Computer security and audits as a measure to protect our information

William Elvis Alarcon Cotrina[1] [0000-0003-1615-2933], Modesto Emerson Delgado Canales[2] [0000-0001-7541-4521], Enrique Michael Gutiérrez Mariño[3] [0000-0001-6870-8441], Diego Andres Crespo Buquich[4] [0000-0002-4550-4208] and José Antonio Ogosi Auqui[5] [0000-0002-4708-610X]

[1] Universidad Privada San Juan Bautista, Lima, Peru william.alarcon@upsjb.edu.pe
[2] Universidad Privada San Juan Bautista, Lima, Peru, modesto.delgado@upsjb.edu.pe
[3] Universidad Privada San Juan Bautista, Lima, Peru, enriquem.gutierrez@upsjb.edu.pe
[4] Universidad Privada San Juan Bautista, Lima, Peru, diego.crespo@upsjb.edu.pe
[5] Universidad Privada San Juan Bautista, Lima, Perú, jose.ogosi@upsjb.edu.pe

Abstract. With the development of this article we want to present the information in a more detailed and concise way on the subject of computer security and the auditorias in such a way, it is easy to enterintoany public that stumbles upon our article. For its development, a compilation of information was made from different articles, books and research on the subject of computer security and auditing. A proposal was made of what are the phases or the essential procedure to carry out an audit in a correct way that will help the people who are starting with the audits.

Keywords: Computer Security, Computer Crimes, Cybersecurity, Auditing.

1 Introduction

The drastic changes that have occurred in the modern world, due to incessant development, accelerated globalization, the importance that the high volume of infor-mation and the systems that provide it now have, the vulnerability of access to that information, such as cyber threats, the level and costs of current and future invest-ments in information and in the development of information systems and the poten-tial that ICTs have for drastically change a company and its business model.

Technology has become indispensable in our daily lives, since most people interact with it at every moment. Electronic devices have been considered harmless, but they can cause injuries or serious damage depending on the way they are used, since the tendency is for everything to become "smart"; however, they are still machines that can fail at the least expected time.

The communication and interaction between devices has been a great technologi-cal advance, but as a counterpart it has opened the possibility to people with antiso-cial behaviors that for malicious purposes harm other users through access to their

information, as a result it has caused losses, alteration of data and attacks against functional hardware and end users suffer because they do not have the necessary knowledge about the risks to which they are exposed when someone is connected to the internet or has access to your important information or resources in some way.

Most people who are immersed in the computer world do not know the magnitude of problems that are had with respect to security and generally do not have ways that make it easier for people to investigate this aspect, they do not have enough knowledge to mitigate this evil; so the way to handle it is reactive, since it is when a damage occurs that it is just resorting to the search for ways to protect or protect its resources, especially the information handled by the person or organization, because information is the resource with the greatest value and the one that is at greater risk if you do not have necessary security measures.

That is why this document is aimed at analyzing and studying on different points of computer security, for example what are the measures that the main companies have in terms of measures and protocols to protect their information, in addition to also exposing what are the alternatives or techniques that computer attackers can use such as Phishing (Creation of fake pages), Vishing (identity theft), Baiting (Devices with computer viruses), Smishing (Fake messages or links), Ransomware (Data hi-jacking) as well as what are the most common measures to combat them.

2 Methodology

To carry out this research, 3 steps were taken. First, the theoretical framework or literature, which was the collection of all the relevant information for our research, this collection will be global. Secondly, we will focus on the incidents, proto-cols,regulations and procedures that Peru has. Thirdly, we will make a proposal of how companies should proceed when carrying out their audits to verify the security that the company has against possible attacks that threaten its information security.

3 Development

3.1 Physical Security

According to [21], it tells us that "physical security consists of placing physical barriers and control procedures, as a measure to prevent and counteract possible threats to resources and confidential information." This refers to the security mechanisms and controls that are in place near and within the computing center or area designat-ed by the company or entity implemented to protect the hardware and any means used for data storage.

3.2 Types of Attacks

As indicated in the various studies [1], [2], [12], [21]; take into account that within physical security it is necessary to focus and cover the threats caused by man as well as by the nature of the physical environment in which our information is stored.

Fire. These can be caused by the improper use of all fuel, failures in electrical installations or any improper storage or transfer of flammable substances. [1] [2] [12] [21], we are presented with some factors that must be taken into account to reduce the risks of fires in computer facilities:

- The area in which the computers are located must be a local
- It should be taken into account to carry out revisions in the electrical installations periodically.
- It should not be placed above, below or adjacent to spaces where flammable materials are processed, manufactured or stored.
- Smoking must be prohibited in the computer area
- Implement "false floor" that must be on the actual floor, these materials must not be flammable

Theft. Computers are valuable instruments for organizations, as they function as an entry point to a large amount of information which they can be; development of new products, customer information, transactions, etc. which may be in the sights of competitors or outsiders.

Sabotage. Research [12] [17] shows that the most feared danger in the areas of data pro-cessing is sabotage.

Physically, magnets are the most used tools, since, with a pass, the information disappears, the data processing centers can be destroyed without entering them. In addition, dirt, metal particles or gasoline can be introduced through air conditioning ducts, communications and electrical lines can be cut, etc.

Therefore, they recommend that access control not only requires identification, but also associates it with the opening or closing of doors, in addition to placing restrictions on how long staff can be within the area or sector within a company or institution.

3.3 Logical Security

According to [21], it tells us that Logical Security consists of the "application of barri-ers and procedures that safeguard access to data and only those authorized to do so are allowed to access them." With this, a series of objectives are proposed:

- Restrict access to company programs and files.

- Ensure that the correct information, files and programs are being used in and by the correct process.
- That the information sent is received only by the person to whom it has been sent and not to another.
- That the information received is the same as that sent
- That there are alternative emergency steps for the transmission of infor-mation.

Cons l de Acceso. For [1], [4], they say that these controls must be implemented in the Operating System, applications, database or in any other utility. This will be of great help when protecting our operating system from the network or from any unauthorized modification.

Identification and Authentication. According to [21], it is called Instant Identification in which the user will be known by the system and authentication to the verification made by the system to check if the identification is valid or not. it will be the first line of defense in the vast majority of systems.
What is recommended is that this identification and authentication be done once to say that the system is efficient in security.

Location and Hours. Restricted access to system resources can be based on the physical or logical location of the data or people. As for the schedules, this type of controls allows to limit the access of the users to certain hours of the day or to certain days of the week.

Encryption. According to [5], encrypted information can only be decrypted by those who possess the appropriate key. Encryption can provide a powerful measure of access control

3.4 Computer Crimes

Phishing. It is the most used technique, the cybercriminal recreates a well-known and reliable website, with this cloned website, the person comes toshare their personal information.

Vishing. It consists of the use of the Voice over IP Protocol (VOIP) to impersonate the identity of the user. A phone call is used to obtain sensitive information from the affected person.

Baiting. They often use infected USB abandoned in public places in the hope that some user will connect them on their devices.

Smishing. Use SMS messages to recreate communications of prestigious entities with the user to capture their personal information

Ransomware (data hijacking). It is a type of harmful program that restricts access to certain parts or files of the infected operating system and asks for a ransom in exchange for removing this restriction. Some types of Ransomwares encrypt operating system files using the device and coercing the user to pay the ransom.

3.5 Computer Viruses

According to [16,18], this means that only computers only understand binary codes, since in the world there are several concepts either such as programs or video games or it could also be operating systems or any kind of software. In the case of software, it is defined as something intangible either from the computer with the instructions that they expect to be performed whether they are complex or simple.

- Worms
- Trojans
- Spyware
- Keyloggers
- Adwares
- Dialers
- Backdoors

3.6 Preventive Mechanisms in Computer Security

According to [16], These mechanisms are the ones that are most forgotten since they are seen as a waste of time since in part of the administration in several cases it has as an extra cost. The mechanisms consist of series that come to make periodic re-views with which some have improvements either hardware or software or any of the elements that have been involved as processes or systems and these have or depend on the processes of the company.

Information Backup. This is a process that comes to be the most common that is done in companies that store a lot of important information. Companies understand that problems with information become very expensive since with this it seems that it is easy, but when pointing out the mechanisms it is not as simple as it is analyzed.

Audit. A procedure used to perform a verification, demonstration, or test of the system that the company has. Which must be carried out periodically and these must provide accurate data and give confidence to the management of the company. Ideally, they should answer the following questions:

- Is the system being used properly?

- Does the system conform to the company's current internal and external regulations?
- What are the security protocols that the company has?
- Does the company comply with these security protocols?

4 Cybercrime in Peru

4.1 National legislation

- Law No. 29733, Law on the Protection of Personal Data, of July 3, 2011.
- Law No. 28493, Law Regulating the Use of Unsolicited Commercial Email
- Law No. 27806, Law on Transparency and Access to Public Information, of August 2
- of 2002.
- Law No. 27291, Law amending the Civil Code allowing the use of electronic means to declare the will and the use of the electronic signature,
- of 24 June 2000.
- Law No. 27269, Law on Digital Signatures and Certificates, of 25 May 2000.
- Legislative Decree No. 681, Use of Advanced Archival Technologies, of 11 November 1991.
- Supreme Decree No. 050-2018-PCM, which approves the definition of Digital Security at the National Level, dated May 14, 2018.
- Supreme Decree No. 081-2013-PCM, approving the National Electronic Government Policy 2013-2017, dated July 9, 2013.

4.2 Computer crime statistics in Peru

Table 1. Computer crimes investigated by divindat. 2013-2020

Crime	2013	2014	2015	2016	2017	2018	2019	2020	Total	%
Abuse of computer mechanisms and devices	**14**	**3**	**6**	**4**	**5**	**1**	**2**	**19**	**54**	**0.4%**
Abuse of computer mechanisms and devices	14	3	6	4	5	1	2	19	54	
Phishing	**10**	**101**	**114**	**134**	**132**	**227**	**247**	**572**	**1537**	**12.6%**
Phishing	10	101	114	134	132	227	247	568	1533	
Virtual phishing										
Proposals to children and adolescents for sexual purposes by technological means.	**9**	**9**			**29**	**94**	**49**	**100**	**290**	**2.4%**
Against the sexual indemnity of minors										

Proposals to children and adolescents for sexual purposes by technological means.	9	9			29	94	49	98	288	
Against data and computer systems	**38**	**62**	**47**	**47**	**104**	**126**	**159**	**177**	**760**	**6.2%**
Illicit access	11	42	1	1	49	84	129	151	468	
Unlawful access to a database										
Attack on the integrity of computer data	21	4	30	22	40	26	5	9	157	
Attack on the integrity of computer systems	6	16	16	24	15	9	5	9	100	
Attack on the integrity of data and computer systems						7	20	6	33	
Against privacy and secrecy of communications						**3**	**2**	**8**	**13**	**0.1%**
Data interpretation								2	2	
Interpretation of personal data								1	1	
Illegal data trafficking						3	2	5	10	
Computer Fraud	**298**	**334**	**414**	**610**	**1219**	**1928**	**2097**	**2615**	**9515**	**78.2%**
Card cloning	83	42	46	44	30	120	25	4	394	4
Fraudulent online purchases						287	431	261	979	10
Unauthorized electronic and/or funds transactions and transfers	215	292	368	566	1189	1521	1641	2350	8142	86
TOTAL	**369**	**509**	**581**	**795**	**1489**	**2379**	**2556**	**3491**	**12169**	**100.0%**

5 Results

5.1 Proposal of the correct procedure to carry out computer audits

This section develops our proposal of what will be the steps when performing an audit.

5.2 Procedure or phases to perform a correct audit.

Determine the nature of the audit.

Internal security audit. Covers the level of internal security of the corporation

Perimeter security audit. The level of security that is in the exterior entrances of the company is analyzed

Intrusion test. It is that methodology that consists of trying to violate the company's systems to verify the level of resistance of the systems to attacks.

Web audit. Dedicated to verifying the security of all the company's websites against the integration of any non-corresponding code of the same.

Determine the subject to be audited. It is the area, department, process, system or application to which it will be audited

Set the scope. How much is going to be reviewed and how long

Plan your resources. How much you budgeted, amount of personnel, equipment needed, etc.

Determine the methodology. Here it is determined under which standards the audit will be carried out (COBIT, ISO, etc.)

Data collection. All information taken from the tests to be carried out according to the nature and standard defined will be collected.

Documentation of discoveries or findings. Here the separation of proven findings from erroneous ones is carried out and then documented.

Make the report. Detailed documentation of all previously found findings will be made, in turn the recommendations for each finding will also be documented.

Follow-up to the recommendation. Verify if the recommendations that were given are being fulfilled correctly through tests or tests to the staff and the system.

References

1. Raydel M. Perurena “Automated and integrated management of information security controls” RIELAC, Vol.XXXIV 1/2013 p.40-58 enero - Abril ISSN: 1815-5928
2. Juan Voutssas M. * "Preservación documental digital y seguridad informática" INVESTIGACIÓN BIBLIOTECOLÓGICA, Vol. 24, Núm. 50, enero/abril, 2010, México, ISSN: 0187-358X, pp. 127-155
3. Yisel N. Benitez and Nemury S. Martinez "Security Requirements for web applications" Revista Cubana de Ciencias Informáticas Vol. 12, No. UCIENCIA Special, September 2018 ISSN: 2227-1899 | RNPS: 2301 Pp. 205-221 http://rcci.uci.cu
4. Yisel N. Benitez and Nemury S. Martinez "Security Requirements for web applications" Revista Cubana de Ciencias Informáticas Vol. 12, No. UCIENCIA Special, Septiembrx|e 2018 ISSN: 2227-1899 | RNPS: 2301 Pp. 205-221 http://rcci.uci.cu
5. R. A Escalante., “Strategy for responding to computer incidents of insecurity set in Ecuadorian law,” V.9-N.1, Mar.2018, pp. 90 - 101
6. C. A. Briceño, “Methodology for the development for a security improvement plan of the informationInfrared navigation—2019

7. R. F Lomparte "Computer Security-CC66-201901, pp. 01–02, April. 2022.
8. E. P. Wigner, “Theory of traveling-wave optical laser,” Phys. Rev., vol. 134, pp. A635–A646, Dec. 1965.
9. E. H. Miller, “A note on reflector arrays,” IEEE Trans. Antennas Propagat., to be published.
10. Victor D. Casares "Advanced Pentest Methodologies" Uruguay 2014
11. Julio C. Ardita " Organizing the Information Security area " Argentina 2013
12. Pablo M. Benitez " The 10 most common security errors in mobile applications " Argentina 2015
13. Fabian D. " Towards a Security and Privacy Model " 2013
14. Julio C. Ardita " Cases of cyberattacks on critical infrastructures " Argentina 2015
15. Martha.R.Castro "Introduction to Computer Security and Vulnerability Analysis" 2018
16. Lady.C.Parada "Computer Attacks, Ethical Hacking and Computer Security Awareness in Children" Colombia-2010
17. Cesar.H.Tarazona "Computer Threats and Information Security" 2006
18. Maria.A.Sisti "Computer Security: The protection of information in a Mendoza wine company" 2019
19. Jose.R. Buendía "Seguridad Informatica" Madrid-2013 ISBN: 978-84-481-8569-5
20. HUERTA, Antonio Villalón. "Security in Unix and Networks". Version 1.2 Digital – Open Publication . License v.10 or Later. October 2, 2000