Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/15698
DOI URL: http://dx.doi.org/10.21474/IJAR01/15698

RESEARCH ARTICLE

INFORMATION SECURITY FUNDAMENTALS APPLIED TO THE DEVELOPMENT OF SYSTEMS

Maída Da Silva Aparício, Marcelo Dos Anjos Caldas and Jaqueline Silva De Souza Pinheiro

Manuscript Info

Manuscript History
Received: 15 September 2022
Final Accepted: 19 October 2022
Published: November 2022

Key words:-
Information Security, Developer, System, Vulnerabilities, Development

Abstract

This article aims to analyze the commitment of developers to the use of information security fundamentals for the development of systems and understand whetherthese professionals understand the importance that and ste theme has today for data protection. Seeking to achieve this purpose, a bibliographic review on the subject was first carried out in several sources to have a good data collection to base this article, and later a searchwas conducted through a questionnaire in Google Forms. The research came to help in understanding the use and implementation of security tools in development. One relevant fact that was acquired by the research is that many programmers understand about the importance of security in system development, however, some do not know how to use them or use them, but do not know how it actually works.

Introduction:-

Com the technological advance diversas areas of technology have had a rise, on the other hand, the growth of the area of information security has not accompanied this evolution so that, currently Brazil has been a country very targeted in question of hacker attacks, every yearthis number only increases, in 2021 according to the Report of Online Criminal Activity in Brazil was counted more than 2.8 billion sensitive data exposed, in view of this it is possible to note that the scope of information security is not yet in parallel with the other areas thus resulting in unprotected and flawed systems.

These events almost always come from the exploitation of vulnerabilities that are present in the system, thus resulting in the breaking of the pillars of security, and toensure this security is necessary to have the support of three pillars: availability, integrity and confidentiality, which together perform an essential work for information security.

Nowadays depending on which system the user uses it is common that at the time of registration are requested data such as e-mail, full name, phone number, date of birth and even identification documents. Only with email and full name obtained by a hacker can already be used lightly, as well as phishing cybercrime, which obtains data and user information through email messages and unscrupulous tactics.

From the reflection of data leaks and the large number of vulnerabilities existing in systems, the difficulty in implementing data security at the time of development is quite remarkable.

Unfortunately many companies do not invest in the area of information security because they aim as a high cost and no return. And the result of this decision is only reviewed after an attack, which data is leaked and unfortunately the cost is much more expensive.

Corresponding Author:- Maída Da Silva Aparício

Therefore, faced with the need to better understand the commitment of developers to information security in the design of softwares and systems, this research aims to analyze the adoption of tools, information security instruments and the difficulties of implementing them.

Theoretical Reference

The theoretical framework of this research was structured in three topics: Information Security; Vulnerability and its potential impact and tools on development.

Information Security

Information has power,so much so that in active days it is one of the most important assets of individuals or business, according to the NBR ISO/IEC 27002 standard (ABNT, 2022), "information is an important asset for the business. By assigning value to the company, the information needs to be adequately protected."

And toensure this necessary protection has developed information security which is a way to ensure the protection of information from existing threats and vulnerabilities through standards, security policies and good practices.

In the definition of Semola (2014), "information security is an area of knowledge dedicated to the protection of information assets against unauthorized access, improper changes or its unavailability."

In the process of being considered protected, it isnecessary that it is based on three basic pillars and the best known information security pillars. integrity, ensuring that the information is not unduly altered in the system life process. Confidentiality, ensuring that data is accessedonly by persons, entities or processes duly authorized. Finally, availability states that the information will be available and secure to be accessed by authorized persons whenever necessary.

Usually, the security of theinf ormation is formed by the three most well-known pillars, but over the years in order to increase the security of information, two new pillars began to integrate. authenticity, ensuring that there is the veracity of the information and who generates it. And the irretraction or non-repudiation, making sure not to let the author deny such information that he manipulated.

For NBR ISO/IEC 27002 (ABNT, 2022) the pillars of Information Security are defined as:

1. **Confidential of** - property that limits access to information only to legitimate entities, that is, those authorized by the owner of the information.
2. **Integrity** - property that ensures that the manipulated information maintains all the characteristics establishedby the owner of the information, including change control and warranty of its life cycle (birth, maintenance and destruction).
3. **Availability** - property that ensures that the information is always available for legitimate use, that is, by those users authorized by the owner of the information.
4. Authenticity - property that ensures that the information comes from the advertised source and that it has not been the subject of mutations throughout a process.
5. **Irretraction** - property that guarantees the impossibility of denying authorship in relation to a previously made transaction.

Vulnerability And Its Potential Impact

We all know what a vulnerability is, but in the world of Information Technology (IT) it has a specific meaning. In terms of vocabulary, a vulnerable thing is something that is sensitive to certain threats. And in the IT business, a vulnerability is something that allows an attack or is associated with a specific risk.

According to Semola (2014), vulnerabilities are "weaknesses present or associated with assets that manipulate and/or process information that, when exploited by threats, allows the occurrence of a security incident, negatively affecting one or more principles ofinformation security". Semola (2014) also defines threats as "agents or conditions that cause incidents that compromise information and its assets, through the exploitation of vulnerabilities, causing loss of confidentiality, integratingdata and availability and, consequently, causing impacts on an organization's business".

Together with vulnerability is to threats, which is a situation in which an internal or external agent accidentally or purposely exploits a vulnerableage, causing negative impacts on a system or resource.

And with all this comes the risk, which refers to the potential associated with the exploitation of vulnerabilities, that is, is what is at stake in terms of economic assets, resulting in an impact for the organization, such as malfunction, theft of information, among other consequences.

Main causes of vulnerabilities in information security. They come from most failures and security holes, can be identified previously bya rigorous analysis.

Among the causes that can be identified by a previously trained employee are human failures in risky situations, such as clicking suspicious links or downloading undue documents.

Other factors are failures in systems and programs. Originally arisingfrom problems in software development, poor configuration, maintenance and updating of programs.

All of these issues can leave loopholes to intrusions and compromise information security.

Tools In Development

Theuse of security tools increases protection and ensures that best market practices are incorporated into system development.

According to Nova 8 Cybersecurity (2019), "Those responsible for the security of a project need to ensure that there is a framework to incorporate security practices into the entire system development process, including code for the creation of the solution, configuration, and deployment of the infrastructure on which the application or service will beexecuted."

The company adds, "Improper application of security tools is one of the main security risks in system development. If development teams cut and paste existing code samples on the web, without reading the security implications the problem will be worse."

The use of some frameworks is widely used to help with development, and has some that also help in security. The following are some of the key frameworks that are applied with security items in system development in the relevant programming languages:

- **Spring** Security is a Spring project framework with an advanced, highly customizable authentication and authorization system forJava applications. This framework is even the official solution for implementing security features in Spring Boot applications, but it can also be used in combination with other frameworks. While Spring Security focuses on authentication and authorizationsystems, it has other features that can improve the security of our Java applications, here are some of its key features: Authentication System; Authorization system; Session fixing, clickjacking and off-site request snare protection; integration with Servlet API; optional integration with Spring Web MVC; easy installation via Spring starter.
- **Django** is a high-level Python web framework for rapid development of secure and easy-to-maintainwebsites. It does most of the web development work, so you can focus on writing applications without reinventing the wheel. It can be used with any client structure. Django provides a secure way to manage user accounts and their passwords, avoiding common errors such as placing session information on vulnerable cookies or storing passwords directly instead of hashing. The password hash is created by sending a fixed-length value to enter a password through a cryptographic hash function. By default, Django has protection against many enabled vulnerabilities, including SQL injection, site-to-site scripting, site-to-site spoofing , and clickjacking.
- **Laravel** is a FRAMEWORk PHP for web development that uses the MVC architecture to facilitate the rapid development of secure and executable applications with clean and concise code, as it encourages the use of good programming practices and uses the PSR-2 standard (an acronymfor PHP Standards Recommendations) as a style guide for coding. Laravel provides a code model for this that ensures maximum security for user authentication. You can integrate with email services (with out-of-the-box caching tools such as Memcached and Redis) and also fix the most common technical vulnerabilities in the early stages of the project. Laravel also has eloquent, its orm (object-relational mapping) pattern. It simplifies and allows developers to program

applications without having to write pure SQL code directly into the code to interact with the database through these classes.

- **AdonisJS** is a powerful framework with a complete library to make life easier forNode senvolvers.js without using additional features. It has several out-of-the-box features such as ORM, authentication, verification, email, registration, and more. It is a back-end structure for Node.js. It's written in TypeScript. In this way, the application to be created will also be in TypeScript. Some advantages: CLI facilitates application scaffolding ; it deals with the structure of websockets (real time); ORM works with SQL.
- There are many other types of frameworks that have not been mentioned, the ones mentioned above are some of the ones we use in quantitative research to base the article.

Methodology:-

The main basis of the study was exploratory bibliographic research in articles, books and monographs published in an academic search site, with the intention of broadeningthe view on the research theme, observing how the authors deal with the issue of the use of safety fundamentals in the development of systems. On top of that, each author has a different way of advocating the use of the security of information, focusing on different vulnerabilities, arguing about tools that claim to be effective to be used in development. All of these topics are vital for a programmer to develop a system in a way that is right for the user.

The other main basis to support the article was the elaboration of a quantitative research with development professionals through the Google Forms tool that consisted of a questionnaire with questions pertinent to the problem of the article. The form was sent by social networks, and the same resulted in a very broad and apro viewfounded on the subject. Questions such as how much the developer considers Information Security an important topic to be studied, whether he has the knowledge of how and what tools to use to perform the protection of user data, were performed in the form to be able to better understand the view of the developer in the face of security.

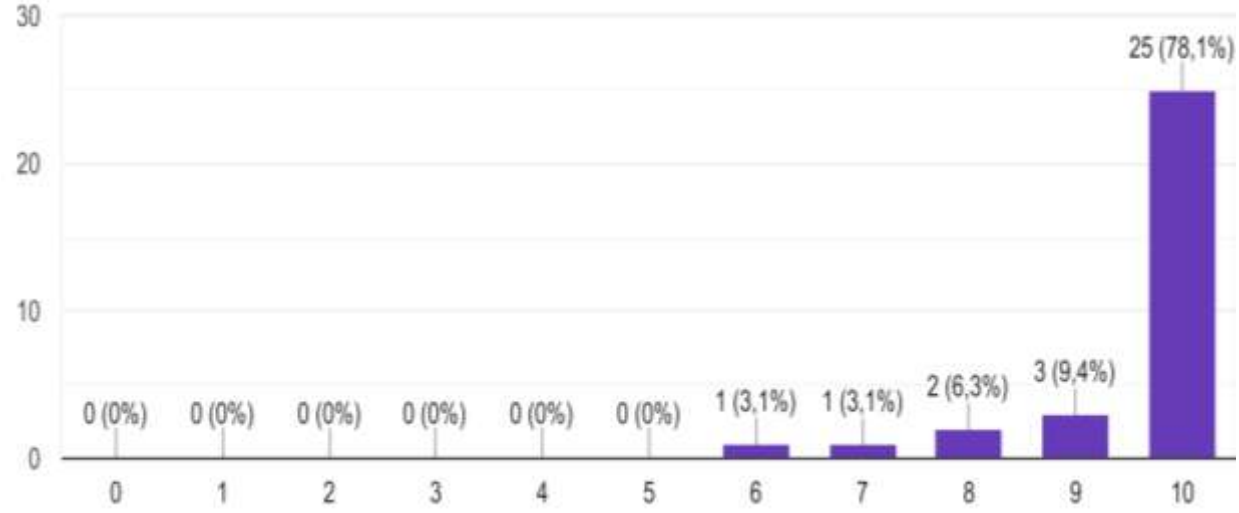
Soon after having the results of this research, we performed an analysis of the data in order to be able to have some conclusions that will be further on.

Results:-

Today, with the lack of commitment of developers to security, has caused a large wave of data leaks caused by existing vulnerabilities in the system. Since if there is a good application of security at the time of development it would already be a means of reducing these incidents that may be a problem later.

An analysis of the search results was performed with a sample of 32 IT professionals who were willing to answer thequestionnaire through the Google Forms tool, where the data were processed and will be shown below.

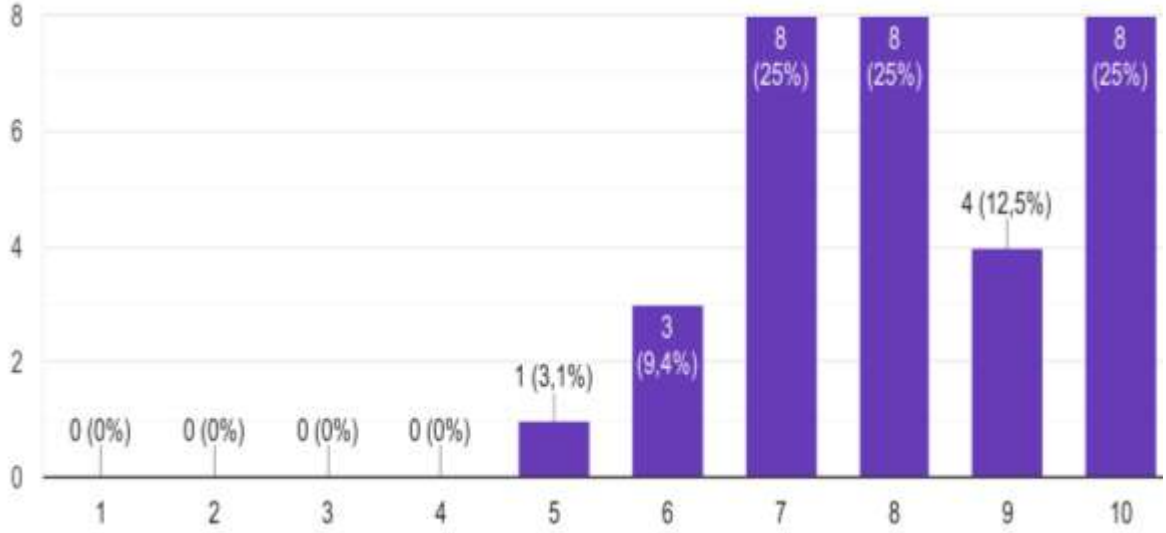
Figure 1:- How much do you think information security is an important topic to be studied?



Source: Own Authorship (2022).

Analyzing graph 1, it is noted that most of the individuals who responded to the survey consider Information Security a pertinent theme to be studied and with a very significant percentage, 78.1% shows that most people have a concern in trying to understand and learn more about this subject.

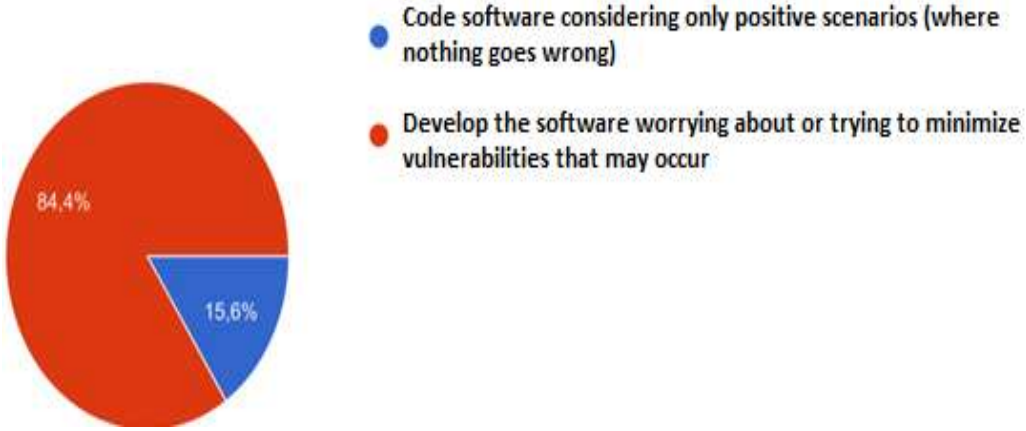
Graph 2:- Do you understand Information Security and how to protectusers' data?



Source: Own Authorship (2022).

Good development security begins when the developer himself realizes that he needs tools and studies on the subject to improve the system and consequently ends upprotecting the users' data. Graph 2 shows that there is an impartiality between the results where 3 responses with the same percentage were obtained, which exposes a difference with the previous graph and also shows that many of the individuals who used securityas an important topic, unfortunately do not know how to use the tools so to implement in the system.

Graph 3:- Choose the alternative that identifies the most.

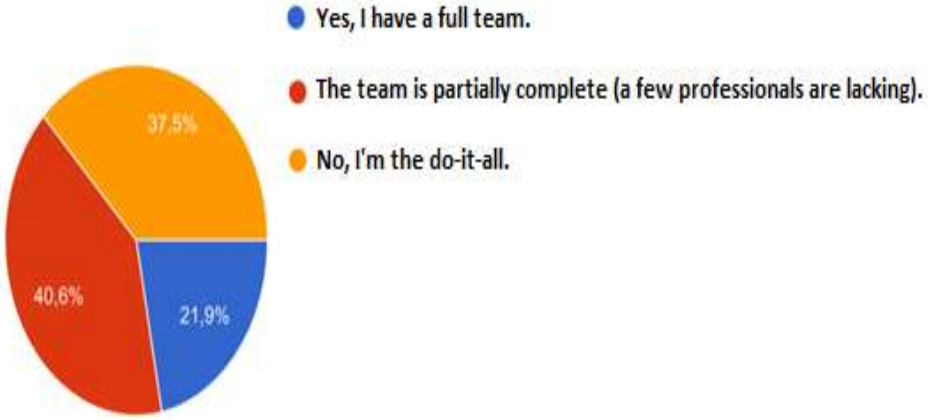


Source: Own Authorship (2022).

Another cause of vulnerabilities in the system may be naïve coding, where the programmer considers only positive scenarios of execution of his code, the development of a system in these conditions can lead to various problems, such as the case of malicious users who can try to find faults and exploit them and several other bottlenecks.

Graph 3 asked a question with this problem and it resulted that most of the people who responded develop the system worrying about or trying to minimize existing vulnerabilities, which shows that many do not use a superficial coding but rather a programming that cares about the well-being of the system.

Graph 4:- Do you have a development team?



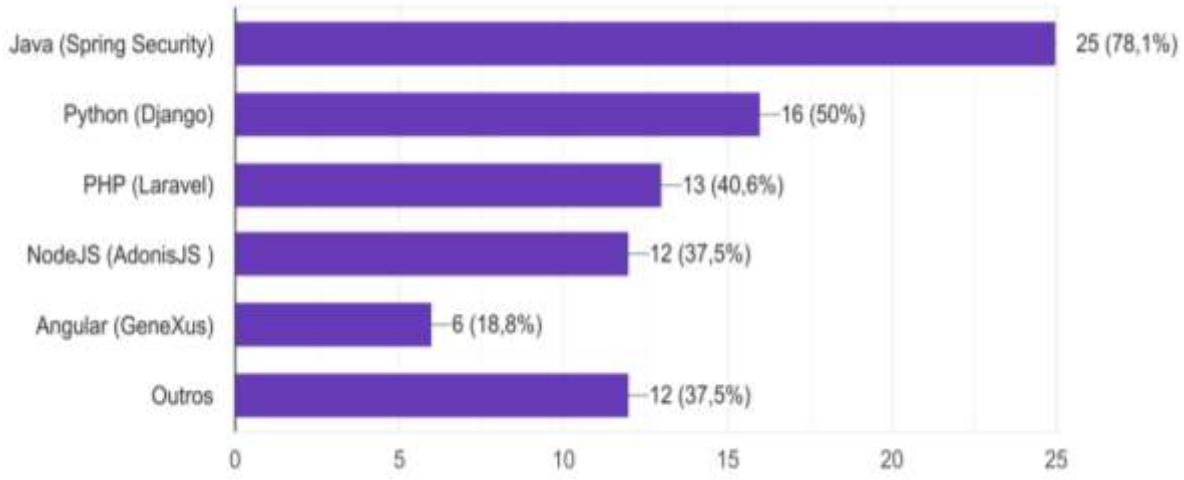
Source: Autoria own (2022).

As much as the developer uses in any way to code a secure system it is very rare for the software to terminate without existing vulnerabilities, since the programmer is a single person and many times it overloads itself with tasksto be performed and consequently can go unnoticed some failure.

The correct thing would be that this developer was part of an IT team, where several professionals in the area are part, such as analysts, programmers, designers, software testers, where the latter can greatly help in the issue of bugs and vulnerabilities, since it works to ensure the correct functioning of programs and review the requirements of the system.

Thinking about this theme was askedin the formulary if the individual was part of a development team and was obtained as a response the data that are in graph 4, in which it is observed that mostly with 40.6% the developer is part of a group, but it is not complete, soon after, 37.5% are not part of any team and do everything alone. It can be seen that the vast majority of programmers are not overwhelmed in performing all the tasks of the development process in a solitary way, on the other hand the second higher perception shows the opposite, where, many of the individuals work in a unique way, where he is the famous "does everything", and the programmer may feel tired and consequently not performed his work correctly.

Figure 5:- Have you studied orused any of these tools?

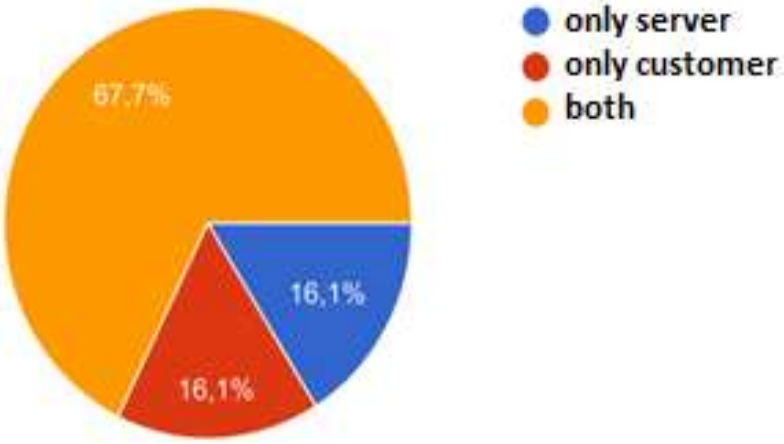


Source: Own Authorship (2022).

To help implement software security, the developer can use some frameworks that are able to help in this process. And in graph 5 it was asked in the form if people use or have already studied some of the frameworks presented and it was obtained as a result that most people use Spring Security which has as main function to help in the process of

authentication and advanced authorization for Java aplicativos. The second most used framework based on research was Django which assists in the process of safe development of web sites for Python applications.

Graph 6:- Develops verification and validation rules in table (server) fields and form (client) controls?



Source: Own Authorship (2022).

A very simple way to make use of security for users is to use a validation rule that is a way to restrict the way a field is entered into the table or form, thereby having greater control of the information that will be stored in the system. In graph 6, a question related to this topic was asked, whether the developer performs validation and verification rules only for user, server or even for both, and it was obtained as a result that in the large casevalidation is done for both cases with 67.7% of the search, which presents a great importance in how the input data is being treated so that information is not accepted in any way.

Many programming professionalsknow the importance of information security, but many unfortunately do not know how to use them correctly, which consequently causes in software that can have many flaws. And with the increasing frequency of attacks issued against theactions, security problems in systems have become something routine.

Discussion:-

Itis logical that over time the systems are increasingly willing to fail and consequently by the mercy of invaders. There are several factors that can cause so many vulnerabilities, but the lack of understanding of the tools, or even the demand to develop a system in the fastest way can generate these failures.

Unfortunately many programmers can even use security tools, but do not know how it really works, use only by use, or cut pieces of code from other systems and suit their own, and there is no study of how those lines of code act in your software.

It was analyzed in the results of the research that many professionals know or use security frameworks, the most used were Spring Security, Django, Laravel and Adonis JS, and each structure presented exposes that the code makers use them or are curious to knowthem.

It was observed in the results of the research the concern of developers with information security, however, many of them do not know how to apply in the systems, and how it is missing an IT team at this time, even more that the team is there for all together to develop a good system where each professional has its specific role, and it is not the developer alone performed all the tasks, and the correct would be this scenario where everyone participates in some group and generate a secure software, however, the reality for many other programmers unfortunately is totally the opposite.

Final Considerations

Withthe large amount of data and information traveling in the systems, the minimum oversight can generate a major problem for both the softwareand the users who will be the most harmed.

Whether the developer or a development company needs to understand the great importance and growth of Information Security today, and start adopting some basic concepts of this branch in their carreiras, it is not only a point for the programmer to code lines of code quickly and easily if it is not minimizing problems that may appear in the future and companies that offer development services also need to be aware to this issue, since, often unfortunately is only taken seriously this topic when the system has data leaks and sadly, it will be too late to try to correct the error, and this failure will only serve to increase the statistics of Brazil as one of the countries most targeted in hacker attacks. The cost of this error will be much more expensive than just becoming aware, studying and trying to understand more about the tools that can be used to minimize system failures or have an IT team where each professional has their task to fulfill.

Many developers need to understand that Information Security alone cannot solve any problem, it is not enough just to think about how to protect the data, if the suficiente is not epowered to perform such a function at the time of encoding.

It is incorrect to say that only the developer can change the current scenario of failures in Brazil, since information security is only complete through various procedures. Lyra (2015)emphasizes that information security is achieved "by implementing a set of appropriate controls that includes policies, processes, procedures, organizational structures, and software and hardware functions", but with the correct implementation in the development, it already assists in minimizing many problems that can affect data protection.

If each process is carried out with excellence the system will not be in trouble in the future.

Therefore, to generate a secure system the development professional needs in addition to knowing how to program the lines of code, also know the fundamentals and security tools and that mainly know how to use them and apply them at the time of the development of the system, so that it provides maximum mitigation of failures, thus ensuring that it will not have the commitment of any of the pillars of information security and consequently also ensuring that the users' data will be saved.

Bibliographic Reference:-

1. Axur. Report of online criminal activity in Brazil. Available in:<https://conteudo.axur.com/pt-br/atividade-criminosa-online-brasil-2021>. Accessed: Aug. 28. 2022.
2. Esx. Framework and its 12 security practices. Available from: https:<//www.esx.com.br/blog/security-development-lifecycle-framework-e-suas-12-práticas-de-segurança/>. Access: Oct. 2 2022.
3. ISO 17799. ABNT NBR ISO/IEC 17799:2005 - Information Technology - Securitytechniques - Code of Practice for Information Security Management. Brazilian Association of Technical Standards - Rio de Janeiro: ABNT, 2005.
4. LYRA, Maurício R. Information Security Governance. 1 ed. Brasilia: Kindle, 2015. Electronic book.
5. New 8 Cybersecurity.Tip those of security tools essential for the development of systems. Available from: https:<//www.nova8.com.br/2019/09/tipos-de-ferramentas-de-seguranca-essenciais-para-o-desenvolvimento-de-sistemas/>. Access: Oct. 5. 2022.
6. Semola, Mark. InformationSecurity Agency: An Executive Vision - 2 ed. São Paulo: Elsevier, 2014.
7. Solutions. Pillars of Information Security. Available in <https://addit.com.br/pilares-da-security/>. Access: Sep 03. 2022.