-07 through its provision that the designated structure must guarantee security functions "permanently and under all circumstances" **(Presidential Decree No. 26-07, 2026, Article 3).**

2.2 Monitoring and Follow-up Mechanisms

Monitoring and follow-up mechanisms constitute a fundamental pillar for ensuring the effectiveness of protecting information systems and data within public institutions. They serve to verify compliance with legal and regulatory requirements while minimizing technical and human-related risks that may threaten information security and the continuity of public services **(ENISA, 2017)**This supervisory framework was established by Presidential Decree No. 26-07, which mandates the newly created structure to ensure information security functions "on a permanent basis and under all circumstances" **(Presidential Decree No. 26-07, 2026, Article 3).**

These mechanisms encompass several levels of oversight and evaluation. The first level consists of internal monitoring conducted by information security committees or internal audit teams within the institution. Their responsibilities include verifying the implementation of security policies and procedures, monitoring employees' compliance with security directives, detecting any unauthorized access attempts or system intrusions, documenting all incidents, and preparing detailed reports. Presidential Decree No. 26-07 explicitly provides for these functions by requiring the structure to "carry out auditing and monitoring operations in the field of information systems security and the protection of personal data in cooperation with the competent authorities according to a predetermined program," as well as to "ensure continuous vigilance and permanent monitoring of the security of information systems falling within its jurisdiction" **(Presidential Decree No. 26-07, 2026, Article 4).**

External oversight bodies also play a crucial role, most notably the National Authority for the Protection of Personal Data, which is expressly identified in Decree No. 26-07 as a coordinating entity responsible for "ensuring the implementation of legislative and regulatory provisions relating to the processing of personal data" **(Presidential Decree No. 26-07, 2026, Article 4; Law No. 18-07, 2018)**. This authority monitors the compliance of public institutions with personal data protection legislation, examines data collection, processing, and storage practices to ensure confidentiality and security, and provides recommendations aimed at reducing risks and improving protection measure**s (Da Veiga, 2020)** The role of such oversight bodies also includes conducting periodic assessments of information systems, including testing the resilience of networks and software against cyber threats and analyzing technical and organizational

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue 1,* 2026
Website: https://ceapress.org

vulnerabilities. This aligns with the requirements of Decree No. 26-07, which mandates the preparation of "a comprehensive risk map of threats to cyber security and personal data protection and the implementation of corrective action plans" **(Presidential Decree No. 26-07, 2026, Article 4),** with the objective of strengthening the administration's capacity to address potential security breaches.

Regular security reporting constitutes another integral component of the monitoring framework. Such reports document the results of monitoring and evaluation activities, identify vulnerabilities and risks, and provide practical recommendations for corrective action **(Scholl, 2018)**They also facilitate the reporting of major security incidents to higher authorities. This obligation is reinforced by Decree No. 26-07, which requires the structure to "immediately notify the competent authorities of any cyber incident and seek their assistance whenever necessary" **(Presidential Decree No. 26-07, 2026, Article 4)**. Furthermore, these reports support strategic decision-making aimed at enhancing information security, including updating policies, strengthening employee training and awareness programs, and improving technical **(Ubowska, 2022)**

Accordingly, monitoring and follow-up mechanisms form an integrated protection framework that combines internal oversight, periodic evaluation, supervision by specialized authorities, and analytical reporting **(Corradini, 2020)** Together, these mechanisms ensure the protection of information systems and data, promote legal compliance, and foster a culture of information security within public institutions. Consequently, they contribute to the establishment of a secure and sustainable digital environment that supports digital transformation while safeguarding citizens' rights and sensitive personal information **(Ikwuanusi, 2024).**

Conclusion

In conclusion, this study demonstrates that Presidential Decree No. 07-26 has established a comprehensive regulatory framework for strengthening information systems security and protecting data within public administrations and institutions. The decree provides a clear legal basis that defines the responsibilities of each entity and employee while setting out the technical and organizational measures necessary to ensure the integrity, confidentiality, and availability of information for authorized users. Furthermore, it has contributed to fostering a culture of information security within public administration through the reinforcement of the role of information security committees, the implementation of monitoring and control policies, and the promotion of compliance with legislation concerning the protection of personal and sensitive data. These measures have enhanced the capacity to manage risks, reduced the likelihood of security breaches and data leaks, and demonstrated the decree's effectiveness in supporting digital transformation within the public sector.

Despite the progress achieved, the study highlights the urgent need to update legal and regulatory provisions in order to keep pace with ongoing technological developments, including advanced cyber attacks, artificial intelligence, and Internet of Things (IoT) technologies. These emerging challenges require modern legal and procedural

mechanisms capable of providing more effective protection for information systems and data. The study also emphasizes the importance of strengthening continuous training and awareness programs for employees in the field of information security, considering that the human factor remains a fundamental element in the success of security measures. Regular training contributes to fostering a culture of compliance and enables employees to identify cyber threats and respond promptly and appropriately to security incidents.

Finally, the study underscores the necessity of enhancing coordination and cooperation among administrative, security, and regulatory bodies to ensure rapid responses to cyber incidents, facilitate information sharing regarding potential risks, and harmonize preventive and emergency response procedures. By combining an effective legal framework, continuous human resource development, and strong institutional coordination, it is possible to establish a secure and integrated information environment that supports digital transformation, ensures the continuity of public services, and safeguards individual rights and freedoms against future digital challenges. Consequently, Presidential Decree No. 07-26 represents an effective instrument for building a secure and sustainable public administration in the digital age.

References

I. Books

1-Corradini, I. (2020). Building a Cyber security Culture in Organizations: How to Bridge the Gap Between People and Digital Technology. Springer Nature.

2-Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security (6th ed.). Cengage Learning.

II. Journal Articles

1-Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture. Computers & Security, 92, 101713.

2-Ikwuanusi, A., Onunka, C., Owoade, A., & Uzoka, P. (2024). Digital transformation in public sector services. International Journal of Applied Research in Social Sciences, 6(11), 2744–2774.

3-Ubowska, A., & Królikowski, T. (2022). Building a cyber security culture of public administration system in Poland. Procedia Computer Science, 207, 1242–1250.

4-Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security. Information & Management, 51(1), 138–151.

5-Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and cybercrime. International Journal of Cyber Criminology, 8(1), 1–20.

6-Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cyber security. Technology Innovation Management Review, 4(10), 13–21.

III. Book Chapters / Scholarly Contributions

1-Scholl, M. (2018). Information security awareness in public administrations. In Public Management and Administration. IntechOpen.

IV. Institutional Reports and Studies

2-ENISA. (2017). Cyber Security Culture in Organisations.
3-Mimecast. (2025). The Human Risk Report.
4-Verizon. (2024). Data Breach Investigations Report (DBIR).

V. Technical Standards

1-ISO/IEC. (2013). ISO/IEC 27001:2013 Information Security Management Systems — Requirements. ISO/IEC.

Sixth: Laws and Regulations

1. Algerian Legislation

1-Official Gazette of the People's Democratic Republic of Algeria. (2007). Presidential Decree No. 07-26 of January 30, 2007, concerning the security of information systems. Official Gazette of the People's Democratic Republic of Algeria (JORA), No. 9.
2-Official Gazette of the People's Democratic Republic of Algeria. (2009). Law No. 09-04 of August 5, 2009, establishing the specific rules for the prevention and combating of offenses related to information and communication technologies. Official Gazette of the People's Democratic Republic of Algeria (JORA), No. 47.
3-Official Gazette of the People's Democratic Republic of Algeria. (2018). Law No. 18-07 of June 10, 2018, relating to the protection of natural persons in the processing of personal data. Official Gazette of the People's Democratic Republic of Algeria (JORA), No. 34.
4-People's Democratic Republic of Algeria. (2020). Constitution of November 1, 2020. Official Gazette, No. 82.

2. European Legislation

1-European Parliament & Council of the European Union. (2016).
2-Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR).
3-Official Journal of the European Union, L119.