RDBCI | Revista Digital de Biblioteconomia e Ciência da Informação
Digital Journal of Library and Information Science

ISSN 1678-765X doi 10.20396/rdbci.v19i0.8661374/26267

ARTICLE RESEARCH

The risks of using unofficial digital media at federal universities

Nadi Helena Presser [1] https://orcid.org/0000-0002-1585-117X
José Alexandre Laurentino de Lima[2] https://orcid.org/0000-0002-2943-4019
Eli Lopes da Silva [3] https://orcid.org/0000-0002-2950-8938

[1] Federal University of Pernambuco – Recife, PE – Brazil / e-mail: nadihelena@uol.com.br
[2] Rural Federal University of Pernambuco – Recife, PE – Brazil / e-mail: jalexandrell@gmail.com
[3] Senac Faculty of Technology – Florianopólis, SC – Brazil / e-mail: elilsilva@globo.com

ABSTRACT
Introduction: This article analyzes the risks of using non-official digital media in an academic unit of distance education of a federal university. Objective: Specifically, it identifies the risks that may impact the processes of recovery and utilization of the information; analyzes the magnitude and impact of these risks; selects responses to them, through controls and other actions; and, finally, proposes actions to monitor and coordinate the risk management processes and results. Methodology: Methodologically, this is a diagnostic, descriptive, and documentary type of research. The technique of the discussion group was the the one used to collect data. In the analysis and interpretation of the data, the model selected was the one recommended by the Federal Audit Court, which includes several stages, as specified throughout this article. Results: The results showed the existence of risks. The measures to be taken in order to handle them, were presented. The main risks identified were the following. Conclusion: Using unofficial e-mail providers, using WhatsApp and social networks to send, receive and store official information, and storing official files in online archives.

KEYWORDS
Cell phones in communication. Risk Management. Digital Media. Information Communication. Federal University.

Os riscos do uso dos meios digitais de comunicação não oficiais nas universidades federais

RESUMO
Introdução: Analisa os riscos de uso dos meios digitais de comunicação não oficiais na unidade acadêmica de educação a distância de uma universidade federal. Objetivo: Especificamente, identifica os riscos que possam impactar nos processos de recuperação e uso da informação; analisa a magnitude e o impacto desses riscos; seleciona respostas para eles, por meio de controles e outras ações; e, por fim, propõe ações para monitorar e coordenar os processos e os resultados do gerenciamento de riscos. Metodologia: Metodologicamente é uma pesquisa do tipo diagnóstico, descritiva e documental. A técnica do grupo de discussão foi a técnica adotada de coleta de dados. Na análise e interpretação dos dados, o modelo selecionado foi o recomendado por Tribunal de Contas da União, que compreende várias etapas, como está especificado ao longo deste artigo. Resultados: Os resultados apontaram a existência de riscos e medidas a serem tomadas para tratá-los foram apresentadas. Conclusão: Usar provedores de *e-mail* não oficiais, usar o WhatsApp e redes sociais para envio, recebimento e armazenamento de informações oficiais e armazenar arquivos oficiais em repositórios *on-line* foram os principais riscos identificados.

PALAVRAS-CHAVE
Celulares na comunicação. Gerenciamento de riscos. Mídias digitais. Comunicação da informação. Universidade federal.

JITA: HI. Electronic media

1 INTRODUCTION

Producing and disseminating information for retrieval and use may not be such an easy task when there is the adoption of cell phones and mobile devices in people's work routine. On the one hand, because everyone knows that the processes of production, search, collection, dissemination and use of information occur within the organizational context, but it is not possible to delimit the boundaries. On the other hand, the use of technological innovations and devices that support them, such as the smartphone, have also introduced new institutional challenges regarding communication.

There are facilities that make WhatsApp one of the most used mobile device apps in the world, among them, its instant communication and viralization features (ROCHA; PEREIRA; SOARES, 2017). A founding characteristic of this app is interactivity, and such a user experience seems to be already starting to cause the change of habits from an institutional and communication control policy to a model pulverized in connections, characteristic of the so-called postmodern society. And, like all of society, contemporary federal public universities are also increasingly becoming mobility universities, where mobile technologies are becoming part of their information communication strategies.

Regarding the exchange of messages through the use of e-mails, a typically asynchronous mode of communication, Gmail, Outlook and others, currently used recurrently, are also characterized as information communication resources for supplying the needs of post-modern society. Although e-mails were not developed as mechanisms for cooperative work, what we see in organizations is that electronic mail services have adapted to the work group environment, speeding up processes and democratizing access to information.

According to Lemos (2002), in addition to the expansion of connection modes, we see the expansion of cooperative work and networked computers, with implications for social practices, as advocated by Capurro (2017), who observes in this phenomenon a moral imperative, that is, an order that forces us to be available all the time. Consequently, this seems to lead to an increase in the use of smart phones, smartphones, since they offer diverse amenities to those who choose to use their added services. For Lemos and Josgrilberg (2009) these are changes in habits, but also in the boundaries between what is public and private; the cell phone expresses the radicalization of digital convergence, becoming what Lemos (2002) calls a "teletype" for the informational management of the daily work of public servants.

Instant messaging applications and e-mails will continue to grow at a rapid pace, especially when used on mobile devices. This new informational infrastructure shows evidence of new processes of information production, search, communication and use. In a general sense, information management takes care of the intermediate processes performed between the origin and the use of information: the collection, organization, storage, retrieval, information products and services, dissemination and use (LE COADIC, 2004; DAVENPORT; PRUSAK, 1998; CHOO, 1998; MCGEE; PRUSAK, 1994).

The activities and tasks described by Davenport and Prusak (1998) occur within what they call the "Information Ecology," a perspective that represents the typical arrangement of information stimuli to which people are regularly exposed, the information resources they routinely use, and, currently, the increasingly fluid arrangements and boundaries between professional and private life (BYSTRÖM; HEINSTRÖM; RUTHVEN, 2019).

Given the range of possibilities for the use of the aforementioned apps and devices, it is timely that questions of risks and the magnitude of these risks in informational practices in universities be taken into consideration. Moreover, the management and control of the application of public resources based on risk have been recurrent recommendations of the

Federal Audit Court (TCU) (BRASIL, 2016; 2018a; 2018b). Although the discussion about the need to manage risks in the public sector is not new, it is still a paradigm to be achieved, especially when it comes to informational risks.

The object of this study is the means of communication - mobile technologies and e-mails from unofficial providers - used in the distance education academic unit of a federal university. Considering that these channels are not the university's official means of communication, this study focuses on the risks and their magnitude in the dissemination, retrieval and use of information. Based on the above, the following problem was investigated in the development of this research: What are the risks and the magnitude of these in the retrieval and use of information, due to the adoption of unofficial means of communication in the distance education academic unit of the university?

To answer the problem, the objective of this research focused on analyzing the risks of using non-institutionalized digital means of communication in the academic unit of distance education of the university, from the specific objectives: a) Identify the risks that may have some impact on the processes of retrieval and use of information; b) Assess the magnitude and impact of risks; c) Recommend responses to risks, through controls and other actions and; d) Propose actions to monitor and coordinate the processes and results of risk management.

In the field of Information Science, risk management particularly emphasizes informational practices embedded in information-related activities. It provides, in the short term, improvements in the quality and security of services related to the informational process of universities, including producing, disseminating and using information, preventing loss, leakage or alteration of information, and avoiding cyber attacks. Basically, the objective of the risk management process operated in the sphere of a university is to protect institutional information. It highlights how the use of unofficial digital means of communication can facilitate, but also restrict information work practices and processes. The model presented here can be adapted to be applied in other public and private organizations as a self-assessment tool, taking the initiative themselves to design and put into practice the process of improving informational practices in the work environment.

Next, the theoretical review consists of a grounding in the thematic areas of the research, by means of documentary and bibliographic sources.

2 THE DIMENSION OF THE INFORMATIONAL PROCESS IN ORGANIZATIONS

Mobile technologies inaugurated the "era of connection", as Lemos (2002) highlights, and configure new mediation devices, assuming the most diverse forms and complexities (such as smartphones), generating a new communicational space that is, by definition, hybrid in nature (SILVA, 2006).

This hybridism, according to Paraguai (2008), has fostered the creation of new cultural products that, by simultaneously inhabiting the digital and physical spatial domains, empower users to reconfigure spatial and temporal relations, transforming notions of physical presence and possibilities of action. In this hybrid space, named by Lemos (2002) as informational space, the person continues acting and present in his/her physical space, while the information received and transmitted remotely adds other characteristics to this phenomenological experience.

According to Capurro (2017), all these changes refer not only to codes or regimes of space, both physical and digital, but also to regimes of time. As Weiser (1991) notes, the most profound technologies are those that disappear. They interweave into the fabric of everyday life until they become indistinguishable. The challenge of information management involves recognizing this era of connection, with its new ways of disseminating and using information.

Capurro (2017) points out that the temporal regime of the cyberworld is not only based on this primacy of the present, but puts it as a moral norm, that is, as an imperative and social value that is based on instantaneous access to information, as well as on a communication regime that is no less instantaneous and displaced from the place where we are physically located. We are at the beginning of an interdisciplinary and intercultural reflection that has as its object information and communication and the gains and losses in the various aspects of work and ways of life. Just as in the sciences it is possible to question a paradigm that conditions and fixes a certain way of interpreting natural or social phenomena, it is also possible in relation to technological inventions, which are also science. To act ethically on this game changer is to think about the meaning of such a transformation. This is, according to Capurro (2017), to ask about the meaning of freedom or, more specifically, liberties, and mutual responsibilities in the digital age.

Risk management is related to the monitoring and control of risks by organizational management. These activities involve responsibilities of people, positions and functions at all levels of the organization.

Risk is the effect of uncertainty on the organization's objectives (ABNT, 2009) and, according to Brazil (2014), encompasses positive events, with the potential to add value, and negative events, with the potential to destroy value. According to Normative Instruction No. 01 of 2016, art. 2, of the Ministry of Planning:

> XIII - risk: possibility of an event occurring that may have an impact on the fulfillment of the objectives. Risk is measured in terms of impact and probability;
> XIV - inherent risk: risk to which an organization is exposed without considering any managerial actions that may reduce the probability of its occurrence or its impact;
> XV - residual risk: risk to which an organization is exposed after the implementation of managerial actions for the treatment of risk. (BRAZIL, 2016)

Effective risk management generally meets legal, regulatory and societal expectations, and creates the conditions for the organization to better respond and adapt to problems that interrupt an event, activity or process (INTERNATIONAL FEDERATION OF ACCOUNTANTS - IFAC, 2015). The key to ensuring effective and integrated risk management, as recommended by IFAC (2015), is the employment of a properly grounded risk management framework as an integral part of the organization's management system. What we read in the IFAC (2015) guidance is that neither risk management nor internal control are objectives in themselves, instead, they are integral to shaping and achieving the organization's objectives.

In 2017, risk management covered all public sector entities under the General Public Sector Governance Index (GGI), including the TCU. That same year, the TCU approved its Risk Management Policy (RMP) and has been taking actions to implement it (BRASIL, 2018b).

Risk treatment options include, according to Brazil (2018a), avoiding, reducing (mitigating), transferring (sharing), and accepting (tolerating) the risk. Accepting or tolerating the risk is deliberately taking no action to change the probability or consequence of the risk. It occurs when the risk is within the organization's tolerance level. Selecting the most appropriate option involves balancing the costs and efforts of implementing the risk mitigation measure on the one hand, and the resulting benefits on the other. However, it should be taken into account that new risks can be introduced by the treatment, but there are risks whose preventive treatment is not economically justifiable, such as risks of great negative consequence, but with very low probability of happening (INTOSAI, 2007 apud BRASIL, 2014).

The next section explains and justifies the set of methodological procedures that helped investigate the problem and answer the objectives presented.

3 METHODOLOGICAL PROCEDURES

Given its characteristics, this study is configured as descriptive research, documentary research, and survey-diagnostic research. It is a descriptive research because, according to Vergara (2016), it seeks to describe a situation in detail, especially what was intended in this study, describing the characteristics of the situation, or even uncovering the relationship between events. This is also a documentary research, conducted on institutional documents, whose contents served to elucidate certain issues and legitimize others. Among the documents, the university's Risk Management Policy and Information Technology Master Plan. This is a diagnostic research, because it explored, raised and defined problems, with the participation of other members of the community. (ROESCH, 2005; MARTINS; TEÓPHILO, 2009). According to Thiollent (1997), a diagnostic process is interactive when researchers adopt a methodology whose nature enables the broad exchange of information with stakeholders. According to the author, input from members of the problem situation is a very satisfactory condition for the diagnosis to be better informed and contextualized.

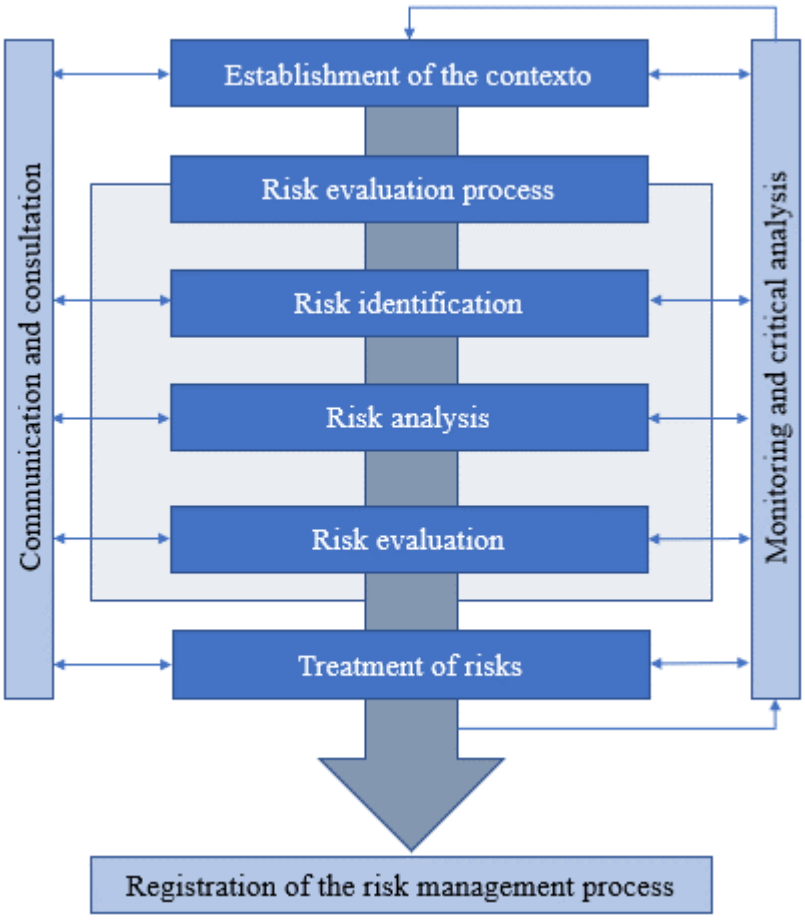
The data collection process took place in the period between January 16, 2020 and February 28, 2020. It began with the formation of a discussion group with technical-administrative servers, professors and outsourced service providers who worked in the university's distance education unit. In the first meeting, after explaining the research objective, the methodological procedures and some of the official documents that would be consulted in the meetings, they signed the Free and Informed Consent Form. Each meeting lasted an average of two hours, with the participation of all members.

The focus group followed the guidelines given by Ibáñez (2003) and Gutiérrez (2011), so that the main objective was to seek practical cooperation to accomplish a task that required the horizon of a consensus. In this context, each participant gave his or her share of contribution until consensus was reached on the objectives of this investigation. The members also assimilated the idea that this is a diagnostic research, because, as Roesch (2005) and Martins and Theóphilo (2009) have argued, problems were explored, raised and defined, with the participation of other members of the community. Moreover, all participants contributed, so that it was possible to create quite satisfactory conditions to deal with the proposed problem situation.

The first objective of the group was to deepen the knowledge about the topic "risk management" and about the Risk Management Policy, instituted at the university. Subsequently, the group identified which are the email operators, the mobile applications, such as WhatsApp, and the other means of information dissemination used in the academic unit. After two meetings, the focus group identified a number of risks inherent in the use of unofficial digital media for information dissemination and retrieval in the distance education academic unit.

The model selected to identify and analyze the risks of the use of communication media - mobile technologies and emails from unofficial providers - was the one recommended by the TCU (BRASIL, 2018a), represented in Figure 1.

Figure 1. Risk management model



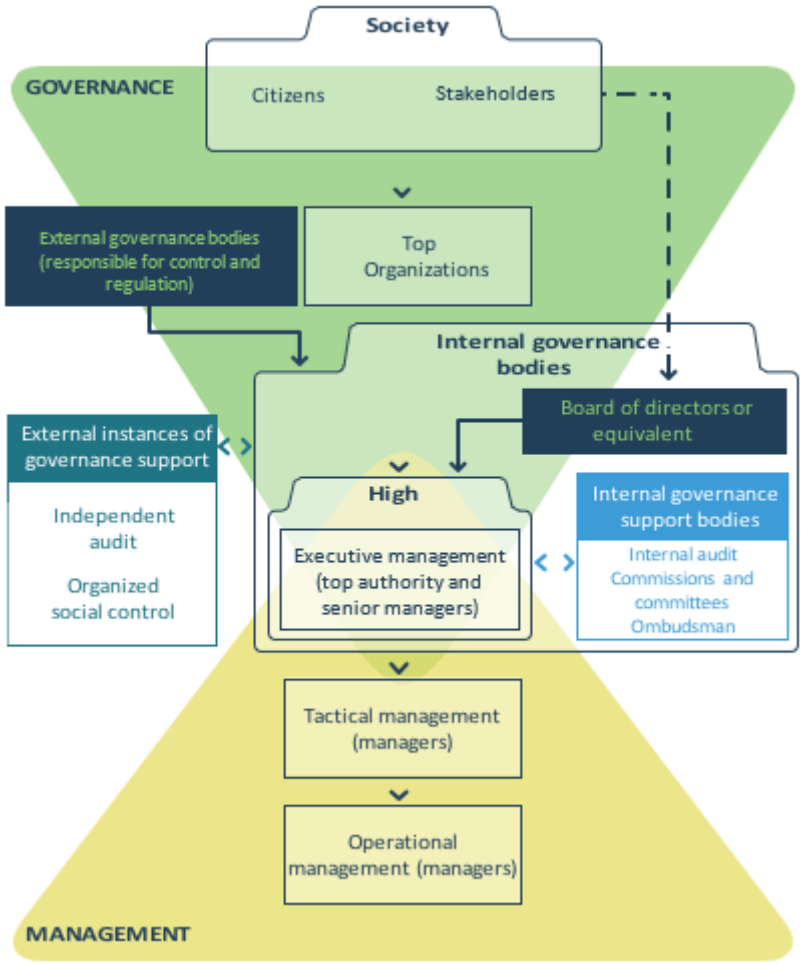
Source: adapted from Brazil (2018a)

The model describes the risk management process according to ISO 31000 (ABNT, 2009). In the presentation of the results, the steps in Figure 1 are detailed and their purpose in risk management is demonstrated.

Communication and consultation (Figure 1) is a way of ensuring that during all stages or activities of the risk management plan development, informative and consultative communication was maintained between the university's EaD academic unit staff and internal and external stakeholders to help establish the appropriate context and ensure that the needs and concerns of stakeholders were considered in the process.

Establishing the context requires identifying the factors of the university's internal and external environment (Figure 2).

Figure 2. System of governance of organs and entities of the public administration



Source: Brazil (2014, p. 28).

In a first moment, this exercise helped to highlight the main stakeholders who, acting internally or externally to the university, influence and are influenced by the activities of the academic unit of distance education. Stakeholders were included in each step or cycle of the risk management process, through the process of communication and consultation, as seen earlier. This step was carried out through document analysis to identify both the stakeholders and their interests, by using the RACI Matrix (acronym for Responsible, Accountable, Consulted and Informed), a technique for assigning responsibilities, consulting and informing stakeholders about an ongoing activity or project. The RACI Matrix presents, in tabular form, the relationship between activities and roles, indicating: responsible (R) for performing an activity (the executor); authority (A) - who should be responsible for the activity, the owner; the consulted (C), who should be consulted and participate in the decision or activity at the time it is performed; the informed (I), who should receive the information that an activity was performed (EMBRAPA, 2014).

The goal of the risk identification step in Figure 1 was to produce a comprehensive list of risks, including sources and events of risks that could have some impact on the achievement of the objectives identified in the context setting step (BRAZIL, 2018a). The involvement of the team of stakeholders working in the distance education academic unit helped to create accountability toward the management process and commitment toward addressing the risks.

The risks were categorized according to the standard in use at the university, contained in its Risk Management Policy, as follows:

a) Operational - Events that can compromise the activities of the organ or entity, usually associated with failures, deficiencies or inadequacy of internal processes, people, infrastructure and systems.
b) Financial/Budgetary - Events that can compromise the body or entity's capacity to count on the budgetary and financial resources necessary to carry out its activities, or events that can compromise the budget execution itself.
c) Image/reputation - Events that can compromise the society's (or partners', clients' or suppliers') trust regarding the body or entity's capacity to fulfill its institutional mission.
d) Legal/compliance - Events arising from legislative or normative changes that may compromise the activities of the body or entity.
e) Environmental - They result from the association between natural risks and the risks arising from natural processes aggravated by human activity and the occupation of the territory.

Each risk event can be contained in more than one category. Besides being categorized, each identified risk was presented along with its probable causes, effects, and consequences. Considering what ABNT (2009) says, risk analysis (shown in Figure 1) is the process of understanding the nature and determining the level of risk. "Risk is a function of both probability and the measure of consequences." (BRAZIL, 2018a, p. 25). Thus, the level of risk is expressed by the combination of the probability of occurrence of the event and the resulting consequences in case the event materializes.

Therefore, following the guidelines of Brazil (2018a), the result of the risk analysis was to assign a rating to each identified risk, both for the probability and the impact of the event, whose combination determined the risk level. Identifying the factors that affected the likelihood and consequences were also part of the risk analysis, including an appreciation of the causes, sources, and positive or negative consequences of the risk, expressed in tangible or intangible terms.

Given the nature of the risk, the risk analysis was configured as a combination of a mixed assessment: qualitative and quantitative. The qualitative analysis defined the impact, probability and risk level by qualifiers such as "extreme", "high", "medium" and "low", based on the perception of the staff and outsourced employees that composed the focus group. The quantitative analysis used previously agreed upon numerical scales to measure consequence and probability, which were combined, by means of a formula[1], which was seen in detail in the data analysis, to produce the level of risk.

Quantitative analysis needs factual data, however, if such information is lacking and such analysis is not possible, although desirable, the use of a qualitative method, combined with mixed analysis, based on expert opinion, may be sufficient and effective (ABNT, 2012). "In mixed analyses, considering that the underlying logic is that the level of risk is proportional to both probability and impact, the function 'Risk' will essentially be a product of these variables." (BRAZIL, 2018a, p. 25).

Following the guidelines of Brazil (2018a), the relationship between risks and their components used in this study is illustrated by means of a simple matrix (Figure 3).

[1] P X I = Risk Rating, where - Probability (P) X Impact (I)

Figure 3. Simple risk matrix

Source: Brazil (2018a, p. 26).

As the focus of this research lies only in the analysis of inherent risk[2] , it was decided to use a risk classification scale proposed by Brazil (2018a), which thus quantified the risks: Low Risk - RB (0-9.99); Medium Risk - MR (10-39.99); High Risk - RA (40-79.99) and Extreme Risk - ER (80-100). To prepare this mixed analysis, scales were used, such as those exemplified in Chart 1, to establish a common understanding of the classifications of probabilities and impacts.

Table 1. Scale of probabilities and consequences

PROBABILITIES	
Probability description, disregarding controls	WEIGHT
Improbable. In exceptional situations, the event might even occur, but nothing in the circumstances indicates this possibility.	1
Rare. Unexpectedly or casually, the event may occur, because the circumstances indicate little of the possibility.	2
Possible. In some way, the event could occur, because the circumstances moderately indicate this possibility.	5
Probable. In an even expected way, the event may occur, because the circumstances strongly indicate this possibility.	8
Practically sure. Unequivocally, the event will occur, the circumstances clearly indicate this possibility.	10
CONSEQUENCES	
Description of the impact on the objectives, should the event occur	WEIGHT
Minimal impact on objectives (strategic, operational, information, communication/ dissemination or compliance).	1

[2] The inherent risk level of an event is the level of risk before consideration of the responses management adopts, including internal controls, to reduce the likelihood of the event and/or its impacts on objectives. It results from the combination of likelihood and impact. Residual risk is that to which an organization is exposed after management actions have been implemented. Treatment of this risk would not be possible here, as no management action has yet been implemented.

Little impact on the objectives (idem).	2
Moderate impact on objectives (idem), but recoverable.	5
Significant impact on the objectives (idem), difficult to reverse.	8
Catastrophic impact on objectives (idem), irreversibly.	10

Source: Adapted from Brazil (2018a).

Then, the results of the combinations of probability and impact, classified according to the scale of risk levels proposed by Brazil (2018a), were expressed in a matrix, such as the one exemplified in Figure 4.

Figure 4. Full risk matrix

IMPACT						
	Very High - 10	10 RM	20 RM	50 RA	80 RE	100 RE
	High - 8	8 RB	16 RM	40 RA	64 RA	80 RE
	Medium - 5	5 RB	10 RM	25 RM	40 RA	50 RA
	Low - 2	2 RB	4 RB	10 RM	16 RM	20 RM
	Very low -1	1 RB	2 RB	5 RB	8 RB	10 RM
		Very low -1	Low - 2	Medium - 5	High (8)	Very High - 10
		PROBABILITY				

Source: Brazil (2018a, p. 28).

These scales may be adapted to become more compatible with the context and the object under study. The purpose of risk assessment, the step shown in Figure 1, is to assist in making decisions about which risks require treatment and the priority for treatment implementation (BRASIL, 2018a). It involves determining whether the risk and its magnitude are acceptable or tolerable or whether any treatment is required (ABNT, 2009). As shown in Exhibit 2, everything is assessed against risk appetite. Risk appetite is the amount of risk an organization is willing to accept in pursuit of its objectives (INTOSAI, 2007 apud BRASIL, 2014)…

Table 2. Guidelines for prioritizing and treating risks

Risk Level	Criteria for risk prioritization and treatment
RE	Risk level well beyond risk appetite. Any risk at this level must be communicated to governance and senior management and have an immediate response. Postponement of measures, only with the authorization of the top management.
RA	Risk level well beyond risk appetite. Any risk at this level must be communicated to governance and senior management and have an immediate response. Postponement of measures, only with the authorization of the top management.
RM	Risk level within the risk appetite. Usually no special action is needed, but requires specific monitoring activities and management attention to maintaining responses and controls to keep the risk at this level, or reduce it at no additional cost..
RB	Risk level within the risk appetite, but it is possible that there are higher return opportunities that can be exploited by taking on more risk, evaluating the cost vs. benefit ratio, such as lowering the level of controls.

Source: Brazil (2013 apud BRAZIL, 2018a, p. 32).

In this step, therefore, the understanding and level of risk obtained in the risk analysis step was used to make decisions about the risks analyzed, in particular:

(a) whether a particular risk needed treatment and the priority for this;
(b) Whether a particular activity should be performed or discontinued;
(c) Whether internal controls should be implemented or, if they already existed, whether they should be modified, maintained or eliminated.

To support the risk assessment process, criteria were established for prioritization and treatment associated with risk levels (recommended level of attention, required response time, who should be communicated, etc.), elaborated based on the example of Brazil (2018a), presented in Table 2, which was the starting point of the risk prioritization assessment process. Even being aware that there are four levels of priority, ascertaining the data may lead to not fulfilling all the priority categories, and it is possible that some of them are repeated in different data.

Therefore, considering that the treatment process is cyclical (BRASIL 2018a), that is, the very treatment of risks can lead to other risks, including some that did not even exist before, in this study, based on ABNT (2009), the treatment included:

(a) an assessment of whether residual risk levels were tolerable;
(b) Where they were not, definition and implementation of additional treatment;
(c) Evaluation of the effectiveness of this treatment.

Finally, still referring to Figure 1, monitoring and critical analysis constitute the essential step in risk management and are intended to

(d) detect changes in the external and internal context, including changes in risk criteria and in the risk itself, that may require revision of risk treatments and their priorities, as well as identify emerging risks;
(e) To obtain additional information to improve the risk management policy, structure and process;
(f) Analyze events, changes, trends, successes and failures and learn from them;
(g) Ensure that controls are effective and efficient in design and operation.

Although following up on this step is not part of this study, nor are monitoring guidelines presented here, attention is drawn to the responsibilities related to monitoring and critical analysis, which have the function of ensuring that the risk register is kept up to date, as well as documenting in it the results of the actions mentioned.

4 PRESENTATION OF THE RESULTS

The presentation of results shows the stakeholders who act internally or externally to the university, influence and are influenced by the activities of the academic unit of distance education.

Currently, the university's official email provider is Zimbra, but Outlook, Gmail, Uol, Yahoo, among others, are in operation in the academic unit. Besides these, the instant messaging application WhatsApp is used, although there is no regulation that officially guides its use. But it is through WhatsApp that requests are made, communications are shared, several documents are sent, received and stored, meetings are scheduled, and all kinds of informational and interactional communication are made possible. There is even a group of university employees called "EaD News" that uses it for information sharing purposes. That is, professors, technicians and service providers exchange information about the university and its daily routine through this channel. The group circulates both official information, such as copies of official documents, internal resolutions, scheduling meetings of committees and working groups, and information that does not necessarily need to go through any formal institutional flow, which we will call here unofficial information from the university, such as informal meetings, various communications, get-togethers, and others.

WhatsApp is also used by smaller and more restricted groups. The technical-

administrative servers of the distance education academic unit, for example, have organized a closed group called "TecAdmEad". In this group they also share information, in the same way as "EAD News". Based on this survey, it is assumed that there are more virtual groups formed only by teachers, service providers, managers, and so on.

There is no mention of commercial email providers, or even instant messengers in the Institutional Development Plan (IDP) that is in force, nor in its Risk Management Policy, as explained in the Information Technology Master Plan (ITDP) in force, even though their use for various purposes within the university is widely and unrestrictedly known. However, in 2018, the Risk Management Coordinator was formally created, designated as responsible for the preparation and approval of the Risk Management Plan, which will contain the risk management methodology in the institution. However, this document is still being drafted and is not available, so there is no way of knowing whether commercial email providers, or even instant digital messengers, will be covered in the actions or not.

At the university, the management of social communication is done by the Coordination of Social Communication (CCS), an advisory body to the Rector's Office, responsible for strategies and actions aimed at internal and external audiences, and other issues that permeate the social communication inside and outside the university. The CCS makes use of internal communication mechanisms, such as the website, direct mail via institutional e-mail, newsletters, and various publications, as well as external ones. It is also responsible for managing the university's official profiles on social media, such as Facebook, Twitter, YouTube, Instagram, Flickr, and Soundcloud, officially mentioned in the current IDP. Although it welcomes information received through non-institutionalized instant messaging applications, the CCS does not disseminate information by this means.

On the other hand, a University Council Resolution deals with the Information and Communication Security Policy Norms (POSIC), highlighting Article 6, which states that the university understands Information as any and all data, processed or not, that may be used for the production and transmission of knowledge, contained in any medium, support or format. Article 7 defines communications within the university as any interactions involving the sending of data or information between university bodies or users, or between the university and external people or institutions, using any means of communication. And art. 9 warns that all information produced, stored or received by the university users as results of their professional activity belongs to the university.

Considering the use of commercial email providers, or even instant messengers, if this data is lost or misplaced, it is difficult to recover access to the email and its data. In official channels, the university's Information Technology Department could recover both the access and the stored data.

In this study, governance is the set and structure of leadership (rector, directors, chiefs, course coordinators, supervisors, professors, researchers and other public servants), strategy and control put into practice to evaluate, direct and monitor management, with a view to conducting university policies and providing services aligned with the expectations of the academic community and society. The external stakeholders are the current and future students, the employers, the Ministry of Education (MEC), the National Institute of Educational Studies and Research Anísio Teixeira (INEP), Capes, the National Association of Directors of Federal Institutions of Higher Education (ANDIFES), the Federal Comptroller General (CGU), and the Federal Audit Court (TCU). The internal stakeholders are the members of the High Council; the Risk Management Coordination; the Open Data and Transparency Committee; the Social Communication Coordination; the Teaching, Research and Extension Council; the Information Technology Committee; the Department of Statistics and Informatics; the Information Technology Center; the directors of the academic units; the Rectory; and the Pro-Rectories.

Table 3 contains the grouping of risk events, their causes and probable effects and/or consequences in the operational category. We chose to analyze only Gmail, because, during the research period, it was the main unofficial email provider used at the university and, moreover, the consequences of its use are very similar to the others, such as Outlook, etc.

Table 3. Risk events, their causes and consequences

Event	Use unofficial providers such as Gmail for sending, receiving and storing official information.	Causes	Facility of use, convenience, range, superiority when compared to the official provider.
Consequences	1) Difficulty in information retrieval. 2) Informality in communication with external and internal institutional actors. 3) Lack of standard in the identification of usual e-mails. 4) Difficulty in publicizing official attendance channels. 5) The credibility of the university can be questioned. 6) Low confidentiality in information retrieval and dissemination, considering that Gmail is not an institutionalized provider at the university.		
Event	Use WhatsApp for sending, receiving and storing official information.	Causes	Speed of access, convenience, diversity of resources, diverse possibilities of use, diverse resources, popularity, ubiquity.
Consequences	1) Access to the application linked to a cell phone number; 2) Exposure of your personal cell phone number; 3) Difficulty to disentangle (untie, detach) the personal experience from the professional one; 4) Difficulty in recovering information; 5) Segregation of employees who do not use the application; 6) Data backup is aggregated to the cell phone number; 7) Risk of information leakage or loss, in the dissemination and storage process; 8) Informality in the communication with external and internal institutional actors.		
Event	Use of social media (Facebook, Instagram, Youtube, Twitter, etc.) for dissemination and retrieval of official information.	Causes	Reach of social networks, ease of disseminating information, offer of service channels, access to various free resources, proximity to the target audience.
Consequences	1) Difficulty in retrieving information in non-institutional environments; 2) Lack of control of what is disseminated; 3) Lack of information management policy; 4) Excessive informality; 5) Need to allocate human resources to control and maintain each channel.		
Event	Use online repositories such as Google Drive, OneDrive, Dropbox MEGA and others to store official files.	Causes	Facility, convenience, breadth, added tools.
Consequences	1) Difficulty in information retrieval. 2) Risk of information leakage, alterations or loss: 3) Informality in communication with external and internal institutional actors; 4) Credibility; 5) Low confidentiality in information retrieval, since these repositories belong to private companies.		

Source: Adapted from Lima (2020, p. 63)

After identifying and categorizing the risks, we proceeded to their analysis and evaluation. Following the guidelines of Brazil (2018a), the result of the risk analysis was to assign each risk a rating for both the likelihood and impact of the event occurring, the combination of which determined the risk level.

Identifying the factors that affected the likelihood and consequences were also part of the risk analysis, including an appreciation of the causes, sources, and positive or negative consequences of the risk, expressed in tangible or intangible terms. Table 4 below summarizes this classification.

Table 4. Assessment and classification of the identified risk events

Nº	Risk event	Risk Assessment			Risk classification
		(P)*	(I)**	P X I	
1	Use unofficial providers such as Gmail for sending, receiving and storing official information.	10	10	100	RE
2	Use WhatsApp for sending, receiving and storing official information.	5	5	25	RM
3	Use of social networks (Facebook, Instagram, Youtube, Twitter, etc.) for dissemination of official information.	10	8	80	RE
4	Use online repositories such as Google Drive, OneDrive, Dropbox MEGA and others to store official files.	10	10	100	RE

*P=Probability, **I=Impact
Source: Adapted from Lima (2020, p. 64)

It can be observed that for the focus group of this study, Risk 1 has a very high probability of occurring. This means that it is practically certain that it will occur, in which case it is assigned the weight 10 within the probability scale. In addition, it was found that this risk event also has a very high impact on the proposed objective, which gave it the weight 10 within the scale of impact and consequences. Thus, based on the risk rating scale (Brazil, 2018a), the product probability X impact of the risk in question equals 100, the maximum score. Based on the risk matrix in the full risk matrix, such a score gives this event the classification of Extreme Risk (ER), as shown in Table 4.

The group deduced that the pairing of the smartphone with access to Gmail acts as a catalyst that shapes workplaces and the way servers carry out their activities and relate to other public servants and other target audiences, even though this application is not the university's official email server. The survey only confirms that Gmail is already part of the information environment of the EaD academic unit and that a good part of the information dissemination is made possible through it. Its use seems to be so recurrent that, depending on how the university treats this risk, and depending on the change, it may not be accepted.

To Risk 2 the focus group assigned the medium probability. This is equivalent to saying that the event might occur, because the circumstances indicate moderately that possibility. At the time of the analysis, the group concluded that the instant communication, interactivity, and viralization characteristics of this application refer to a pulverized model in connections, sometimes without institutional control. Thus, the team's inference that its use to disseminate and retrieve information within the academic unit is, in fact, a risk event, given that official information passed on inaccurately, or incompletely, can reach a large number of people quickly, is in line with the understanding of researchers such as Rocha, Pereira, and Soares (2017). In addition, indiscriminate use of the app can cement problems with image and reputation issues. As occurred in the analysis of Risk 1, in this second one, the group also showed concern about the convergence of the WhatsApp app with the smartphone, since the

latter is the default device for the use of the app in question. Similarly to Gmail, the ease and practicality of accessing WhatsApp on this type of device avigorates the server's willingness to use it, which can make it difficult to address these risks.

Even though it has become clear that the use of WhatsApp in information dissemination and retrieval has a medium risk, it is also notable that it fits into what authors call intermediate processes that enable the exchange of information between people (LE COADIC, 2004; CHOO, 1998; MCGEE; PRUSAK, 1994). But mostly, what we see here is what Capurro (2017) has called the new moral imperative that forces people to be available and accessible all the time and everywhere. This transformation of the spatio-temporal code through a change of the technological code changes people's working lives, particularly from the point of view of their social, economic, political, and legal codes. In view of this, the treatment of this risk is a cultural challenge regarding the information culture of public servants.

Risk 3 was considered an Extreme Risk, as the group agreed that its probability and impact are very high, respectively, thus weighting 10 for probability and 8 for impact. The great debate at this point revolved around the issues raised by Lemos (2002), regarding the transformations in social practices, in the experience of urban space, and in the way of producing and consuming information. As beneficial as these new connections incorporated into social media may be, the group pondered that disseminating and retrieving official information from them remains a high risk, given the little control over the profiles used, over the people responsible for them, or even over the ownership of the data that is disseminated. Moreover, in this case some specific observations can be applied, related to image and reputation, and of legal and compliance order, among others arising from the constant use of the smartphone.

Finally, Risk 4 was considered by the group as a risk with a high probability of occurring, being assigned a weight of 10 in this item. The same weight 10 was attributed to the impact item. Thus, the product of probability X impact was 100, resulting in its classification as Extreme Risk (ER).

In this last risk event the group's concern about the difficulty in accomplishing what is stated in the university's University Council Resolution, which deals with the Information and Communication Security Policy Norms, became visible. The Resolution indicates that all the information produced, stored or received by the university users as results of their professional activity belongs to the university. However, the study found that all the repositories identified in the risk event analysis belong to private companies, revealing who the real "owners" of the information produced and recorded there are. All this certainly helped the group to determine the classification of this as an Extreme Risk (ER), as shown in Table 4.

Risk 4 is contained in the information management context, especially in the issue about adjusting and aligning managerial and organizational activities and informational processes. It is necessary to pay attention to the fact that every risk management practice needs guidelines, which can be expressed in an information policy that, according to Braman (2006), is a set of laws and regulations that establish procedures and guidelines concerning the creation, storage, dissemination, and use of information. Without clear and instituted guidelines, each user will manage information in his or her own way, further raising the degree of potential risk events. Part of this seems to be happening in the study object, as the focus group confirmed that multiple users make constant use of various online repositories to manage their personal and work information.

Following with the guidelines of Brazil (2018a), this is the stage in which the diagnosis group chooses to avoid, reduce (mitigate), transfer (share) and/or accept (tolerate) the risk, and it should be noted that the options are not mutually exclusive. Table 5 contains the proposals for handling the risks identified, generated from the consensus among the participants of the

focus group created for the purposes of this research.

Table 5. Proposed risk treatment

Nº	Risk events	Risk treatment
1	Use unofficial providers such as Gmail for sending, receiving and storing official information.	Avoid
2	Use WhatsApp for sending, receiving and storing official information	Tolerate
3	Use of social networks (Facebook, Instagram, Youtube, Twitter, etc.) for dissemination of official information.	Mitigate
4	Use online repositories such as Google Drive, OneDrive, Dropbox MEGA and others to store official files.	Transfer

Source: Adapted from Lima (2020, p. 65)

Regarding Risk 1 - Extreme Risk, the Guidelines for Risk Prioritization and Treatment in Table 4 point out that risk levels that go beyond the risk appetite, that is, that go beyond the amount of risk an organization is willing to accept in the pursuit of its objectives (INTOSAI, 2007 apud BRASIL, 2014), must be communicated to senior management and must also have an action taken within a certain period. That said, Risk 1 will be placed on the priority list in the risk treatment step.

As can be seen in Table 5, the focus group suggested that the academic unit under study and other stakeholders work towards avoiding such a risk, i.e., the university needs to avoid using Gmail to send, receive and retrieve official information. However, following the protocol suggested in the methodological procedures, the identified risk, with its analysis and evaluation, will be sent to the university's governance and top management, who, in turn, have the autonomy to take the necessary measures regarding the treatment of such risk.

However, it is worth noting that the university is studying and committed to a plan to migrate from the Gmail personal account to the use of corporate accounts of this same email provider, thus starting to treat it as an official and institutionalized client. This action is being agreed upon by the Rector's Office and the Information Technology Center and, by the end of the presentation of the results of this research in May 2020, this process was in progress.

Risk 2 presents a level within the risk appetite. According to ABNT (2009), this appetite would be the amount and also the types of risks that an organization is prepared to seek, retain, or assume. In this case, usually no special measures are needed, but it does require specific monitoring activities by managers. Then this risk can be tolerated.

Risk 3 has characteristics of Risk 1. That is, both need to come to the attention of top management, who must take measures to avoid, mitigate, tolerate or transfer this risk. The focus group for this research suggested, in the case of this particular risk, that it should be mitigated. This means that the university can use social media to disseminate official information and for synchronous contact with students, but in a more moderate way. Social networks have the potential to become resources for scientific dissemination, bringing scientists and the public closer together beyond the reach of formal means of scientific communication. The scientific information available on social networks requires organization and systematization, and it is expected that researchers give the deserved attention to readers who have become new groups of users accessing these information and scientific communication services.

Finally, Risk 4 is another extreme risk that requires attention (Table 5). In this case, the group understood that this risk should be transferred or shared, given that what is on the

table are online repositories. It is understood that the university's Information Technology Core can and should be involved in resolving the possible impacts related to this risk. However, the migration to Gmail corporate accounts, already mentioned in the text referring to Risk 1, will help to avoid or even mitigate such risk, considering that said provider has a more robust cloud storage system. Therefore, Risk 4 will be duly reported to the university's top management to take the appropriate action, whether or not the suggestions presented here are followed.

Finally, all the data collected and analyzed were forwarded to the university's internal stakeholders, according to the RACI matrix presented in Chart 6, so that, if there is willingness to continue the monitoring process and critical analysis, the university's top management will have all the results of this research in hand.

Table 6. RACI Matrix for treatment of identified risks

Risks	Actions List			
1	The Academic Unit is committed to migrating from the personal Gmail account to use the corporate accounts of the same provider. This action is being articulated and provided by the Rectory and the Information Technology Center (ITC).			
R (Responsible)		A (Authority)	C (Consulted)	I (Informed)
Distance Education Academic Unit		ITC	Information Technology Committee (ITC)	All academic units
Risks	Actions List			
2	Promote training on the correct use of the digital tool, so that its use does not cause impacts on the dissemination and retrieval of information.			
R (Responsible)		A (Authority)	C (Consulted)	I (Informed)
Distance Education Academic Unit		Rectory	ITC	All academic units
Risks	Actions List			
3	Promoting training and capacitation that stimulate zeal and care in the use of such tools for information dissemination and retrieval.			
R (Responsible)		A (Authority)	C (Consulted)	I (Informed)
Pró-Reitoria de Gestão de Pessoas (PROGEPE)		Rectory	ITC	All academic units
Risks	Actions List			
4	Check, with NTI, about migration procedures for the corporate repository, either the repository itself or a private provider, but officially registered and institutionalized.			
R (Responsible)		A (Authority)	C (Consulted)	I (Informed)
ITC		Rectory	ITC Rectory	All academic units

Source: Adapted from Lima (2020, p. 71)

Often, when it comes to promoting change, managers get lost in some details and end up not clearly defining responsibilities. Chart 6 highlights who is responsible for the actions that need to be taken, who has authority over them, who or which sectors of the university should be consulted, and who should be informed about such actions.

Taking Risk 1 as an example: the responsibility for the migration lies with the distance education academic unit, but who has authority over the action to be taken is the Information Technology Center (NTI), because these are changes that require the use of several technologies that demand specific technical knowledge. However, it is necessary to consult the Information Technology Committee (CTI), since this committee is a deliberative and advisory body of the university on matters related to information technology. Finally, the matrix identifies who or which bodies need to be informed about such actions. In all cases analyzed in Chart 8, all

academic units will be informed, since the risks faced may be the same. And, if this is not the case, such communication will also serve as a warning.

5 FINAL CONSIDERATIONS

The main objective of this research was to identify what are the risks and the magnitude of these risks in the retrieval and use of information, due to the adoption of non-official means of communication in the distance education academic unit of a federal university. Based on the aspects analyzed and the results obtained, it was found that there are many risks involved in this process, some of them considered extreme, indicating that measures need to be taken to address them. The results presented not only identified the risks that may have some impact on the processes of dissemination, retrieval and use of information within and outside the academic unit under study, but also measured their magnitude.

The analysis of these risks revealed that, of the four events identified, three (75%) require some attention from the university's top management. This is because, as risk events 1, 3 and 4 were classified as extreme risks, the methodology adopted in this study suggests that risk levels that go beyond the risk appetite, which is the case in emphasis, should be communicated to top management and also have an action taken within a certain period.

Responses to the identified risks aim to minimize the impacts of these events on the university with regard to information dissemination and retrieval. The matrix consists in delimiting who is responsible for the actions that need to be taken, what is the authority of these people over the actions, who or which bodies will be consulted, and who should be informed. By adhering to this method, stakeholders are also involved in the search for solutions that aim to reduce the impacts of the identified risk events.

The study also demonstrated that good information management is intrinsically linked to the informational context in which the university is inserted. In this context is contained a set of interrelated vehicles, such as websites, mobile applications, social networks, telephones, computers, that facilitate the examination of information in integrated communication environments. The study also showed how important it is to build a clear and comprehensive Information Management Policy, so that diverse tools are enabled to contribute and people are empowered to use them.

Finally, even though it was not one of the goals originally proposed for this research, the study showed the informational practices in the work environment and how influential technologies and social media are on everyone's daily lives. There was a consensus in the discussion group responsible for identifying all the risk events analyzed that a good part of these risks come from the intense and constant use of electronic devices that keep us connected almost constantly, such as the cell phone and the personal computer, especially when any of these has a constant connection to the Internet. The ease of use of these technological tools and their various applications end up influencing the way we work, how we interact and, especially, how information is disseminated and retrieved.

During the studies it was possible to identify some limitations of this research, in the sense that, at first, the discussion group formed to identify and analyze the risk events that impact the main objective analyzed in this study did not have enough autonomy to deal with the risks effectively.

The research also did not address the survey of the risks that could be generated by suspending the use of the analyzed services. Although there was no survey and analysis of these secondary risks, one wonders how much risk the university might be exposed to if the information is unavailable for a period of time.

It would also be of great relevance to reproduce this study and its methodology in other departments, academic units and even in other agencies of the Executive Branch. Although there are cultural, geographical and organizational factors that may influence the information environment of the work, there are also commonalities that go beyond these boundaries.

CRediT

RECOGNITIONS: Not applicable.
FINANCING: Not applicable.
INTEREST CONFLICTS: The authors certify that they have no commercial or associative interest that represents a conflict of interest in relation to the manuscript.
ETHICAL APPROVAL: Not applicable.
AVAILABILITY OF DATA AND MATERIAL: Not applicable.
AUTHORS 'CONTRIBUTIONS: Conceptualization, Methodology, Supervision, Validation, Visualization, Original Writing: Presser, N. H.; Conceptualization, Research Methodology, Supervision, Validation, Visualization, Original writing: Lima, J.A.L.; Formal analysis; Supervision; Writing - proofreading and editing: Silva, E.L.

REFERENCES

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **NBR ISO 31000**: Gestão de riscos: Princípios e diretrizes. Rio de Janeiro, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **NBR ISO/IEC 31010**: Gestão de riscos*:* Técnicas para o processo de avaliação de riscos. Rio de Janeiro, 2012.

BRASIL. Ministério do Planejamento. **Instrução normativa conjunta nr. 1 de 10 de maio de 2016.** Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. [2016]. Available at: http://www.in.gov.br/. Access on: 30 Jun. 2020.

BRASIL. Tribunal de Contas da União. **Referencial básico de governança aplicável a órgãos e entidades da administração pública**. Tribunal de Contas da União. Versão 2. Brasília: TCU, Secretaria de Planejamento, Governança e Gestão, 2014. 80 p.

BRASIL. Tribunal de Contas da União. **Referencial básico de gestão de riscos**. Tribunal de Contas da União. Brasília: TCU, Secretaria Geral de Controle Externo, 2018a. 154 p.

BRASIL. Tribunal de Contas da União. **Roteiro de avaliação de maturidade da gestão de riscos**. Tribunal de Contas da União. Brasília: TCU, Secretaria de Métodos e Suporte ao Controle Externo, 2018b. 164 p.

BRAMAN, S. **Change of state**: information, policy and power. London: MIT Press, 2006.

BYSTRÖM, K.; HEINSTRÖM, J.; RUTHVEN, I. Work and information in modern society: a changing workplace. *In*: BYSTRÖM, K.; HEINSTRÖM, J.; RUTHVEN, I. (org.). **Information at work**. Information management in the workplace. London: Facet Publishing, 2019. p. 1-32.

CAPURRO, R. A liberdade na era digital. *In*: GOMEZ, M.N. G. de.; CIANCONI, R. de B. (Orgs.) **Ética da informação**: perspectivas e desafios. Rio de Janeiro: Editora Garamond, 2017. p. 45-66. Available at: http://www.capurro.de/gonzalezdegomez.pdf. Access on: 14 May 2019.

CHOO, C. W. **The knowing organization**: how organizations use information for construct meaning, create knowledge and make decisions. Nova York: Oxford Press, 1998.

EMPRESA BRASILEIRA DE PESQUISA AGROPECUÁRIA (EMBRAPA). **Guia de uso do modelo corporativo de processos de software da Embrapa (MCPSE)**. Ministério da Agricultura, Pecuária e Abastecimento. Belém, PA: Embrapa Amazônia Oriental, 2014. 33 p.

GUTIÉRREZ, J. Grupo de discusión: ¿Prolongación, variación o ruptura con el focus group? **Cinta Moebio**, n. 41, p. 105-122. 2011.

IBÁÑEZ, J. **Más allá de la sociología.** El grupo de discusión: Teoría y crítica. 5. ed. Madrid: Sieglo Veintiuno Editores, 2003.

INTERNATIONAL FEDERATION OF ACCOUNTANTS (IFAC). **From bolt-on to built**. Nova Iorque: IFAC, 2015. Available at: https://www.ifac.org/publications-resources/bolt-built. Access on: 17 May 2019.

LE COADIC, Y. **A ciência da informação**. Tradução Maria Yêda F. S. de Filgueiras Gomes. 2. ed. Brasília, DF: Briquet de Lemos Livros, 2004.

LEMOS, A. **Cibercultura, tecnologia e vida social na cultura contemporânea**. Porto Alegre: Sulina, 2002.

LEMOS, A; JOSGRILBERG, F. **Comunicação e mobilidade**: aspectos socioculturais das tecnologias móveis de comunicação no Brasil. Salvador, BA: EDUFBA, 2009.

LIMA, J. A. L. **Os riscos do uso dos meios digitais de comunicação não institucionalizados em uma Unidade da Universidade Federal Rural de Pernambuco**. 2020. 93 f. Dissertação (Mestrado em Gestão Pública), Recife, Centro de Ciências Sociais Aplicadas, Universidade Federal de Pernambuco, 2020.

MARTINS, G. A.; THEÓPHILO, C. R. **Metodologia da investigação científica para ciências sociais aplicadas**. 2. ed. São Paulo: Atlas, 2009.

MCGEE, J; PRUSAK, L. **Gerenciamento estratégico da informação**: aumente a competitividade e a eficiência da sua empresa utilizando a informação como uma ferramenta estratégica. Rio de Janeiro: Campus, 1994.

PARAGUAI, L. D. Interfaces multisensoriais: espacialidades hibridas do corpoespaço. **Revista FAMECOS** [Online], v. 15, n. 37, p. 54-60, 2008. Available at: https://revistaseletronicas.pucrs.br/index.php/revistafamecos/article/view/4800. Access on: 2 ago. 2019.

ROCHA, D.; PEREIRA, I. A.; SOARES, V. WhatsApp: de mensageiro instantâneo e chamada de voz em smartphones, para dispositivo de comunicação ubíqua dos gestores EAD

da UFT/UAB no cerrado tocantinense. **Revista Desafios,** v. 4, n. 2, p. 185-193, 2017. Available at: https://doi.org/10.20873/uft.2359-3652.2017v4n2p185. Access on: 11 May 2019.

ROESCH, M. A. S. **Projetos de estágio e de pesquisa em administração**: Guia para estágios, trabalhos de conclusão, dissertações e estudos de caso. 3. ed. São Paulo: Atlas, 2005.

SILVA, A. S. e. Do ciber ao híbrido: tecnologias móveis como interfaces de espaços híbridos. *In:* ARAUJO, D. C. (org.). **Imagem (ir)realidade**: comunicação e cibermídia. Porto Alegre: Sulina, 2006. p. 21- 51.

THIOLLENT, M. **Pesquisa-ação nas organizações**. São Paulo: Atlas, 1997.

VERGARA, S. C. **Projetos e relatórios de pesquisa em administração**. 16. ed. São Paulo: Atlas, 2016. 104 p.

WEISER, M., The computer for the 21st century. **Scientific American**, v. 265, n. 3, p. 66-75, January 1991. Available at: https://bit.ly/3kwYQuA. Access on: 2 Aug. 2019.

Article submitted in the similarity system

Submitted: 24/09/2020 – Accepted: 10/02/2021 – Published: 27/02/2021