Journal of Human Sciences
Oum El Bouaghi University
ISSN 1112-9255/E-ISSN 2588-2414
Volume 09 Numéro 02 – Juin -2022

OEB Univ. Publish. Co.

Information Security and the need to move towards the application of Standard Specifications in Algerian institutions

أمن المعلومات وضرورة الانتقال إلى تطبيق المواصفات القياسية في المؤسسات الجزائرية

Seffari Asma [1*]

[1] Oum El Bouaghi University, seffariasma84@yahoo.com

Date of receipt: 2022-01-29 Date of revision: 2022-02-15 Date of acceptation: 2022-04-17

Abstract

Through this study, we will try to show the need to move towards building information protection management systems through the application of the international standard ISO 27001 for Algerian institutions, and that with the massive spread of the use of information systems which led to an increase in threats to data integrity, information reliability, and the expansion of cybercrime.

We concluded that the rate of financial losses as a result of information crime exceeds the traditional crime in Algeria, and there is still a clear absence of the need to activate international standards for information protection, as the matter does not exceed the application of the quality management standard, and standards related to environmental systems, food safety, health and safety professional in a number of qualified institutions.

Keywords : Information protection systems, cybercrime, ISO 27001.

ملخص

من خلال هذه الدراسة سنحاول ابراز ضرورة انتقال المؤسسات الجزائرية نحو بناء نظم لإدارة حماية المعلومات عن طريق تطبيق المواصفة العالمية ايزو 27001، وذلك مع الانتشار الهائل لاستخدام نظم المعلومات الأمر الذي أدى إلى زيادة تهديدات سلامة البيانات وموثوقية المعلومات وتوسع الجريمة الالكترونية.

توصلنا إلى أن معدل الخسائر المالية نتيجة الجريمة المعلوماتية يفوق الجريمة التقليدية في الجزائر، كما أنه يزال هناك تغييب واضح لضرورة تفعيل المواصفات العالمية لحماية المعلومات، حيث لا يتعدى الأمر تطبيق عدد من المؤسسات المؤهلة لمعيار إدارة الجودة ، والمعايير المتعلقة بأنظمة البيئة، السلامة الغذائية والصحة والسلامة المهنية.

الكلمات المفتاحية: نظم حماية المعلومات، الجريمة الالكترونية، ايزو 27001 .

[*] Corresponding Author: Seffari Asma, Email: seffariasma84@yahoo.com

1. INTRODUCTION

Information has become a prominent feature of the modern age to the extent that it is called **the information era**, as it represents the main pillar of decision-making and also become the nerve that drives any activity carried out in the various fields, and due to this prominent role, it has become a force with in the hands of states and individuals.

Information systems in the contemporary business environment are important and sensitive factors for the success of institutions, and this is due to the strategic value these systems represent, therefore, the institution that fails to benefit from the inherent value of these systems, loses a large market share in favor of competitors, as well as the possibility of its exit from competition, which puts the issue of its continuity and survival hostage to the use of these modern systems.

However, the use of modern information systems makes it vulnerable to constantly evolving electronic attacks, which motivates institutions every time to provide various methods and tools that would ensure the confidentiality, safety and availability of the information from those attacks. Therefore, the task of information security has become difficult in light of the information crime that does not recognize borders and its professionals live in a virtual world. On this basis, the development of information security has become inevitable.

1.1. Statement of the problem

Based on the above, we raise the following fundamental question:

What is the reality of adopting a security strategy in Algerian institutions to protect their information systems from the various crimes that encounter?

1.2. Research Questions

Proceeding from the previous main question, the analysis was guided by the following question:

- What are the most important electronic risks facing the organization in light of the widespread use of information technology, and how to provide information security in the organization?
- What are the international standards developed to help institutions in managing their information security?
- What are the various measures adopted by Algerian institutions to protect their information systems?

1.3. Significance of study

The importance of the study lies in the fact that information has become an emerging economic force, also that the issue of information systems security is one of the most important topics, as it directly affects the lives of all those who deal with electronic media including business enterprises, and reflects their interests and ways of performing their work.

1.4. Research Methodology

Due to the nature of this study and the identification of its objectives, we relied on the descriptive and inductive approach.

The present study has been organized in three main chapters as follows:

- Presentation of the concept information security;
- Exposure of ISO 27000 standard specification;
- Reality of the various measures adopted by Algerian institutions to protect their information systems.

2. Information Security:

The development and protection of information system is so important and necessary for any organization to continue and keep pace with the surrounded changes, as it ensures the supply with the required information from the environment, whether it was internal or external, with the required specifications. Therefore, the organization must build an effective information system and work hard to protect it in all ways, as it is not a static thing but a dynamic one that changes and develops continuously and passes through several stages.

2.1. Defining information security

2.1.1. Information security meaning:

Several definitions have been provided to information security, some of which will be listed below:

- The US National Security Systems Committee defines information security as: The protection of information and its important elements, including the systems and devices that use, store and transmit this information. (Hadid & Mesos, 2016, p. 35)
- From an academic point of view, Information security is the science that deals with theories and strategies which provide protection for information from the risks that threaten it and from their activities. From a technical point of view, it is the means, tools and procedures

that must be provided to ensure the protection of information from internal and external risks. From a legal angle, information security is the subject of studies and measures to protect confidentiality, the integrity of the content and availability of information, and the fight against activities of abuse or exploitation of its systems in the commission of crimes. (Abdel-Latif Abdel-Karim & Al-Rubaie, 2013, p. 295)

- It means also all policies, procedures and technical tools that are used to protect the system from all forms of illegal use of resources such as theft, alteration and modification, damage to information or databases or intentional physical damage to devices in addition to the presence of other threats such as human errors, natural accidents and disasters. (Yahya Sharif, 2018, p. 53)

The previous definitions all indicate that information security is nothing but a set of procedures and measures taken by the institution in order to protect its information assets, by relying on technical means and tools to ensure its protection.

2.1.2. The objectives of information security:

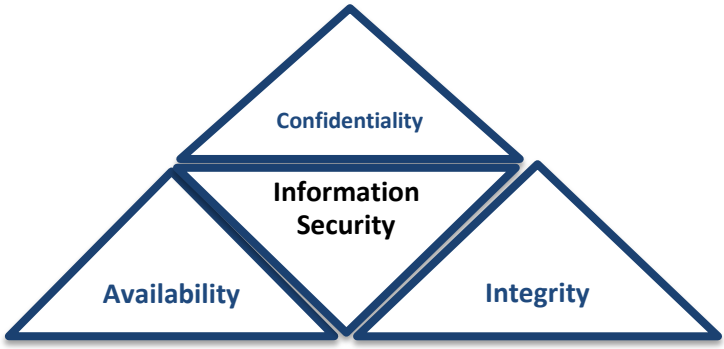
It is to develop, implement and maintain information which constitutes a large and increasing part of business cost; it also helps to ensure that organizations perform their operations effectively; therefore, the main objectives of information security can be summarized as follows (Bin Al-Tayeb, 2018, p. 37):

- Reducing the risks of interruption of the functioning of economic systems and institutions;
- Keeping the confidentiality of information;
- ensuring the integrity and reliability of information sources;
- ensuring availability of information sources and online operations without interruption;
- Guarantee comply to policies and laws related to security and privacy.

2.1.3. Security information basis:

In order to protect information security, it is necessary to provide a set of elements that must be taken into consideration. These elements are represented in what is known as the information security triangle:

Fig.1. CIA triangle.



Source: Prepared by the researcher.

These elements are (Hadid & Kribet, 2014, p. 198) :

- **Confidentiality:** it is protecting information from spreading in an unauthorized way, by preventing not allowed users from entering and accessing information sources. In order to ensure this, you must monitor access to information and encrypt it in order to increase its security and protection during the storage or transmission process, while providing authorized persons to view this information with decryption keys.
- **Integrity**: it focuses on keeping data clean and untainted, both when it's uploaded and when it's stored. This means making sure only those who are allowed to modify it, modify it.
- **Availability**: it means keeping data accessible**,** essentially when an authorized user needs to access data or information, they can. It can be sometimes confused with or even seem to contradict confidentiality.

2.2. Electronic attacks and Cybercrimes

The risks that threaten information security are numerous and have developed year after year as they keep pace with every innovative modern technology in the world of information and communication technology.

2.2.1. Types of electronic attacks:

Electronic attacks are those attacks that may occur to information within the electronic scope, such as information stored in a personal computer, the network or the server, and include various methods such as impersonation, unauthorized use, service obstruction, eavesdropping and malicious programs. The forms of attacks varied and took many ways and names

including (Hadid & Kraybit, Public Services in the Light of the Application of Electronic Management, 2017, p. 190):

- **Malware attack**: They are malicious programs that run away without the help of the computer user such as:
- **Viruses**: A malicious program that includes destructive targets for the contents of infected computers, characterized by its ability to copy itself.
- **The Ver worm**: A malicious program capable of multiplication and moving from one computer to another. Its goal is overcrowding the infected computer and slow network speed.
- **Macro program**: It is designed to work on a single application such as word or Excel.
- **Logic Bombs**: A program that infects the system and waits for an event (such as date, verbs, private data, etc.).
- **Trojan horse**: It is a program hidden in another program that performs malicious operations without the user's knowledge and takes control of the device. It works to steal passwords and sensitive information.
- **Spyware attack:** These are hidden programs that leak information and send it abroad via Internet.
- **Sniffing:** This technique relies on eavesdropping on transmitted data in the organization's network.
- **Service Denial**: physical damage to the server to prevent service provision.
- **Spamming:** This is to harm the system of electronic messages and to send them randomly.

- **The IP address spoofing method**: that is, replacing the sender's IP address with another address and thus breaking into the organization's network.

2.2.2. Effects of Cybercrimes:

The definition of information crime has evolved as it was linked to the development of information technologies. Therefore, we find that its definitions have developed moving from "computer misuse", to "computer fraud", "information crime", then "computer crimes", and "computer-related crime". Then "high-tech crimes" ,"hackers crimes" ,"internet crimes" ,and finally "cybercrime".

Many business owners get so busy that they forget about other important factors like cybercrime. If you haven't considered your company's cyber security needs, your business and customers could already be at risk.

In reality, there are many things you can do to stop cybercriminals from harming your company. By learning more about cybercrime's effects on business, you can also determine ways to prevent your company from becoming a victim. In 2017, the newsworthy Equifax data breach affected 147.9 million consumers. Mobile game producer Zynga was targeted by hackers in 2019, and the hack led to data breaches for 218 million users. These hacks gave cybercriminals access to Facebook IDs, emails, phone numbers, and other personal information (Desmet, 2021).

Cyber attacks like these can damage more than a company's brand image. Medical information, personal banking details, and much more can also be lost. With the Quest Diagnostics data breach in 2019, 11.9 million records were hacked. Today, cybercrime costs companies and individuals across the world more than 445 billion$ per year. Cybercrime effects on businesses play a big part in these numbers and continue to grow.

3. International information system security standards

To help organizations in managing their information security, many international standards have been developed, which are the minimum security controls recommended by information security experts.

3.1. What is the international standard ISO/IEC 27001:

Known as **ISO/IEC 27001**, it is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes.

Part of the **ISO 27000 series** of information security standards, ISO 27001 is a framework that helps organizations to establish, implement, operate, monitor, review, maintain and continually improve an ISMS. (Bernardino, 2021)

ISO/IEC 27001, is an information security management standard jointly-published by the International Organization for Standardization, and the International Electro technical Commission. ISO 27001, structures how businesses should manage risk associated with information security threats; including policies, procedures and staff training.

Defined within the ISO 27001 standard are information security guidelines, requirements intended to protect an organization's data assets from loss or unauthorized access and recognized means of demonstrating their commitment to information security management through certification.

ISO 27001, includes a risk assessment process, organizational structure, Information classification, Access control mechanisms, physical and

technical safeguards, Information security policies, procedures, monitoring and reporting guidelines. (Darby, 2005)

ISO 27001 has three main versions:

- **ISO 27001 :2005,** covers all types of organizations (eg commercial enterprises, public organizations, non-profit organizations). ISO/IEC 27001:2005 specifies requirements for establishing, implementing, operating, monitoring and reviewing, updating and improving a documented ISMS in the context of the overall risks related to the organization's activity. (ISO, Information security management systems, 2005)
- **ISO 27001 :2013,** its official title was: Information technology - Security techniques - Information security management systems - Requirements, specifies requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of an organization. It also includes requirements on the assessment and treatment of information security risks, adapted to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and intended to apply to any organization, regardless of its type, size and nature. It is not acceptable for an organization to waive any of the requirements specified in Clauses 4 to 10 when claiming conformity to ISO/IEC 27001:2013. (ISO O. T., 2013)

- **ISO 27001 :2017,** In practical terms, very little has changed between the 2013 and 2017 ISO 27001 information security standards except for a few minor cosmetic points and a small name change. The latest published version of the Information Security Management System standard is: BS EN ISO/IEC 27001: 2017. The ISO version of the standard (2013) was not affected by the 2017 publication and the changes do not introduce any new requirements.

3.2. ISO/IEC 27001 controls:

The Standard takes a risk-based approach to information security. This requires organizations to identify information security risks and select appropriate controls to tackle them. Those controls are outlined in Annex A of the Standard. There are 114 ISO 27001 Annex A controls, divided into 14 categories as it is shown below: (Bernardino, 2021)

- **Information security policies :** This annex is designed to make sure that policies are written and reviewed in line with the overall direction of the organization’s information security practices.

- **Organization of information security :** This annex covers the assignment of responsibilities for specific tasks.
- **Human resource security :** The objective of this Annex is to make sure that employees and contractors understand their responsibilities.
- **Asset management :** This annex concerns the way organisations identify information assets and define appropriate protection responsibilities.
- **Access control** : The aim of it to ensure that employees can only view information that's relevant to their job.
- **Cryptography**: This annex is about data encryption and the management of sensitive information. Its two controls ensure that organizations use cryptography effectively to protect data confidentiality, integrity and availability.
- **Physical and environmental security :** This annex addresses the organization's physical and environmental security. It's the most extensive annex in the Standard, containing 15 controls separated into two sections.
- **Operations security:** This annex ensures that information processing facilities are secure and is comprised of seven sections.
- **Communications security :** This annex concerns the way organisations protect the information in networks.
- **System acquisition, development and maintenance:** Its objective is to ensure that information security remains a central part of the organization's processes across the entire lifecycle.
- **Supplier relationships**: This annex concerns the contractual agreements organizations have with third parties.
- **Information security incident management :** This annex is about how to manage and report security incidents. This process involves identifying which employees should take responsibility for specific actions, thus ensuring a consistent and effective approach to the lifecycle of incidents and responses.
- **Information security aspects of business continuity management:** The aim of it is to create an effective system to manage business disruptions.
- **Compliance**: This annex ensures that organizations identify relevant laws and regulations. This helps them understand their legal and contractual requirements, mitigating the risk of non-compliance and the penalties that come with that.

3.3. ISO 27001/IEC benefits:

This standard can help to: (Darby, 2005)

- Protect everything from your organization's intellectual property to its confidential financial information;
- Put defined information security policies in place to help you manage processes including your access control policy, communications security, system acquisition, information security aspects of business continuity planning and many others;
- Make sure your information security incident management is carefully planned and demonstrably effective if and when a compromise happen;
- Perform risk assessment and management activities in a clear, practical and transparent way;
- Make sure key stakeholders and other third parties are aware of, in agreement with and where necessary fully compliant with your information security measures;
- Meet specific industry regulations or operating procedures, as set by any relevant regulatory bodies;
- Secure your employees' and customers' personal data.

3.4. Main steps to obtain an ISO 27001 certification:

The adoption of **ISO 27001** does not give its full effectiveness except by activating its basic principles, this project must take its place in the heart of information security management, or be adopted by the information system security administrator with the help of quality and risk management groups, but it must be supported by the administration. (Filali, 2021, p. 216)
This part explains how to obtain ISO 27001 certification and looks at the certification process as it is shown below: (Irwin, 2019)

- **Prepare:** by getting an understanding of ISO 27001, appointing an ISO 27001 champion and Securing senior management support.
- **Establish the context, scope, and objectives:** it is essential to pin down the project and ISMS objectives from the outset, including project costs and timeframe.
- **Establish a management framework:** this process include asserting accountability of the ISMS, a schedule of activities, and regular auditing to support a cycle of continuous improvement**.**
- **Conduct a risk assessment:** this implies that the process must be planned, and the data, analysis, and results must be recorded. Before conducting a risk assessment, you must establish your baseline security criteria.

- **Implement controls to mitigate risks:** once the relevant risks have been identified, the organization must decide whether to treat, tolerate, terminate, or transfer the risks. It is crucial to document all risk responses since the auditor will want to review them during the registration (certification) audit.
- **Conduct training**: the Standard requires that staff awareness programs be initiated to raise awareness about information security throughout the organization.
- **Review and update the required documentation:** documentation is required to support the necessary ISMS processes, policies, and procedures.
- **Measure, monitor, and review:** this requires that the performance of the ISMS be constantly analyzed and reviewed for effectiveness and compliance, in addition to identifying improvements to existing processes and controls.
- **Conduct an internal audit:** ISO/IEC 27001:2013 requires internal audits of the ISMS at planned intervals.
- **Registration/certification audits :** during the stage one, the auditor will assess whether your documentation meets the requirements of ISO 27001 and during stage two, he will conduct a thorough assessment to establish whether you comply with the ISO 27001 standard.

4. Information security in Algeria between the reality and Challenges

Knowing the reality of information security in Algeria requires focusing on various aspects, the legal and legislative side, the infrastructure and structures confronting cybercrimes and the necessity of adopting the standard ISO 27001 by Algerian institutions.

4.1. Information security within the framework of Algerian laws and legislation:

Due to the tremendous development of the computer that touched all fields and the adoption of legislative texts and laws that affected computer programs by the majority of countries, Algeria waited until 2003 to promulgate Order No. 05/03 related to copyright and related rights, which in its entirety, keeps pace with recent developments in the field of legislation in modern technologies through Articles 03 and 41 respectively, where the first of it allowed the introduction of computer programs within the framework of copyright-protected works, and the second one stipulates: ‘‘Not to reproduce in writing an entire book or a musical work in written form, not to reproduce databases in digital form, and not to reproduce

computer programs except in the cases stipulated in Article 52 of this order." (Boufes & Talhi, 30 April 2014, p. 13)

The Algerian legislator has criminalized acts committed against computer systems, as a result of the information revolution's production of new forms of criminality. This pushed the Algerian legislator to Amend Law under the Penal Code dated in 10 November, 2004 supplementing Ordinance No. 1566, which includes the Penal Code under the title "Aggression to automated data processing systems," as this section includes eight articles (394- to 394 bis 7), The legislator introduced another amendment in 2006 to the Penal Code under Law No. 2306 of December 20, 2006, where this amendment touched the seventh bis section related to crimes against automated data processing systems, and the penalties for these acts were tightened, this amendment came due to the increased awareness of this new type of crimes. (Akili, 25 March 2017, p. 14)

However, this law contained many legal vacuums due to dealing with electronic crime in a traditional way, but this led to the promulgation of an independent Law No. 04-05 dated August 5, 2009 [containing 19 articles divided into six chapters, deriving its provisions from the international conventions], in particular, the 2001 Budapest Convention on Information Crimes. (Bediaf & Hamrani, 2020, p. 181), it includes special rules for the prevention and control of crimes related to information and communication technologies; Where the Algerian legislator created procedural rules that fit the nature of the information crime, such as expedited retention of data, information inspection, monitoring of electronic communications and other precautionary and procedural measures.

After that, Algerian legislator passed new laws such as: (Ben karra, January 2021, p. 34)

- Law No. 15-04 of February 1, 2015 laying down the general rules relating to electronic signature and certification;
- Executive Decree No. 16-142 dated May 5, 2016, specifying the methods of preserving the electronically signed document;
- Law No. 18-04 of May 10, 2018, laying down the general rules relating to postal and electronic communications;
- Law No. 18-05 of May 10, 2018, relating to electronic commerce;
- Law No. 18-07 of June 1, 2018, relating to the protection of persons in the field of data processing of a personal nature, with the aim of protecting the confidentiality and privacy of data.

In 2020, in the Official journal, a decree was passed related to the establishment of a national system for the information systems security to

undertake the preparation of a comprehensive strategy in this field, with digital investigations conducted in the event of cyber attacks targeting national institutions.

4.2. Statistics on cybercrimes in Algeria

Cybercrime targets victims from individuals to large companies, through various methods such as phishing and illicit installation of malware. This leads to loss of income, damage to reputation, financial losses and encrypting data with viruses that can only be processed by paying money to hackers.

The rate of financial losses as a result of cybercrimes in many cases exceeds the same rate in traditional crime, due to the large amount of high financial value information that are programmed automatically, which can be manipulated in a few seconds and transferred from one person to another.

According to the Police Magazine, 2130 cybercrimes were handled, including 1570 cases during 2017, and the same source indicated that the number of resolved cases represents a success rate of 73.71%, as 2101 people were arrested, including 2026 adults and 75 minors, also 2704 victims of crimes related to computer media were registered, including 2300 adults and 188 minors. The crimes of extortion via the Internet amounted 47 cases, most of them related to fake offers to obtain money. The judicial police services also dealt with 28 cases of assault on information systems, e-mail and websites for institutions and individuals, which claimed 45, including 26 moral persons. (www.Radioalgerie.dz, 2018)

Although the majority of criminals have very simple technical capabilities, digital attacks are witnessing an increasing use of advanced tools available in the virtual criminal market on the Internet. As some criminal groups develop their activities, cybercrime is also developing and growing rapidly.

Kaspersky Company, which is specialized in combating cybercrime, thwarted 95,000 electronic attacks against Algeria during the year 2020, as the year 2018 ranked first in the Arab world and the 14th globally in terms of countries most vulnerable to electronic attacks. (Bachouch, 2021)

The Algerian security services recorded a significant increase in the number of crimes, according to different patterns, during 2020. While presenting the annual outcome of the activities of the judicial police, the Director of the Judicial Police, Haj Said Arezki, revealed that the number of registered cases related to various types of crime reached 258171 cases for the year,

in cybercrime, 5163 cases were registered, after 4210 cases in 2019. These crimes relate to harming people and information systems, fraud, and information terrorism. (Algerian News, 2021)

Dr. Bashir Bouijra Abdel-Razzaq, the youngest researcher specializing in cybersecurity nationally, and the first Arab Muslim to obtain 36 internationally recognized certificates in this field, the highest of which was the Cisco Systems American Award for "the highest quality trainer in the world." claimed that Algeria lacks a clear vision, strategies, accurate plans, and practical programs that aim to provide information security and raise its level for individuals and institutions, especially as we are on the verge of digitizing many sectors and in a period where cyber dangers are surrounding us from all sides. it threatens the security of information and hence the security of the state and the security of its institutions and individuals, and perhaps the biggest evidence is the attack on the website of the National Agency for the Valuation of Hydrocarbon Resources recently by "foreign hackers", which warns that what is coming is more dangerous than we imagine. (Khmissa, 2020)

4.3. Algerian efforts to adopt Information Security in institutions

The establishment of the National Institute for Standardization is one of the manifestations of the Algerian state's interest in the need to adopt international standards and keep pace with economic developments to protect its institutions.

The Algerian Institute of Standardization **(IANOR)** is an official national body representing the state in the International Standards Organization, its tasks include in particular: (www.iso.org, 2021)

- to ensure the development of national standards in coordination with the other sectors;
- to identify national standardization needs;
- to ensure the implementation of the national standardization plan;
- to ensure the dissemination of information on standardization and related activities;
- to manage the national information point on Technical Barriers to Trade of the World Trade Organization (WTO);
- to manage the mark of conformity to Algerian standards.

The Director-General of the Algerian Institute for Standardization, Jamel Hales, confirmed that the institute had prepared, until November 30, 2021, about 662 national standards, including 339 new standards and 283 revised standards. He added that, Algeria had a set of 10744 Algerian standards, including 1094 basic standards, 2060 in chemistry and petro chemistry, 1608 in food industry, 1569 in electro-technology, and 2232 in mines, iron

and mechanics sector and 1123 standards in building materials and **1058** in Health, **Security** and Environment sector.

In 2022, the Institute also seeks to initiate new work in order to take care of national normative needs, and to organize 300 meetings of technical committees in order to embody the national standardization program. He affirmed also that the national authority intends to create 750 Algerian standards during the next year. (Algerian press service, 2021)

In Algeria, there is still a clear absence of information security adoption as an important element in the development of national institutions, as the number of qualified institutions according to the ISO 9001 quality management system standard in Algeria does not exceed about 1000 institutions out of 300 thousand institutions active in the national economy. It is also indicated that no Algerian institutions obtained ISO 27001 certificate, while the most important certificates sought by Algerian institutions revolved around the ISO 9001 certificate for the application of quality systems, ISO 14001 related to environmental systems, ISO 22000 related to food safety, ISO 18001 related to occupational health and safety. (Boufes & Talhi, 30 April 2014, p. 13)

In an investigation led by the Algerian Association for the Security of Information Systems **(AASSI)** in 2015 on a group of Algerian institutions about information systems, the following conclusions were reached: (Filali, The level of information security in the Algerian organization and the extent to which it is affected by the nature of threats and the nature of the protection applied, 2019, p. 9)

- 1% of Algerian institutions use ISO 27001 information security standard;
- 7,5 % do not have IT compliance procedures;
- 1/10 do not have activity resume plan;
- 1% have a bridge gaps management policy.

According to the International Information Security Report, which included a study on information security in 194 countries, in which a set of pillars for measuring information security were identified, including legislation, techniques, regulations and cooperation, Algeria was ranked among 77 countries in the category of medium countries in terms of information security, where it ranked 67th globally and ninth in Arab world. According to the report, it has achieved a low degree in terms of structures and mechanisms to confront accidents and emergencies related to information security. (Bediaf & Hamrani, 2020, p. 188)

5. Conclusion

Through this study, we tried to sensitize Algerian institutions to the need to adopt standards for information security because of their direct positive impacts on reducing the risks of interruption of the functioning of economic systems and keeping the confidentiality of information, ensuring the integrity and reliability of information sources and ensuring availability of information sources and online operations without interruption. Also the need to improve Algerian laws and legislation that are related to information security and especially in light of an environment with interconnected and fast-paced business, which increases the volume of threats and risks. It is necessary to strive to confront these dangers and to develop the necessary technical methods and means for this confrontation.

We came up with a set of recommendations that we can summarize as follows:

- Enacting a stand-alone law on cybercrime with an emphasis on its implementation on the ground;
- Striving to obtain ISO 27001 standard, as it is the best application for the security of information systems in organizations and attracting support staff specialized internally and externally in information security to supervise this aspect.
- Awareness of the dangers of cybercrime through media campaigns and the inclusion of specialties in the field of information security in Algerian universities;
- Establishing mechanisms to deal with accidents and emergencies in the field of information security by forming centers and teams for immediate response that work seriously.

6. References

1. Abdel-Latif Abdel-Karim, N., & Al-Rubaie, K. H. (2013). Information Security and Confidentiality and its Impact on Competitive Performance, An Applied Study in the Iraqi General Insurance Companies and Al-Hamra National Insurance. *Journal of Accounting and Financial Studies, Volume 8, No. 23, University of Baghdad, Iraq*, 295.
2. Akili, F. (25 March 2017). Cybercrime and its Confrontation through Algerian Legislation. *Fourteenth International Conference on Cybercrime.*
3. Algerian News, a. (2021). Récupéré sur https://www.alaraby.co.uk/society
4. Algerian press service. (2021, 12 20). *National Standardization Day: Preparing 662 national standards in 2021*. Consulté le 12 23, 2021, sur aps.dz: https://www.aps.dz/ar/economie/118496-662-2021
5. Bachouch, N. (2021, 11 23). *Cybercrime.. terrifying numbers*. Consulté le 12 12, 2021, sur https://www.echoroukonline.com

6. Bediaf, s., & Hamrani, A. (2020). Information security in Algeria. *Algerian journal for security and development, Issue16*, 177-190.
7. Ben karra, a. (January 2021). A strategy to achieve information security for e-government in Algeria. *Comprehensive International Conference on Theoretical Issues and Their Operational Solution Methods.* Dar Arafid for production.
8. Bernardino, R. (2021, 01 02). *ISO 27001:2013 ISMS implementation and certification.* University of Liverpool: Research Publications.
9. Bin Al-Tayeb, I. (2018, March). The Importance of Information Systems Security for Modern Economic Institutions. *Journal of Development and Applied Economics, Al-Masila University, Issue 3*.
10. Boufes, c., & Talhi, f. z. (30 April 2014). Towards building ISO27001 information protection management systems in Algerian institutions. *The Second International Conference on Economic Intelligence on:Strategic vigilance and information systems in the economic enterprise.* Annaba, Algeria.
11. Darby, M. (2005). *ISMS.online*. Consulté le 12 23, 2021, sur https://www.isms.online: https://www.isms.online/iso-27001/
12. Desmet, N. (2021, 02 17). *Cybercrime Effects on Business: Why You Should Care*. Consulté le 12 12, 2021, sur https://www.linkedin.com/: https://www.linkedin.com/pulse/cybercrime-effects-business-why-you-should-care-nils-desmet
13. Filali, A. (2019, 06 20). The level of information security in the Algerian organization and the extent to which it is affected by the nature of threats and the nature of the protection applied. *Phd Thesis*. University of Tlemcen, Algeria.
14. Filali, A. (2021). The role of ISO/IEC 27001 in raising the credibility of the ISMS in the organization. *Economic additions journal, Volume 5, Issue 5*, 204-223.
15. Hadid, N., & Kraybit, H. (2017). Public Services in the Light of the Application of Electronic Management. *Foundation Journal, Issue 6, University of Algiers*.
16. Hadid, N., & Kribet, H. (2014). nformation Security and its Role in Confronting Electronic Attacks on the Institution's Information System,. *The Foundation's Journal, No. 3, University of Algiers 3*.
17. Hadid, N., & Mesos, K. (2016). Approaches to protecting the organization's information systems from electronic attacks. *Foundation magazine, University of Algiers 3, No. 5*, 35.
18. Irwin, L. (2019, 03 13). ISO 27001 Certification: 10 Easy Steps. USA: IT Governance.
19. ISO, O. T. (2005, 10). *Information security management systems*. Consulté le 12 23, 2021, sur https://www.iso.org: https://www.iso.org/fr/standard/42103.html
20. ISO, O. T. (2013, 10). *www.iso.org*. Consulté le 12 23, 2021, sur https://www.iso.org: https://www.iso.org/fr/standard/54534.html
21. Khmissa, m. (2020, 12 19). *Algeria should adopt a national project for information security*. Consulté le 12 13, 2021, sur https://elwassat.dz/
22. www.iso.org. (2021, 12 23).
23. www.Radioalgerie.dz. (2018).
24. Yahya Sharif, H. (2018). The impact of the information system on strategic vigilance in small and medium enterprises, a field study on some Algerian enterprises. *PhD thesis in economic sciences*. Algeria: Farhat Abbas Setif University 1.