ISSN: 2230-9926

Available online at http://www.journalijdr.com

IJDR

International Journal of Development Research
Vol. 09, Issue, 09, pp. 29633-29639, September, 2019

RESEARCH ARTICLE OPEN ACCESS

MAPPING OF INFORMATION TECHNOLOGY RISKS IN THE JUDICIARY TOCANTINENSE

***[1,2]Danillo Lustosa Wanderley, [1,2]João Carlos Vilela Batello, [1,2]Marcelo Leal de Araújo Barreto and [1]Gentil Veloso Barbosa**

[1]UFT – Universidade Federal do Tocantins, Brazil
[2]TJTO – Tribunal de Justiça do Estado do Tocantins, Brazil

ARTICLE INFO

Article History:
Received 20th June, 2019
Received in revised form
29th July, 2019
Accepted 14th August, 2019
Published online 28th September, 2019

Key Words:
Risk Management. IT Infrastructure. Threats. Information Security.

ABSTRACT

Managing an Information Technology (IT) environment and keeping it secure is not a simple task. Corporate networks and their assets are subject to various attacks, which can compromise computers, servers, and programs, causing disruption to critical services. This reality increasingly requires organizations to cope with the uncertainties and risks inherent to security in the field of information technology. Thus, this study will present a discussion about the risks related to the IT infrastructure of the judiciary of the state of Tocantins, in which critical events are punctuated with a chance of occurrence and impact before the institution's objective. After the study, it was possible to observe the strong dependence of the primary activity of the Judiciary Tocantinense with the IT infrastructure, since most of the operations are digital, including the judicial process system.

Citation: Danillo Lustosa Wanderley, João Carlos Vilela Batello, Marcelo Leal de Araújo Barreto and Gentil Veloso Barbosa. 2019. "Mapping of information technology risks in the judiciary tocantinense", *International Journal of Development Research*, 09, (09), 29633-29639.

INTRODUCTION

Managing an Information Technology (IT) environment and keeping it secure is not a simple task for organizations. Even with the advancement of information security tools, corporate networks and their assets are subject to various attacks, which can compromise computers, servers, and programs, causing disruption to essential services. This reality increasingly requires organizations to cope with the uncertainties and risks inherent to security in the field of information technology. Preserving the confidentiality, integrity, availability and authenticity of data is a key factor for any organization, whether public or private. Therefore, managing risks is of paramount importance to protect information. According to Bezerra (2013), risk is the combination of the probability of an unwanted event occurring and its consequences for the organization. That is, it is uncertainty in achieving the objectives. According to the author, in information security, uncertainty lies in the technological aspects, in the processes performed and, mainly, in the people who interact with the technology and engage with the processes.

***Corresponding author: [1,2]Danillo Lustosa Wanderley**
[1]UFT – Universidade Federal do Tocantins, Brazil
[2]TJTO – Tribunal de Justiça do Estado do Tocantins, Brazil

In conformity with ABNT (2011), risk of information security is associated with the potential that threats can exploit vulnerabilities of an asset or a set of information assets and, consequently, cause damage to an organization. Thus, organizations should manage the risks to information security in order to keep them at acceptable levels and thus achieve their goals. According to the guidelines for the management of information security within the judiciary, the adoption of procedures that ensure the security of information must be a constant priority in this power, in order to reduce failures and damages that may compromise the image of justice or to bring harm to society (CNJ, 2012). These guidelines establish that the management model should contemplate, among the various normative processes, the risk management in order to minimize the impact of potentially negative events on the assets and services provided by the judiciary, provoking, continuous improvement in judicial provision. In order to improve the infrastructure and governance of information and communication technology (ICT) so that the judiciary can be able to fulfill its institutional function, the National Council of Justice (CNJ) established by resolution No. 211, of 2015 , the National Strategy for Information Technology and Communication of the Judiciary (ENTIC-JUD) for the period of 2015-2020. In short, ENTIC-JUD is a planning tool for

governance of information technology and communication, because it consists in the establishment of a set of mechanisms in order to ensure that the use of this technology adds value to the main activity of the organ, with acceptable risks and costs. Among the mechanisms that ENTIC-JUD establishes in its art. 9, it says that each organ should elaborate and apply policy, management and process of information security to be developed at all levels of the institution, through a steering committee and in harmony with the national guidelines advocated by the Council National justice. Thereby, the Court of Justice of the State of Tocantins, through Ordinance No. 3,433, of 2017, instituted the Information Security Policy (PSI) in the context of the Judiciary Tocantinense. The information security policy, among its purposes, aims at the protection of information, and in its chapter VIII-A deals with the management of information security risks. Art. 21-A says that the "court should adopt a set of procedures to identify and implement the protective measures necessary to minimize or eliminate the risks to which their information assets are subject and to balance them with the operational costs and financial resources involved".

Thus, to meet what is established in art. 21-A of the information security policy it is necessary to implement mechanisms to manage the risks to the security of information in the judiciary of the state of Tocantins. Thereby, this work proposes to study the risks related to the information technology infrastructure of the judiciary of the state of Tocantins, where critical events will be punctuated with a chance of occurrence and impact on the business. For this, a case study was carried out, concentrating on evaluating the study environment and relating the results found to the objective of the work. The research in question did not take into consideration the external context as recommended by the standard, because the objective is to evaluate the internal controls and procedures. Therefore, the objective of this paper is to identify the threats to which the Information Technology infrastructure is subjected and the risks they impose on the final activity of the judiciary, as well as the construction of a risk response map related in this study with the implementation of controls to mitigate risks and ensure the principles of information security, such as confidentiality, integrity, availability and authenticity.

METHODOLOGY

This case study was carried out at the Court of Justice of the state of Tocantins with a qualitative and quantitative approach of the exploratory and descriptive type. For the study in question, a bibliographic review was performed with a view to presenting a theoretical basis on the subject treated. The literary materials were collected by searches in ACM, IEEE and Google academic bases, during the month of October 2018, and used the following descriptors for the research: IT risk Management, IT infrastructure, threats, information security. The selection criteria of the literary materials of the study were considered: a) without delimitation of the time of publication; b) Content related to risk management, IT infrastructure, threats and information security; c) Languages in Portuguese and English. For the development of this analysis, the area of information technology infrastructure of the explored environment was considered. For this, a risk map was built based on the most critical services, where risk identification and monitoring are relevant. Considering that the environment studied does not have a risk monitoring plan for its information technology infrastructure, points related to the principles of information security were addressed, making clear the most important items to be managed.

Information Technology Risk Mapping: This section discusses the results obtained by the study of the infrastructure environment of information technology and the risks imposed by it in the activities of the judiciary of the state of Tocantins. For the research in question, a risk management methodology was used based on the ABNT NBR ISO/IEC 27005 and ABNT NBR ISO/IEC 31000 standards. The study aims to detail the current scenario of the information technology infrastructure of the Court of Justice of the State of Tocantins in order to conduct an analysis of the threats to which the environment is subject, assessing the impacts and consequences that they can generate. Initially, the current scenario of the information technology infrastructure and its relationship with the main activity of the judiciary of Tocantins will be detailed. The information technology infrastructure existing in the judiciary is comprised of servers, switches, firewall, virtualization solution, data storage system, structured cabling, main and redundant Internet linkage, electricity supply, data center, among others. The central point of this structure is the data center, where all the processing and storage of information occurs, in order to meet all the demands of the judiciary of the state of Tocantins. The network of Judicial Power Tocantinense, called TELEJURIS, is formed by a virtual private network (VPN) and several subnets as shown in Figure 1.

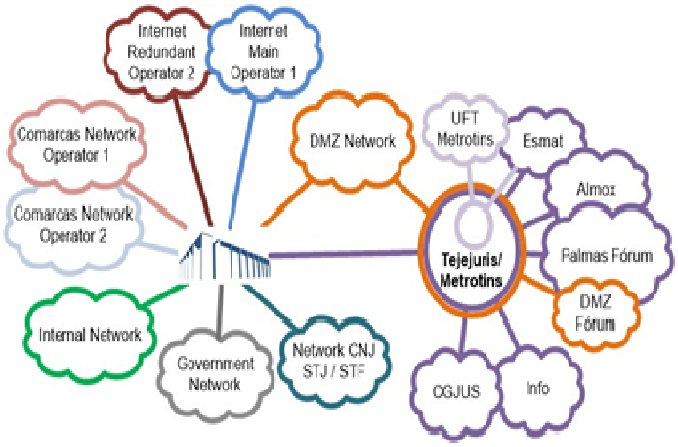

Figure 1. Network Telejuris

The Intranet subnet provides data communication between the Comarcas and annexes with the Court of Justice, through a long-distance virtual private network with Multiprotocol Label Switching (MPLS) technology. The Intranet consists of the subnets Comarcas operator 1, Comarcas operator 2, internal and Metrotins. The DMZ network is perimeter, all systems and services of the judiciary that have external access, such as HTTP servers, electronic mail, among others, are maintained.
The Government and CNJ/STJ/STF subnets interconnect the State Court of Tocantins to the network of the state executive branch and to the network of the National Council of Justice and Superior Courts, respectively. The METROTINS subnet offers a pair of dedicated fiber optics with a speed of 1G, whose purpose is to make the interconnection of the Court of Justice of the State of Tocantins with the forum of Palmas, CGJUS, Tocantinense Magistracy School (ESMAT) and other annexes in the capital. The access of all judicial units to the Internet occurs by the Court of Justice, where are the Internet

links main operator 1, with speed of 300 MB, and Internet redundant operator 2, 100 MB. The risk management model defined by the ABNT NBR ISO/IEC 27005 standard is basically divided into three stages: the definition of the context, the risk assessment process and the risk treatment. The methodology proposed for this study covers the steps cited and is based on the norm. As illustrated in Figure 2, the internal context of the Court of Justice of the State of Tocantins is composed of the people who develop the judicial activities and the computational environment with the assets that contribute to the judiciary To cantinense fulfill its mission, namely, "guaranteeing citizenship through the distribution of swift, safe and effective justice".

and risk assessment were carried out considering the computer network and the set of assets that compose it. As described in ABNT (2011), the risk management process involves defining the context, identification, analysis and evaluation, selection and implementation of responses to the risks assessed, monitoring and controls, and communication on risks with the stakeholders. Figure 3 contextualizes the flow of the risk management process adopted for this study. As previously mentioned, the proposed methodology is based on the ABNT NBR ISO/IEC 27005 standard. To identify risks, we used the techniques of brainstorming and the preliminary hazard analysis, which is like the previous one.

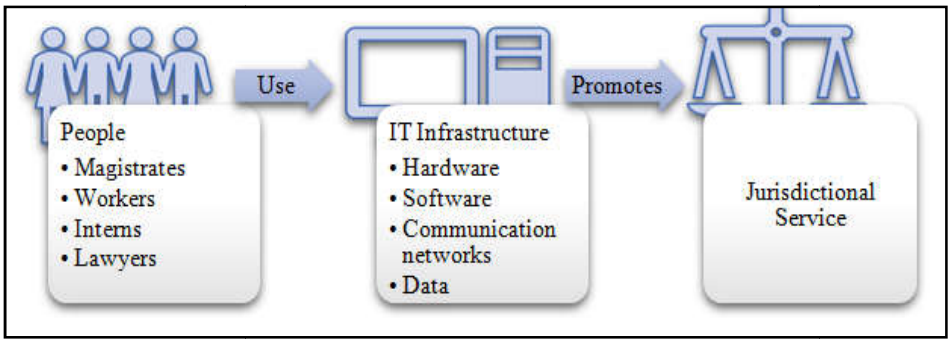

Figure 2. Internal context of the Court of Justice of the State of Tocantins

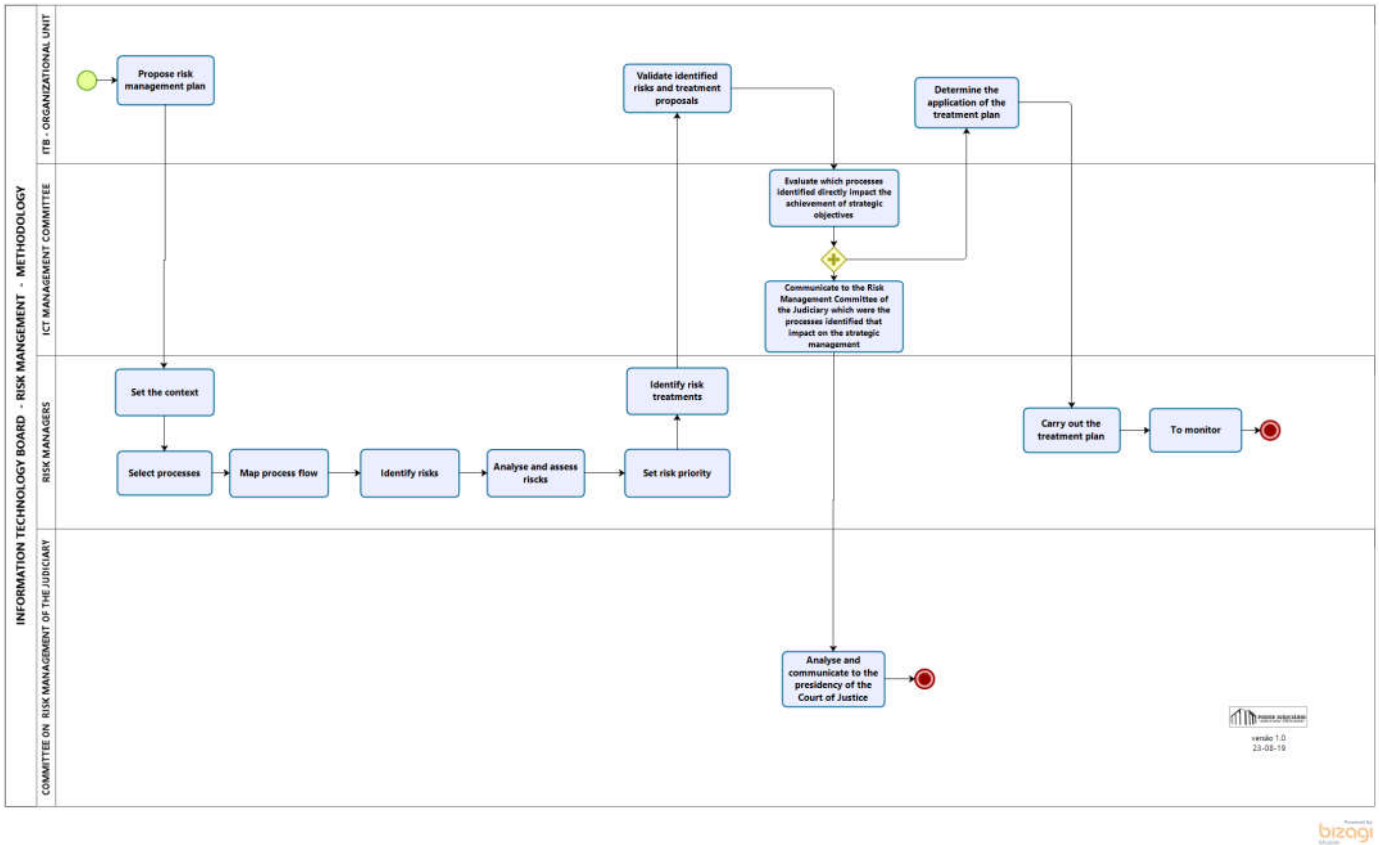

Figure 3. Risk management process flow

As most of the operations of the Court of Justice of the State of Tocantins are digital, including the judicial process system, called E-Proc/TJTO, the computational environment has a very high relevance for the realization of the main activity of the organ in question. The unavailability of information and communication technology resources greatly affects the functioning of the judiciary, because it causes delays and interrupts activities routinely performed. Thus, the analysis

The techniques cited were used according to the norm ABNT NBR ISO/IEC 31010, which is an addition to the standard ABNT NBR ISO/IEC 31000. According to Bermejo et al. (2019), the tools and techniques adopted in the study are strongly applied for the identification of risks and allow to raise relevant information that assists in decision making and the establishment of prioritization for the treatment of risks. Table 1 presents the risks identified by the five servers that

occupy strategic functions in the security of the judiciary network, including the authors of this study. The most relevant ones that could negatively impact the jurisdictional service were listed. The identified risks are analyzed by determining the consequences and their probability. The result of the analysis process will be to assign to each risk a classification, both for the probability and for the impact of the event, the combination of which will determine the level of risk (BRASIL, 2018). At this stage of the study, risks were analyzed using a semi-quantitative method that uses previously agreed numerical scales to measure the consequence and its likelihood of occurrence, which are combined using a formula to produce the risk level. Considering the simplicity that is intended in the application of this method, absolute real values of probability and consequences will not be employed, but their degrees:

- Degree of probability of occurrence (P);
- Degree of expected consequences (C).

In this way, the risk level (R) will be calculated by the formula:

$$R = P \; x \; C$$

To establish a common understanding of the ratings of probabilities and consequences, the analysis in question used the semiquantitative method based on the scales exemplified. The level of risk that will be calculated in this section is the one before the adoption of control and treatment measures, which is called the inherent risk level. The results of the combinations of probability and consequence, classified according to the scale of risk levels presented in Table 4, can be expressed in an array, as exemplified in Table 5 (BRASIL, 2018). For each risk presented in the study, the probability criteria were applied, which is the possibility of the threat being realized, and consequence, that are the losses that the threat can offer to the final activityof the judiciary, according to Tables 2 and 3.

Table 1. Risks identified using the techniques of brainstorming and preliminary hazard analysis, according to ISO 31010

ID	IDENTIFIED RISKS
1.	Fire in the Data Center
2.	Unavailability of the main Internet access
3.	Unavailability of the electronic process system – e-Proc/TJTO
4.	Malicious code software attacks on workstations

Table 2. Probability scale of occurrence of a threat (BRASIL, 2018, adapted)

PROBABILITY	DESCRIPTION OF THE PROBABILITY, DISREGARDING THE CONTROLS	VALUE
Very low	Unlikely. In exceptional situations, the event may even occur, but nothing in the circumstances indicates this possibility.	0.1
Low	Rare. Unexpectedly or casually, the event may occur, because the circumstances do not indicate this possibility.	0.2
Average	Possible. In some way, the event may occur, because the circumstances indicate moderately that possibility.	0.5
High	Likely. Until expected, the event may occur, because the circumstances strongly indicate this possibility.	0.8
Very high	Practically certain. Unambiguously, the event will occur, the circumstances clearly indicate this possibility.	1.0

Table 3. Scale of consequences resulting in the case of materialization of a threat (BRASIL, 2018, adapted)

Consequence	Description of the impact on strategic and operational objectives if the event occurs	Value
Very low	Minimum impact on objectives.	1
Low	Small impact on objectives.	2
Average	Moderate impact on objectives, but recoverable.	5
High	Significant impact on objectives, difficult to revert.	8
Very high	Catastrophic impact on objectives, irreversibly.	10

Table 4. Risk Rating Scale (BRASIL, 2018, adapted)

LR (Low Risk)	MR (Medium Risk)	HR (High Risk)	ER (Extreme Risk)
0 – 0.9	1.0 – 3.9	4.0 – 7.9	8.0 – 10.0

Table 5. Risk Matrix (BRASIL, 2018, adapted)

CONSEQUENCE	Very High 10	1.0 MR	2.0 MR	5.0 HR	8.0 ER	10.0 ER
	High 8	8 LR	1.6 MR	4.0 HR	6.4 HR	8.0 ER
	Average 5	0.5 LR	1.0 MR	2.5 RM	4.0 HR	5.0 HR
	Low 2	0.2 LR	0.4 LR	1.0 MR	1.6 MR	2.0 MR
	Very Low 1	0.1 LR	0.2 LR	0.5 LR	0.8 LR	1.0 MR
		Very Low 0.1	Low 0.2	Average 0.5	High 0.8	Very High 1.0
		PROBABILITY				

Then, the inherent risk was calculated using the aforementioned formula and classified according to the risk matrix (Table 5). The result of the classification, according to the methodology adopted, is presented in Table 6. To estimate the probability and consequences, an analysis of the occurrences records of the events listed in Table 1 was performed. In addition, the existing controls and the efficiency with which reduce the risks of each of the listed events were evaluated.

Table 6. Classification of identified risks (BRASIL, 2018, adapted)

ID	IDENTIFIED RISKS	PROBABILITY	CONSEQUENCE	INHERENT RISK LEVEL
1.	Fire in the Data Center	A (0.5)	VH (10)	HR (5.0)
2.	Unavailability of the main Internet access	L (0.2)	A (5)	MR (1.0)
3.	Unavailability of the electronic process system – e-Proc/TJTO	A (0.5)	A (5)	MR (2.5)
4.	Malicious code software attacks on workstations	A (0.5)	L (2)	MR (1.0)

Table 7. Criteria for prioritization and risk treatment (BRASIL, 2018, adapted)

RISK LEVEL	CRITERIA FOR PRIORITIZATION AND RISK TREATMENT
ER	Risk level far beyond risk appetite. Any risk at this level should be communicated to the Governance Committee and the General Board and have an immediate response.
HR	Risk level beyond risk appetite. Any risk at this level must be communicated to the General Board and have an action taken in a given period.
MR	Risk level within the risk appetite. Usually no special measures are required, but it requires monitoring the controls adopted to keep the risk at this levelor reduce it at no additional cost.
LR	Risk level within the risk appetite. No special measures are required. Requires monitoring of the controls adopted to maintain the level of risk.

Table 8. List of risks requiring treatment

ID	IDENTIFIED RISKS	RISK LEVEL	CONTROL
1.	Fire in the Data Center	HR	NO
2.	Unavailability of the electronic process system – e-Proc/TJTO	MR	YES
3.	Malicious code software attacks on workstations	MR	YES
4.	Unavailability of access to the main Internet	MR	YES

As shown in Table 6, the event unavailability of the main Internet access was classified with a low probability, due to having occurred only twice in the period from 2012 to 2018. The consequence of this event, according to the criteria set out in Table 3, was classified as mean, since one of the impacts will be the unavailability of access to the judicial process system (e-Proc) by the external public. Although the e-Proc is one of the main systems of the Judiciary Tocantinense and its unavailability generate delays in the process progress, in general the risk of the unavailability of the main Internet link was considered medium because it is not of difficult recovery.

Another example of the event listed in Table 6 is fire in the Data Center. Its probability of occurrence was classified as mean because there are no efficient and effective controls to mitigate this threat. Although it has never occurred before, it is not impossible that at some point this will occur, since the recent history of fires in the building of the Court of Justice of the State of Tocantins brings an incident that occurred in August 2018. Its consequences were classified as high, because they generate a significant impact on the objectives of the Judiciary Tocantinense. Thus, by applying the established criteria, the risk is considered high and impacts in an important way in the jurisdictionalservices. For the evaluation process, criteria were established for prioritization and treatment associated with risk levels as exemplified in Table 7. The documentation of this step usually consists of a list of the risks that require treatment, with their respective classifications and priorities. For each risk classified in the analysis stage, the criteria contained in Table 7 were applied. They were prioritized according to the level of risk and their probability of occurrence, in that order. Thus, a list was generated (Table 8) in which the first were placed those that could cause more damage to the judicial provision. Table 8 presents four threats from the area of information technology that are correlated to the final activity of the judiciary. Of these, 75% are medium-risk and 25% high-risk threats. It can also be observed that three threats already have some control implemented treatment, corresponding to 75% of the total. In this same table, a single high-risk threat was listed, and it has no treatment or control implemented. According to the criteria set out in table 7, high-risk threats must have an action taken in a given period and be communicated to the General Board of the Court of Justice of the State of Tocantins. After the analysis and assessment of the risks that the infrastructure imposes on the judicial provision, it is possible to establish whether or not to treat threats based on their level of risk. Risk treatment involves the selection of one or more options to modify the level of each risk and the elaboration of treatment plans that, once implemented, will imply new controls or modification of existing ones (BRASIL, 2018). Table 9 presents an analysis and risk assessment matrix, and the events related to these, their consequences, the existing controls and the level of risk assessed by the proposed method were identified. Table 10 presents an action plan and proposes solutions to the risks identified and analyzed, enumerating the measures to be taken, the necessary resources and the monitoring required to maintain effective risk management. According to the risk analysis carried out in the study, 25% of the threats present a high risk to the institution's business and no control has yet been implemented to treat them adequately. In this case, the institution accepts the risk for the momentary inability to take any measure on the risk. As identified in Table 10, the action needed to treat the risk identified as high (fire in the Data Center) would be the implementation of a fire prevention and combat system, which requires financial resources, resources that the institution does not currently available. The proposed action plan aims to maintain the existing controls, while maintaining the monitoring of threats, as well as proposing new controls to treat them.

Table 9. Analysis and risk Assessment matrix

IDENTIFIED RISK	CAUSES	CONSEQUENCES	IDENTIFIED CONTROLS	RISK LEVEL
Fire in the Data Center	1. Short circuit in the Data Center; 2. Short circuit on the premises of the building.	1. Partial or total destruction of the Data Center.	1. None	High Risk (5.0)
Unavailability of the electronic process system – e-Proc/TJTO	1. Human error (programming and configuration); 2. Failure to communicate with the database; 3. Failures in the services running on the application server.	1. Suspension of procedural deadlines; 2. User dissatisfaction; 3. Hearings reschedules.	1. Monitoring of system and infrastructure parameters by management software.	Medium risk (2.5)
Malicious code software attacks on workstations	1. Do not have antivirus installed; 2. Antivirus is out of date; 3. Improper access to malicious website; 4. Misuse of external storage devices.	1. Malfunction of the workstations; 2. Data theft; 3. Proliferation of malicious code programs for other workstations.	1. Enterprise Antivirus solution.	Medium Risk (1.0)
Unavailability of the main Internet access	1. Fiber optic disruption; 2. Failure, burning or stopping of network assets; 3. Cables disconnected accidentally; 4. Traffic overhead in the logical network.	1. Total unavailability of access to external services and systems; 2. Unavailability of external users in accessing the services and systems provided by the TJTO.	1. Monitoring of network assets via management software; 2. Service level Agreement (SLA) with the telecommunication operator.	Medium Risk (1.0)

Table 10. Action plan

ACTION PLAN			
IDENTIFIED RISK	**PROPOSED ACTIONS**	**REQUIRED RESOURCES**	**MONITORING**
Fire in the Data Center	1. Implement fire prevention and combat system.	1. Financial availability; 2. Bidding process.	1. Monitoring by means of smoke sensors. 2. Reports of periodic preventive maintenance of all devices.
Unavailability of the electronic process system – e-Proc/TJTO	1. Analyze the failure presented and apply the necessary corrections; 2. Provide redundancy of service hosting; 3. Maintain network assets reserve.	1. Training of the human resources of the intervening areas regarding the unavailability of the service; 2. Allocate spare network assets.	1. System and infrastructure management via monitoring software.
Malicious code software attacks on workstations	1. Make users aware of information security; 2. Adopt policy of using external devices in the TJTO network.	1. Users ' awareness of the topic of information security; 2. Maintenance of the safety solution.	1. Monitoring of stations via antivirus administration server; 2. Device usage policy in the TJTO network.
Unavailability of the main Internet access	1. Enable redundant Internet binding and apply traffic controls; 2. Provide external access to the services and systems of the TJTO via redundant Internet linkage; 3. Configure the DNS service with the addresses of the redundant Internet operator; 4. Get autonomous system number (ASN).	1. Training of procedures regarding the unavailability of the service; 2. Technical consultancy; 3. Financial resources.	1. Monitoring via software of communication linkage availability and bandwidth utilization; 2. Pro-active monitoring of the carrier; 3. Service level Agreement (SLA).

Even if several actions are implemented to address the identified threats, there will still be residual risk, which still remains after considering the effect of the responses adopted by the management to reduce the probability and impact of risks, including Internal controls and other actions.

Conclusion

According to the study, it was possible to verify the strong dependence of the primary activity of the Judiciary Tocantinense with the infrastructure of information technology, and most of the operations are digital, including the judicial process system, and the unavailability of information and communication technology resources greatly affects the functioning of the judiciary. In this sense, it is possible to affirm that the activities of the judiciary have a significant degree of dependence in relation to the area of information technology, since this provides support for the judiciary to achieve its objectives. The data collected in the study refer to the analysis carried out in the infrastructure area of the Court of Justice of the State of Tocantins. The most critical events of the organ were mapped and identified in the analysis and risk assessment matrix (Table 9).

A plan of actions was proposed (Table 10) with the measures to be taken, the necessary resources and the monitoring required to maintain effective risk management. Considering that the studied environment has implemented security controls, but does not yet have a risk management policy or a risk monitoring plan for its structured and documented information technology infrastructure, it is believed that this study can help in making important decisions that help to treat risks identified during the realization of this research and that may affect the functioning of the judiciary.Finally, it is understood that the management of information security risks should be implemented at the Court of Justice of the State of Tocantins in search of the protection of assets and to ensure the confidentiality, integrity, availability and authenticity of Information, your most valuable asset. Thus, the adoption of procedures that ensure the security of information must be a constant priority in the judiciary, in order to reduce failures and damages that may compromise the image of justice or bring harm to society.

Acknowledgements

We would like to thank the Court of Justice of the State of Tocantins for the institutional and financial support to

accomplish this work. We also thank the Information Technology Board and the Coordination of Strategic Management for technical support in mapping the process of risk management and diagramation.

REFERENCES

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 27005:2011: Tecnologia da Informação - Técnicas de Segurança - Gestão de Riscos de Segurança da Informação. Rio de Janeiro, 2011. 87 p.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 31000:2018: Gestão de Riscos - Diretrizes. Rio de Janeiro, 2018. 17 p.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 31010:2012: Gestão de Riscos - Técnicas para o processo de avaliação de riscos. Rio de Janeiro, 2012. 96 p.

BERMEJO, P. H. de S. et al. 2019. ForRisco: gerenciamento de riscos em instituições públicas na prática, 2 ed., Editora Evobiz, Brasília, Brasil. Disponível em: <http://forrisco.org/livro.php>. Acesso em: 29ago. 2019.

BEZERRA, E. K. Gestão de Riscos de TI: NBR 27005. Rio de Janeiro: RNP/ESR, 2013. 138 p.; 28 cm.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. Referencial básico de gestão de riscos / Tribunal de Contas da União. Brasília: TCU, Secretaria Geral de Controle Externo (Segecex), 2018. 154 p. Disponível em: <https://portal.tcu.gov.br/biblioteca-digital/referencial-basico-de-gestao-de-riscos.htm>. Acesso em: 5 out. 2018.

CNJ. CONSELHO NACIONAL DE JUSTIÇA. Resolução n. 211, de 15 de dez. de 2015. Dispõe sobre a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário. Brasília, 2015. Disponível em: <http://www.cnj.jus.br///images/atos_normativos/resolucao/resolucao_211_15122015_18122015173345.pdf>. Acesso em: 13 out. 2018.

CNJ. CONSELHO NACIONAL DE JUSTIÇA. Segurança da Informação – Diretrizes para a gestão de segurança da informação no âmbito do Poder Judiciário. Brasília, 2012. Disponível em: <http://www.cnj.jus.br/images/dti/Comite_Gestao_TIC/Diretrizes_Gestao_SI_PJ.pdf>. Acesso em: 13 out. 2018.

GERHARDT, T. E. Métodos de pesquisa. / [organizado por] Tatiana Engel Gerhardt e Denise Tolfo Silveira; coordenado pela Universidade Aberta do Brasil – UAB/UFRGS e pelo Curso de Graduação Tecnológica – Planejamento e Gestão para o Desenvolvimento Rural da SEAD/UFRGS. – Porto Alegre: Editora da UFRGS, 2009. 120 p.; 17,5x25cm. (Série Educação à Distância).

SÊMOLA, M. Gestão da segurança da informação: uma visão executiva. 2 ed. Rio de Janeiro: Elsevier, 2014.

SILVA, E. L. DA. Metodologia da pesquisa e elaboração de dissertação. Edna Lúcia da Silva, Estera Muszkat Menezes. – 4. ed. rev. atual. – Florianópolis: UFSC, 2005. 138p. Disponível em: <https://projetos.inf.ufsc.br/arquivos/Metodologia_de_pesquisa_e_elaboracao_de_teses_e_dissertacoes_4ed.pdf>. Acesso em: 13 jun. 2018.

TJTO. TRIBUNAL DE JUSTIÇA DO TOCANTINS. Portaria n. 3433, de 26 de jun. de 2017. Dispõe sobre a Política de Segurança da Informação (PSI). Palmas, 2017. Disponível em: <http://www.tjto.jus.br/tic/index.php/governanca-de-tic/documentos-normativos/send/98-normativas/1147-politica-de-seguranca-da-informacao>. Acesso em: 15 nov. 2018.

****