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

ISSN 1678-765X doi 10.20396/rdbci.v19i0.8661286

ARTIGO DE PESQUISA

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

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] Universidade Federal de Pernambuco – Recife, PE – Brasil / e-mail: nadihelena@uol.com.br
[2] Universidade Federal Rural de Pernambuco – Recife, PE – Brasil / e-mail: jalexandrell@gmail.com
[3] Faculdade de Tecnologia Senac – Florianopólis, SC – Brasil / e-mail: elilsilva@globo.com

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.

The risks of using unofficial digital media at federal universities

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. Communication of information. Federal university.

JITA: HI. Electronic media

1 INTRODUÇÃO

Produzir e disseminar informações para recuperação e uso pode não ser tarefa tão simples quando há a adoção dos celulares e dos aparelhos móveis na rotina de trabalho das pessoas. De um lado, porque todos sabem que os processos de produção, busca, coleta, disseminação e de uso de informação ocorrem dentro do contexto organizacional, mas não se consegue delimitar as fronteiras. Por outro lado, o uso das inovações tecnológicas e dispositivos que as suportam, como o *smartphone*, também introduziram novos desafios institucionais em relação à comunicação.

Há facilidades que tornam o WhatsApp um dos aplicativos para dispositivos móveis mais utilizados no mundo, entre elas, suas características de comunicação instantânea e de viralização (ROCHA; PEREIRA; SOARES, 2017). Uma característica fundante desse aplicativo é a interatividade, e tal experiência de uso parece já começar a provocar a mudança de hábitos de uma política institucional e de controle de comunicação para um modelo pulverizado em conexões, característico da chamada sociedade pós-moderna. E, como toda a sociedade, as universidades públicas federais contemporâneas também, cada vez mais, tornam-se as universidades da mobilidade, onde as tecnologias móveis passam a fazer parte de suas estratégias de comunicação da informação.

No que concerne à troca de mensagens mediante uso dos *e-mails,* um modo tipicamente assíncrono de comunicação, o Gmail, Outlook e outros, na atualidade usados recorrentemente, também se caracterizam como recursos de comunicação da informação para suprimento das necessidades da sociedade pós-moderna. Embora os *e-mails* não tenham sido desenvolvidos como mecanismos de trabalho cooperativo, o que se constata nas organizações é que os serviços de correio eletrônico se adaptaram ao ambiente de grupos de trabalho, agilizando processos e democratizando o acesso às informações.

De acordo com Lemos (2002), além da ampliação de modos de conexão, vemos a ampliação de trabalhos cooperativos e dos computadores em rede, com implicações nas práticas sociais, como advoga Capurro (2017), que observa nesse fenômeno um imperativo moral, isto é, uma ordem que nos obriga a estarmos disponíveis o tempo todo. Consequentemente, isso parece levar ao aumento no uso dos telefones celulares inteligentes, os *smartphones*, uma vez que oferecem comodidades diversas para aqueles que optam por usar seus serviços agregados. Para Lemos e Josgrilberg (2009) trata-se de mudanças de hábitos, mas também de limites entre o que é público e privado; o celular expressa a radicalização da convergência digital, transformando-se no que Lemos (2002) chama de "teletudo" para a gestão informacional do trabalho quotidiano dos servidores públicos.

Os aplicativos de mensagens instantâneas e os *e-mails* continuarão crescendo em ritmo acelerado, especialmente quando usados em dispositivos móveis. Essa nova infraestrutura informacional mostra evidências de novos processos de produção, busca, comunicação e uso de informação. Em sentido geral, a gestão da informação cuida dos processos intermediários executados entre a origem e a utilização da informação: a coleta, a organização, o armazenamento, a recuperação, os produtos e serviços de informação, a disseminação e uso (LE COADIC, 2004; DAVENPORT; PRUSAK, 1998; CHOO, 1998; MCGEE; PRUSAK, 1994).

As atividades e tarefas descritas por Davenport e Prusak (1998) ocorrem dentro do que eles chamam de "Ecologia da Informação", perspectiva que representa o arranjo típico dos estímulos de informação a que as pessoas são expostas regularmente, os recursos de informação que usam rotineiramente e, atualmente, os arranjos e os limites cada vez mais fluidos entre a vida profissional e a vida privada (BYSTRÖM; HEINSTRÖM; RUTHVEN, 2019).

Diante da gama de possibilidades de uso dos aplicativos e dispositivos citados, é oportuno que questões de riscos e da magnitude desses riscos nas práticas informacionais nas universidades sejam levadas em consideração. Ademais, a gestão e o controle da aplicação dos recursos públicos com base em risco têm sido recomendações recorrentes do Tribunal de Contas da União (TCU) (BRASIL, 2016; 2018a; 2018b). Apesar de não ser nova a discussão sobre a necessidade de gerenciar riscos no setor público, isso ainda é um paradigma a ser alcançado, principalmente em se tratando dos riscos informacionais.

O objeto deste estudo são os meios de comunicação – tecnologias móveis e *e-mails* de provedores não oficiais – usados na unidade acadêmica de educação a distância de uma universidade federal. Considerando que esses canais não são os meios de comunicação oficiais da universidade, este estudo foca nos riscos e em sua magnitude na disseminação, recuperação e uso da informação. Com base no exposto, o seguinte problema foi investigado no desenvolvimento desta pesquisa: **Quais os riscos e a magnitude desses na recuperação e uso da informação, devido à adoção de meios de comunicação não oficiais na unidade acadêmica de educação a distância da universidade?**

Para responder ao problema, o objetivo desta pesquisa se concentrou em analisar os riscos de uso dos meios digitais de comunicação não institucionalizados na unidade acadêmica de educação a distância da universidade, a partir dos objetivos específicos: a) Identificar os riscos que possam ter algum impacto nos processos de recuperação e uso da informação; b) Avaliar a magnitude e o impacto dos riscos; c) Recomendar respostas aos riscos, por meio de controles e outras ações e; d) Propor ações para monitorar e coordenar os processos e os resultados do gerenciamento de riscos.

No campo da Ciência da Informação, a gestão de riscos enfatiza, particularmente, práticas informacionais incorporadas nas atividades relacionadas à informação. Proporciona, no curto prazo, melhoramentos na qualidade e na segurança dos serviços relativos ao processo informacional das universidades, entre eles, produzir, disseminar e utilizar informações, prevenir perdas, vazamentos ou alterações de informações e evitar ataques virtuais. Basicamente, o objetivo do processo de gestão de riscos operado na esfera de atuação de uma universidade é proteger as informações institucionais. Evidencia como o uso dos meios digitais de comunicação não oficiais pode facilitar, mas também restringir as práticas e processos de trabalho com informação. O modelo aqui apresentado pode ser adaptado para ser aplicado em outras organizações públicas e privadas como instrumento de autoavaliação, tomando elas próprias a iniciativa de elaborar e colocar em prática o processo de aperfeiçoamento das práticas informacionais no ambiente de trabalho.

A seguir, a revisão teórica consiste no embasamento a respeito das áreas temáticas da pesquisa, por meio de fontes documentais e bibliográficas.

2 A DIMENSÃO DO PROCESSO INFORMACIONAL NAS ORGANIZAÇÕES

As tecnologias móveis inauguraram a “era da conexão”, como destaca Lemos (2002), e configuram novos dispositivos de mediação, assumindo as mais diversas formas e complexidades (como os *smartphones*), gerando um novo espaço comunicacional que é, por definição, híbrido em sua natureza (SILVA, 2006).

Esse hibridismo, segundo Paraguai (2008), tem fomentado a criação de novos produtos culturais que, por habitarem simultaneamente os domínios espaciais digital e físico, potencializam aos usuários a reconfiguração de relações espaciais e temporais, transformando noções de presença física e possibilidades de atuação. Nesse espaço híbrido, denominado por

Lemos (2002) de espaço informacional, a pessoa continua atuando e presente em seu espaço físico, enquanto as informações recebidas e transmitidas remotamente adicionam outras características a essa experiência fenomenológica.

De acordo com Capurro (2017), todas essas mudanças se referem não apenas a códigos ou regimes do espaço, tanto físico quanto digital, senão também a regimes de tempo. Como observa Weiser (1991), as tecnologias mais profundas são aquelas que desaparecem. Elas se entrelaçam no tecido da vida quotidiana até se tornarem indistinguíveis. O desafio da gestão informacional passa pelo reconhecimento desta era da conexão, com seus novos modos de disseminar e usar informação.

Capurro (2017) ressalta que o regime temporal do *cibermundo* não apenas se baseia nessa primazia do presente, como a põe como norma moral, isto é, como imperativo e valor social que se baseia no acesso instantâneo à informação, assim como em um regime de comunicação não menos instantâneo e deslocado do lugar em que nos encontramos fisicamente. Estamos no começo de uma reflexão interdisciplinar e intercultural que tem como objeto a informação e a comunicação e os ganhos e as perdas nos diversos aspectos do trabalho e de formas de vida. Assim como nas ciências é possível questionar um paradigma que condiciona e fixa determinada maneira de interpretar os fenômenos naturais ou sociais, também é possível em relação às invenções tecnológicas, que também são ciência. Agir eticamente sobre essa mudança de jogo é pensar no significado de tal transformação. Isso é, de acordo com Capurro (2017), perguntar pelo sentido da liberdade ou, mais concretamente, das liberdades, e das responsabilidades mútuas na era digital.

A gestão de riscos está relacionada ao monitoramento e controle de riscos pela gestão organizacional. Essas atividades envolvem responsabilidades de pessoas, cargos e funções em todos os níveis da organização.

Risco é o efeito da incerteza sobre os objetivos da organização (ABNT, 2009) e, de acordo com Brasil (2014), abrange eventos positivos, com o potencial de agregar valor, e negativos, com o potencial de destruir valor. De acordo com a Instrução Normativa nº 01 de 2016, art. 2º, do Ministério do Planejamento:

> XIII – risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos. O risco é medido em termos de impacto e de probabilidade;
> XIV – risco inerente: risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto;
> XV – risco residual: risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco. (BRASIL, 2016)

O gerenciamento eficaz de riscos, em geral, atende às expectativas legais, regulatórias e societárias, além de criar as condições para que a organização responda melhor e se adapte aos problemas que interrompem um evento, atividade ou processo (INTERNATIONAL FEDERATION OF ACCOUNTANTS – IFAC, 2015). A chave para garantir uma gestão eficaz e integrada do risco, conforme recomenda a IFAC (2015), é o emprego de uma estrutura de gestão de risco devidamente alicerçada, como parte integrante do sistema de gerenciamento da organização. O que se lê nas orientações da IFAC (2015) é que nem o gerenciamento de riscos nem o controle interno são objetivos neles mesmos, em vez disso, eles são parte integrante da configuração e realização dos objetivos da organização.

Em 2017, a gestão de riscos abrangeu todas as entidades do setor público no âmbito do Índice Geral de Governança do Setor Público (IGG), incluindo o TCU. Nesse mesmo ano o TCU aprovou sua Política de Gestão de Riscos (PGR) e vem adotando ações para implementá-

la (BRASIL, 2018b).

As opções de tratamento de riscos incluem, segundo Brasil (2018a), evitar, reduzir (mitigar), transferir (compartilhar) e aceitar (tolerar) o risco. Aceitar ou tolerar o risco é não tomar, deliberadamente, nenhuma medida para alterar a probabilidade ou a consequência do risco. Ocorre quando o risco está dentro do nível de tolerância da organização. Selecionar a opção mais adequada envolve equilibrar, de um lado, os custos e esforços de implementação da medida de mitigação do risco e, de outro, os benefícios decorrentes. Todavia, deve-se levar em consideração que novos riscos podem ser introduzidos pelo tratamento, porém existem riscos cujo tratamento preventivo não é economicamente justificável, como riscos de grande consequência negativa, porém com probabilidade muito baixa de acontecer (INTOSAI, 2007 apud BRASIL, 2014).

A próxima seção explicita e justifica o conjunto de procedimentos metodológicos que ajudaram na investigação do problema e na resposta aos objetivos apresentados.

3 PROCEDIMENTOS METODOLÓGICOS

Dadas as suas características, este estudo se configura como pesquisa descritiva, documental e pesquisa-diagnóstico. É uma pesquisa descritiva, pois, segundo Vergara (2016), busca descrever uma situação em detalhe, especialmente o que se pretendeu neste estudo, descrevendo as características da situação, ou até desvendar a relação entre os eventos. Esta é também uma pesquisa documental, realizada em documentos institucionais, cujos conteúdos serviram para elucidar determinadas questões e legitimar outras. Entre os documentos, a Política de Gestão de Riscos e o Plano Diretor de Tecnologia da Informação da universidade. Esta é uma pesquisa-diagnóstico, pois explorou, levantou e definiu problemas, com a participação de outros membros da comunidade. (ROESCH, 2005; MARTINS; TEÓPHILO, 2009). De acordo com Thiollent (1997), um processo de diagnóstico é interativo quando os pesquisadores adotam uma metodologia cuja natureza possibilita a ampla troca de informações com os interessados. De acordo com o autor, a contribuição dos membros da situação problema é uma condição bastante satisfatória para o diagnóstico ser mais bem informado e contextualizado.

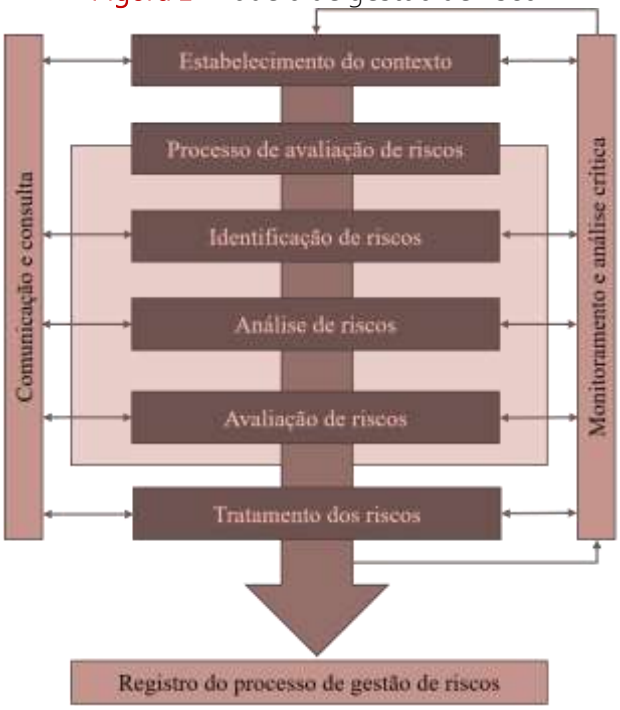
O processo de coleta de dados ocorreu no período compreendido entre os dias 16 de janeiro de 2020 e 28 de fevereiro de 2020. Iniciou com a formação de um grupo de discussão com servidores técnico-administrativos, professores e prestadores de serviço terceirizados que atuavam na unidade de educação a distância da universidade. Na primeira reunião, após explicar o objetivo da pesquisa, os procedimentos metodológicos e alguns dos documentos oficiais que seriam consultados nas reuniões, foi colhida a assinatura do Termo de Conhecimento Livre e Esclarecido. Cada reunião durou em média duas horas e contou com a participação de todos os membros.

O grupo de discussão seguiu as orientações dadas por Ibáñez (2003) e Gutiérrez (2011), de modo que o objetivo maior foi buscar uma cooperação prática para realizar uma tarefa que exigia o horizonte de um consenso. Nesse contexto, cada participante deu sua parcela de contribuição até que se atingisse o consenso sobre os objetivos desta investigação. Os integrantes também assimilaram a ideia de que esta é uma pesquisa diagnóstico, pois, como defenderam Roesch (2005) e Martins e Theóphilo (2009), foram explorados, levantados e definidos problemas, com a participação de outros membros da comunidade. Além disso, todos os participantes contribuíram, de modo que foi possível criar condições bastante satisfatórias para lidar com a situação problema proposta.

O primeiro objetivo do grupo consistiu em aprofundar o conhecimento acerca do tema "gestão de riscos" e acerca da Política de Gestão de Riscos, instituída na universidade. Posteriormente, o grupo identificou quais são os operadores de *e-mails*, os aplicativos móveis, como o WhatsApp, e os demais meios de disseminação de informação usados na unidade acadêmica. Após duas reuniões, o grupo de discussão identificou uma série de riscos inerentes ao uso de meios de comunicação digitais não oficiais para a disseminação e recuperação de informação na unidade acadêmica de educação a distância.

O modelo selecionado para identificar e analisar os riscos do uso de meios de comunicação – tecnologias móveis e *e-mails* de provedores não oficiais – foi o recomendado pelo TCU (BRASIL, 2018a), representado na Figura 1.

Figura 1. Modelo de gestão de risco



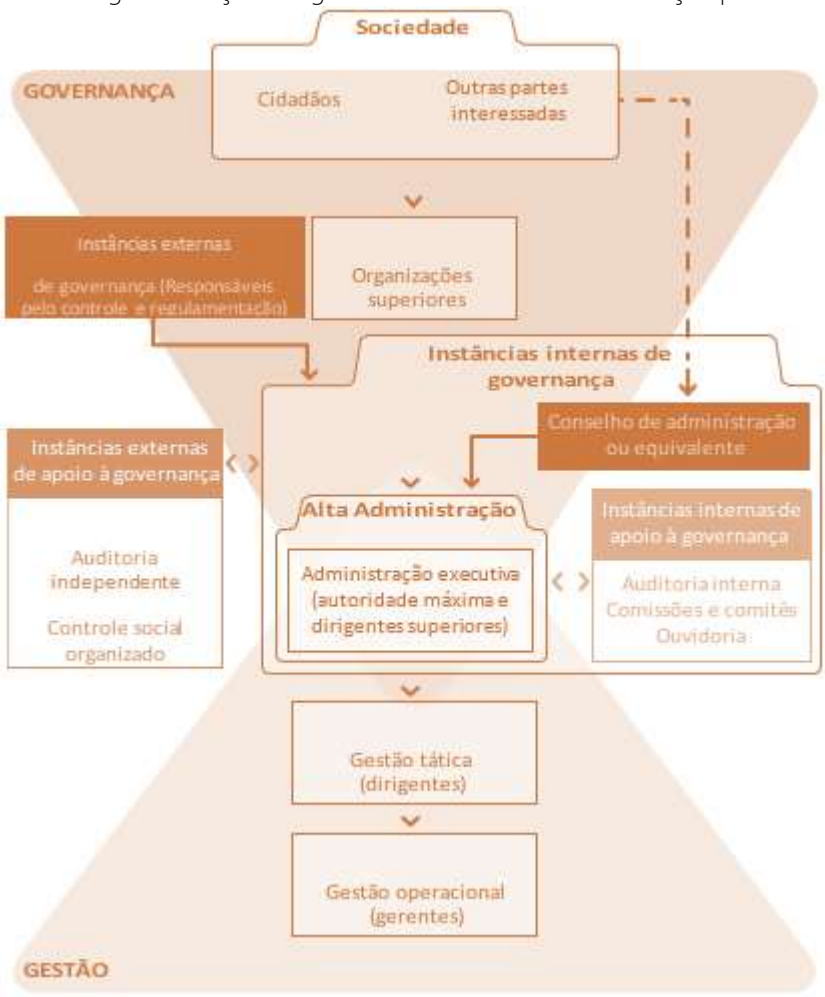
Fonte: adaptado de Brasil (2018a)

O modelo descreve o processo de gestão de riscos de acordo com a norma ISO 31000 (ABNT, 2009). Na apresentação dos resultados são detalhadas as etapas constantes na Figura 1 e demonstradas suas finalidades na gestão de riscos.

A Comunicação e consulta (Figura 1) é um modo de assegurar que, durante todas as etapas ou atividades da elaboração do plano de gestão de riscos, fosse mantida comunicação informativa e consultiva entre os servidores da unidade acadêmica EaD da universidade e as partes interessadas, internas e externas, para auxiliar a estabelecer o contexto apropriado e assegurar que as necessidades e preocupações das partes interessadas fossem consideradas no processo.

O estabelecimento do contexto requer a identificação dos fatores do ambiente interno e externo da universidade (Figura 2).

Figura 2. Sistema de governança de órgãos e entidades da administração pública



Fonte: Brasil (2014, p. 28).

Em um primeiro momento, esse exercício ajudou a evidenciar as principais partes interessadas (*stakeholders*) que, atuando internamente ou externamente à universidade, influenciam e são influenciadas pelas atividades da unidade acadêmica de educação a distância. As partes interessadas foram incluídas em cada etapa ou ciclo do processo de gestão de riscos, por meio do processo de comunicação e consulta, como visto anteriormente. Esta etapa foi realizada por meio da análise documental para identificação tanto dos *stakeholders* quanto de seus interesses, mediante uso da Matriz RACI (acrônimo em inglês para: *Responsible*, *Accountable*, *Consulted* e *Informed*), uma técnica para atribuir responsabilidades, consultar e informar as partes interessadas sobre uma atividade ou projeto em andamento. A Matriz RACI apresenta, de forma tabular, o relacionamento entre atividades e papéis, indicando: responsável (R) por executar uma atividade (o executor); autoridade (A) – quem deve responder pela atividade, o dono; o consultado (C), quem deve ser consultado e participar da decisão ou atividade no momento em que for executada; o informado (I), quem deve receber a informação de que uma atividade foi executada (EMBRAPA, 2014).

O objetivo da etapa de identificação dos riscos da Figura 1 foi produzir uma lista abrangente de riscos, incluindo fontes e eventos de riscos que poderiam ter algum impacto na consecução dos objetivos identificados na etapa de estabelecimento do contexto (BRASIL, 2018a). O envolvimento da equipe dos participantes que atuavam na unidade acadêmica de educação a distância ajudou a criar a responsabilidade em relação ao processo de gestão e o

comprometimento em relação ao tratamento dos riscos.

Os riscos foram categorizados de acordo com o padrão em uso na universidade, constantes em sua Política de Gestão de Riscos, como se segue:

a) Operacionais – Eventos que podem comprometer as atividades do órgão ou entidade, normalmente associados a falhas, deficiências ou inadequação de processos internos, pessoas, infraestrutura e sistemas.
b) Financeiros/orçamentários – Eventos que podem comprometer capacidade do órgão ou entidade de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que podem comprometer a própria execução orçamentária.
c) De imagem/reputação – Eventos que podem comprometer a confiança da sociedade (ou de parceiros, de clientes ou de fornecedores) em relação à capacidade do órgão ou da entidade de cumprir sua missão institucional.
d) Legais/de conformidade – Eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do órgão ou entidade.
e) Ambientais – Resultam da associação entre os riscos naturais e os riscos decorrentes de processos naturais agravados pela atividade humana e pela ocupação do território.

Cada evento de risco pode estar contido em mais de uma categoria. Além de categorizado, cada risco identificado foi apresentado junto a suas prováveis causas, efeitos e consequências. Considerando o que diz a ABNT (2009), a análise de riscos (constante na Figura 1) é o processo de compreender a natureza e determinar o nível de risco. "O risco é uma função tanto da probabilidade como da medida das consequências." (BRASIL, 2018a, p. 25). Desse modo, o nível do risco é expresso pela combinação da probabilidade de ocorrência do evento e das consequências resultantes no caso de materialização do evento.

Logo, seguindo as orientações de Brasil (2018a), o resultado da análise de riscos foi o de atribuir uma classificação a cada risco identificado, tanto para a probabilidade como para o impacto do evento, cuja combinação determinou o nível do risco. A identificação dos fatores que afetaram a probabilidade e as consequências também fizeram parte da análise de riscos, incluindo a apreciação das causas, as fontes e as consequências positivas ou negativas do risco, expressas em termos tangíveis ou intangíveis.

Dada a natureza do risco, a análise de riscos se configurou em uma combinação de uma avaliação mista: qualitativa e quantitativa. A análise qualitativa definiu o impacto, a probabilidade e o nível de risco por qualificadores como "extremo", "alto", "médio" e "baixo", com base na percepção dos servidores e funcionários terceirizados que compunham o grupo de discussão. A análise quantitativa usou escalas numéricas previamente convencionadas para mensurar a consequência e a probabilidade, as quais foram combinadas, por meio de uma fórmula[1], que foi vista em detalhes na análise de dados, para produzir o nível de risco.

A análise quantitativa necessita de dados factuais, porém, se faltarem essas informações e essa análise não for possível, embora desejável, a utilização de um método qualitativo, combinado com análises mistas, baseado na opinião de especialistas, pode ser suficiente e eficaz (ABNT, 2012). "Em análises mistas, considerando que a lógica subjacente seja que o nível de risco é proporcional tanto à probabilidade como ao impacto, a função 'Risco' será essencialmente um produto dessas variáveis." (BRASIL, 2018a, p. 25).

Seguindo as orientações de Brasil (2018a), a relação entre os riscos e os seus componentes utilizada neste estudo é ilustrada por meio de uma matriz simples (Figura 3).

[1] P X I = Classificação de Risco, onde - Probabilidade (P) X Impacto (I)

Figura 3. Matriz de risco simples

Fonte: Brasil (2018a, p. 26).

Como o foco desta pesquisa reside apenas na análise do risco inerente[2], optou-se por utilizar uma escala de classificação de riscos proposta por Brasil (2018a), que assim quantificou os riscos: Risco Baixo – RB (0-9,99); Risco Médio – RM (10-39,99); Risco Alto – RA (40-79,99) e Risco Extremo – RE (80-100). Para elaboração dessa análise mista foram utilizadas escalas, como as exemplificadas no Quadro 1, para estabelecer um entendimento comum das classificações de probabilidades e impactos.

Quadro 1. Escala de probabilidades e consequências

PROBABILIDADES	
Descrição da probabilidade, desconsiderando os controles	PESO
Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	1
Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	2
Possível. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	5
Provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	8
Praticamente certa. De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.	10
CONSEQUÊNCIAS	
Descrição do impacto nos objetivos, caso o evento ocorra	PESO
Mínimo impacto nos objetivos (estratégicos, operacionais, de informação, comunicação/divulgação ou de conformidade).	1
Pequeno impacto nos objetivos (idem).	2
Moderado impacto nos objetivos (idem), porém, recuperável.	5
Significativo impacto nos objetivos (idem), de difícil reversão.	8
Catastrófico impacto nos objetivos (idem), de forma irreversível.	10

Fonte: Adaptado de Brasil (2018a).

[2] O nível de risco inerente de um evento é o nível de risco antes da consideração das respostas que a gestão adota, incluindo controles internos, para reduzir a probabilidade do evento e/ou os seus impactos nos objetivos. Resulta da combinação da probabilidade com o impacto. O risco residual é aquele ao qual uma organização está exposta após a implementação de ações gerenciais. O tratamento desse risco aqui não seria possível, uma vez que nenhuma ação gerencial havia sido ainda implementada.

Depois, os resultados das combinações de probabilidade e impacto, classificados de acordo com a escala de níveis de risco proposta por Brasil (2018a), foram expressos em uma matriz, como a exemplificada na Figura 4.

Figura 4. Matriz de risco completa

IMPACTO						
	Muito Alto - 10	10 RM	20 RM	50 RA	80 RE	100 RE
	Alto - 8	8 RB	16 RM	40 RA	64 RA	80 RE
	Médio - 5	5 RB	10 RM	25 RM	40 RA	50 RA
	Baixo - 2	2 RB	4 RB	10 RM	16 RM	20 RM
	Muito Baixo -1	1 RB	2 RB	5 RB	8 RB	10 RM
		Muito Baixa (1)	Baixa (2)	Média (5)	Alta (8)	Muito Alta (10)
		PROBABILIDADE				

Fonte: Brasil (2018a, p. 28).

Essas escalas poderão ser adaptadas de modo a se tornarem mais compatíveis com o contexto e o objeto em estudo. A finalidade da avaliação de riscos, etapa constante na Figura 1, é auxiliar na tomada de decisões sobre quais riscos necessitam de tratamento e a prioridade para a implementação do tratamento (BRASIL, 2018a). Envolve determinar se o risco e sua magnitude são aceitáveis ou toleráveis ou se algum tratamento é exigido (ABNT, 2009). Como se lê no Quadro 2, tudo é avaliado em relação ao apetite de risco. O apetite a risco é a quantidade de risco que uma organização está disposta a aceitar na busca de seus objetivos (INTOSAI, 2007 apud BRASIL, 2014)..

Quadro 2. Diretrizes para priorização e tratamento de riscos

Nível de risco	Critérios para priorização e tratamento de riscos
RE	Nível de risco **muito além do apetite a risco**. Qualquer risco neste nível deve ser comunicado à governança e alta administração e ter uma resposta imediata. Postergação de medidas, só com autorização do dirigente máximo.
RA	Nível de risco **além do apetite a risco**. Qualquer risco neste nível deve ser comunicado à alta administração e ter uma ação tomada em período determinado. Postergação de medidas, só com autorização do dirigente de área.
RM	Nível de risco **dentro do apetite a risco**. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da gerência na manutenção de respostas e controles para manter o risco neste nível, ou reduzi-lo sem custos adicionais.
RB	Nível de risco **dentro do apetite a risco**, mas é possível que existam oportunidades de maior retorno que possam ser exploradas assumindo-se mais riscos, avaliando a relação custo X benefícios, como diminuir o nível de controles.

Fonte: Brasil (2013 apud BRASIL, 2018a, p. 32).

Nesta etapa, portanto, se fez uso da compreensão e do nível do risco obtidos na etapa de análise de riscos para tomar decisões acerca dos riscos analisados, em especial:

a) Se um determinado risco precisava de tratamento e a prioridade para isso;
b) Se uma determinada atividade deveria ser realizada ou descontinuada;
c) Se controles internos deveriam ser implementados ou, se já existissem, se deveriam ser modificados, mantidos ou eliminados.

Para apoiar o processo de avaliação de riscos foram estabelecidos critérios para priorização e tratamento associados aos níveis de risco (nível recomendado de atenção, tempo de resposta requerido, quem deve ser comunicado, etc.), elaborados com base no exemplo de

Brasil (2018a), apresentado no Quadro 2, que foi o ponto de partida do processo avaliativo de priorização dos riscos. Mesmo tendo ciência de que existem quatro níveis de prioridade, a averiguação dos dados pode levar ao não preenchimento de todas as categorias de prioridade, sendo possível que alguns deles se repitam em dados diversos.

Portanto, considerando que o processo de tratamento é cíclico (BRASIL 2018a), ou seja, o próprio tratamento dos riscos pode levar a outros riscos, inclusive alguns que antes sequer existiam, neste estudo, fundamentado em ABNT (2009), o tratamento incluiu:

a) Uma avaliação para verificar se os níveis de risco residual eram toleráveis;
b) Nos casos em que não eram, definição e implementação de tratamento adicional;
c) Avaliação da eficácia desse tratamento.

Por fim, ainda se referindo à Figura 1, o monitoramento e análise crítica constituem a etapa essencial da gestão de riscos e têm por finalidade:

d) Detectar mudanças no contexto externo e interno, incluindo alterações nos critérios de risco e no próprio risco, que podem requerer revisão dos tratamentos de riscos e suas prioridades, assim como identificar riscos emergentes;
e) Obter informações adicionais para melhorar a política, a estrutura e o processo de gestão de riscos;
f) Analisar eventos, mudanças, tendências, sucessos e fracassos e aprender com eles;
g) Assegurar que os controles sejam eficazes e eficientes no projeto e na operação.

Embora acompanhar esta etapa não faça parte deste estudo, nem sejam aqui apresentadas diretrizes de monitoramento, chama-se a atenção para as responsabilidades relativas ao monitoramento e à análise crítica, que têm como função assegurar que o registro de riscos seja mantido atualizado, bem como que nele sejam documentados os resultados das ações mencionadas.

4 APRESENTAÇÃO DOS RESULTADOS

A apresentação dos resultados evidencia as partes interessadas (*stakeholders*) que atuam interna ou externamente à universidade, influenciam e são influenciadas pelas atividades da unidade acadêmica de educação a distância.

Atualmente, o provedor de *e-mail* oficial da universidade é o Zimbra, mas estão em operação na referida unidade acadêmica o Outlook, Gmail, Uol, Yahoo, entre outros. Além desses, usa-se o aplicativo de mensagens instantâneas WhatsApp, embora não haja normativa que oriente sua utilização de forma oficial. Mas é por meio dele que solicitações são feitas, comunicados são compartilhados, documentos diversos são enviados, recebidos e armazenados, reuniões são marcadas e todo tipo de comunicação informacional e interacional é viabilizado. Há, inclusive, um grupo de servidores da universidade intitulado “EaD Notícias” que o utiliza para fins de compartilhamento de informações. Ou seja, professores, técnicos e prestadores de serviços trocam informações sobre a universidade e seu cotidiano por essa via. Pelo grupo circulam tanto informações oficiais, a exemplo de cópia de ofícios, resoluções internas, agendamento de reuniões de comissões e grupos de trabalho, como também informações que não necessariamente precisam percorrer algum fluxo institucional formal, que chamaremos aqui de informações não oficiais da universidade, como reuniões informais, comunicados diversos, confraternizações, entre outros.

O WhatsApp também é usado por grupos menores e mais restritos. Os servidores técnico-administrativos da unidade acadêmica de educação a distância, por exemplo, organizaram um grupo fechado chamado de “TecAdmEad”. Nele também são compartilhadas

informações diversas, nos mesmos moldes do "EAD Notícias". Partindo desse levantamento, se supõe que existam mais grupos virtuais formados apenas por professores, prestadores de serviços, gestores e assim por diante.

Não há menção sobre os provedores de *e-mail* comerciais, ou mesmo sobre os mensageiros digitais instantâneos no Plano de Desenvolvimento Institucional (PDI) que está em vigor, e tampouco na sua Política de Gestão de Riscos, tal como explicitada no Plano Diretor de Tecnologia da Informação (PDTI) vigente, mesmo sendo de conhecimento amplo e irrestrito o seu uso para fins diversos dentro da universidade**.** Porém, em 2018 foi criada formalmente a Coordenadoria de Gestão de Riscos, designada como responsável pela elaboração e aprovação do Plano de Gestão de Riscos, no qual constará a metodologia de gerenciamento de riscos na instituição. Contudo, o referido documento ainda está em fase de elaboração e não está disponível, sendo assim, não há como saber se os provedores de *e-mail* comerciais, ou mesmo se os mensageiros digitais instantâneos serão ou não contemplados nas ações.

Na universidade, a gestão da comunicação social é realizada pela Coordenadoria de Comunicação Social (CCS), órgão de assessoramento da Reitoria, responsável pelas estratégias e ações voltadas aos públicos internos e externos, e demais questões que permeiam a comunicação social dentro e fora da universidade. A CCS faz uso de mecanismos de divulgação interna, como o *site*, mala-direta via *e-mail* institucional, boletins e publicações diversas, e também externas. O referido órgão é também responsável por gerir os perfis oficiais da universidade nas mídias sociais, sendo elas o Facebook, Twitter, YouTube, Instagram, Flickr e Soundcloud, oficialmente citadas no PDI vigente. Embora acolha informações recebidas por meio de aplicativos de mensagem instantânea não institucionalizados, a CCS não dissemina informação por esse meio.

Por outro lado, uma Resolução do Conselho Universitário trata sobre as Normas da Política de Segurança da Informação e Comunicação (POSIC), com destaque para o art. 6º, que diz que a universidade entende por Informação todos e quaisquer dados, processados ou não, que possam ser utilizados para a produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato. No art. 7º, define comunicações no âmbito da universidade como quaisquer interações que envolvam o envio de dados ou informação entre órgãos ou usuários da universidade ou entre a universidade e pessoas ou instituições externas, utilizando qualquer meio de comunicação. E o art. 9º alerta que todas as informações produzidas, armazenadas ou recebidas pelos usuários da universidade como resultados da atividade profissional pertencem à universidade.

Considerando o uso dos provedores de *e-mail* comerciais, ou mesmo dos mensageiros digitais instantâneos, caso esses dados sejam perdidos ou extraviados, dificilmente o acesso ao *e-mail* e seus dados serão recuperados. Em canais oficiais, o Departamento de Tecnologia da Informação da universidade poderia recuperar tanto o acesso, quanto os dados armazenados.

Neste estudo, governança é o conjunto e a estrutura de liderança (reitoria, diretores, chefias, coordenadores de curso, supervisores, professores, pesquisadores e demais servidores públicos), estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução das políticas da universidade e à prestação de serviços alinhados com as expectativas da comunidade acadêmica e da sociedade. As partes interessadas externas se constituem pelos estudantes atuais e futuros; os empregadores; Ministério da Educação (MEC); o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP), a Capes, a Associação Nacional dos Dirigentes das Instituições Federais de Ensino Superior (ANDIFES); a Controladoria Geral da União (CGU) e o Tribunal de Contas da União (TCU). As partes interessadas internas se constituem pelos integrantes do Conselho Superior; Coordenadoria de Gestão de Riscos; Comitê de Transparência e Dados Abertos; Coordenadoria de Comunicação Social; Conselho de Ensino, Pesquisa e Extensão; Comitê de Tecnologia da Informação;

Departamento de Estatística e Informática; Núcleo de Tecnologia da Informação; os diretores das unidades acadêmicas; a Reitoria; e as Pró-Reitorias.

O Quadro 3 contém o agrupamento de eventos de risco, suas causas e prováveis efeitos e/ou consequências na categoria operacional. Optou-se pela análise somente do Gmail, pois, no período da pesquisa, era o principal provedor de *e-mail* não oficial usado na universidade e, além do mais, as consequências de seu uso são muito semelhantes aos demais, como o Outlook, etc.

Quadro 3. Eventos de risco, suas causas e consequências

Evento	Usar provedores não oficiais tal como o Gmail para envio, recebimento e armazenamento de informações oficiais.	Causas	Facilidade de uso, comodidade, amplitude, ferramentas agregadas, superioridade quando comparado com o provedor oficial.
Consequências	1) Dificuldade na recuperação das informações. 2) Informalidade na comunicação com atores institucionais externos e internos. 3) Falta de padrão na identificação de *e-mails* usuais. 4) Dificuldade na divulgação de canais de atendimento oficiais. 5) A credibilidade da universidade pode ser questionada. 6) Baixa confidencialidade na recuperação e disseminação da informação, tendo em vista que o Gmail não é um provedor institucionalizado na universidade.		
Evento	Usar o WhatsApp para envio, recebimento e armazenamento de informações oficiais.	Causas	Rapidez de acesso, comodidade, diversidade de recursos, possibilidades diversas de uso, recursos diversificados, popularidade, ubiquidade.
Consequências	1) Acesso ao aplicativo ligado a um número de celular; 2) Exposição de seu número pessoal de celular; 3) Dificuldade para desvencilhar (desamarrar, desprender) a vivência pessoal da profissional; 4) Dificuldade na recuperação das informações; 5) Segregação dos colaboradores que não fazem uso do aplicativo; 6) O *backup* de dados é agregado ao número de celular; 7) Risco de vazamento ou perda de informações, no processo de disseminação e armazenamento; 8) Informalidade na comunicação com atores institucionais externos e internos.		
Evento	Uso de redes sociais (Facebook, Instagram, Youtube, Twitter, etc.) para disseminação e recuperação de informações oficiais.	Causas	Alcance das redes sociais, facilidade na divulgação de informações, oferta de canais de atendimento, acesso a recursos diversos e gratuitos, aproximação com o público-alvo.
Consequências	1) Dificuldade na recuperação das informações em ambientes não institucionais; 2) Falta de controle do que é disseminado; 3) Falta de política de gestão da informação; 4) Excesso de informalidade; 5) Necessidade de alocação de recursos humanos para controle e manutenção de cada canal.		
Evento	Usar repositórios *on-line*, como o Google Drive, OneDrive, Dropbox MEGA e outros, para armazenar arquivos oficiais.	Causas	Facilidade, comodidade, amplitude, ferramentas agregadas.
Consequências	1) Dificuldade na recuperação das informações. 2) Risco de vazamento, alterações ou perda de informações:		

	3) Informalidade na comunicação com atores institucionais externos e internos; 4) Credibilidade; 5) Baixa confidencialidade na recuperação da informação, tendo em vista que esses repositórios pertencem a empresas privadas.

Fonte: Adaptado de Lima (2020, p. 63)

Após a identificação e categorização dos riscos, prosseguiu-se para a sua análise e avaliação. Seguindo as orientações de Brasil (2018a), o resultado da análise dos riscos foi o de atribuir a cada um deles uma classificação, tanto para a probabilidade como para o impacto de o evento ocorrer, cuja combinação determinou o nível do risco.

A identificação dos fatores que afetaram a probabilidade e as consequências também fizeram parte da análise de riscos, incluindo a apreciação das causas, as fontes e as consequências positivas ou negativas do risco, expressas em termos tangíveis ou intangíveis. O Quadro 4 a seguir resume essa classificação.

Quadro 4. Avaliação e classificação dos eventos de risco identificados

Nº	Evento de risco	Avaliação do risco			Classificação do risco
		(P)*	(I)**	P X I	
1	Usar provedores não oficiais tal como o Gmail para envio, recebimento e armazenamento de informações oficiais.	10	10	100	RE
2	Usar o WhatsApp para envio, recebimento e armazenamento de informações oficiais.	5	5	25	RM
3	Uso de redes sociais (Facebook, Instagram, Youtube, Twitter, etc.) para disseminação de informações oficiais.	10	8	80	RE
4	Usar repositórios *on-line*, como o Google Drive, OneDrive, Dropbox MEGA e outros para armazenar arquivos oficiais.	10	10	100	RE

*P=Probabilidade, **I=Impacto
Fonte: Adaptado de Lima (2020, p. 64)

Observa-se que, para o grupo de discussão deste estudo, o Risco 1 tem uma probabilidade muito alta de ocorrer. Isso quer dizer que é praticamente certo que ele ocorrerá, sendo-lhe, neste caso, atribuído o peso 10 dentro da escala de probabilidade. Além disso, verificou-se que este evento de risco também tem um impacto muito alto sobre o objetivo proposto, o que lhe conferiu o peso 10 dentro da escala de impacto e consequências. Dessa maneira, com base na escala de classificação de riscos (Brasil, 2018a), o produto probabilidade X impacto do risco em questão equivale a 100, a nota máxima. Com base na matriz de risco constante na matriz de risco completa, tal nota confere a este evento a classificação de Risco Extremo (RE), como se lê no Quadro 4.

O grupo deduziu que a junção do *smartphone* com o acesso ao Gmail atua como catalisador que molda os locais de trabalho e a maneira como os servidores realizam suas atividades e se relacionam com outros servidores públicos e demais públicos-alvo, mesmo se sabendo de que tal aplicação não é o servidor de *e-mail* oficial da universidade. A pesquisa só confirma que o Gmail já faz parte do ambiente informacional da unidade acadêmica de EaD e que boa parte da disseminação da informação é viabilizada por meio dele. Seu uso parece ser tão recorrente que, a depender do modo como a universidade trate esse risco, e conforme a mudança, ela poderá não ter aceitação.

Ao Risco 2 o grupo de discussão atribuiu a probabilidade média. Isso equivale a dizer que o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.

No momento da análise, o grupo concluiu que as características de comunicação instantânea, interatividade e viralização desse aplicativo remetem a um modelo pulverizado em conexões, por vezes, sem controle institucional. Assim, a inferência da equipe de que seu uso para disseminar e recuperar informações dentro da unidade acadêmica é, de fato, um evento de risco, tendo em vista que informações oficiais repassadas de forma imprecisa, ou incompletas, podem atingir um grande número de pessoas rapidamente, vai ao encontro do entendimento de pesquisadores como Rocha, Pereira e Soares (2017). Além disso, o uso indiscriminado da aplicação pode cimentar problemas com questões de imagem e reputação. Assim como ocorreu na análise do Risco 1, neste segundo, o grupo também demonstrou preocupação com a convergência do aplicativo WhatsApp com o *smartphone*, visto que este último é o dispositivo padrão para o uso da aplicação em questão. Da mesma forma como o Gmail, a facilidade e praticidade de acessar o WhatsApp nesse tipo dispositivo avigora a vontade do servidor de utilizá-lo, o que pode dificultar o tratamento desses riscos.

Ainda que tenha ficado claro que o uso do WhatsApp na disseminação e recuperação da informação tem um risco médio, também é notório que ele se encaixa no que os autores chamam de processos intermediários que viabilizam a troca de informações entre as pessoas (LE COADIC, 2004; CHOO, 1998; MCGEE; PRUSAK, 1994). Mas, principalmente, o que vemos aqui é aquilo que Capurro (2017) denominou de o novo imperativo moral que obriga as pessoas a estarem disponíveis e acessíveis o tempo todo e em todo lugar. Essa transformação do código espaço-temporal mediante uma mudança do código tecnológico muda a vida laboral das pessoas, particularmente, desde o ponto de vista de seus códigos sociais, econômicos, políticos e legais. Diante disso, o tratamento desse risco é um desafio cultural no que diz respeito à cultura em informação dos servidores públicos.

O risco 3 foi considerado um Risco Extremo, pois o grupo concordou que sua probabilidade e seu impacto são muito altos, respectivamente, tendo assim peso 10 de probabilidade e 8 de impacto. O grande debate desse ponto girou em torno das questões levantadas por Lemos (2002), quanto às transformações nas práticas sociais, na vivência do espaço urbano e na forma de produzir e consumir informação. Por mais benéficas que sejam essas novas conexões incorporadas nas mídias sociais, o grupo ponderou que disseminar e recuperar informações oficiais a partir delas continua sendo um risco alto, haja vista o pouco controle sobre os perfis usados, sobre as pessoas responsáveis por eles ou ainda sobre a propriedade do dado que é disseminado. Além disso, neste caso podem ser aplicadas algumas observações pontuais, relativas à imagem e à reputação, e de ordem legal e de conformidade, entre outras decorrentes do uso constante do *smartphone.*

Por fim, o Risco 4 foi considerado pelo grupo um risco com um alta probabilidade de ocorrer, atribuído o peso 10 neste quesito. O mesmo peso 10 atribuído no quesito impacto. Dessa forma, o produto da probabilidade X impacto foi 100, resultando em sua classificação de Risco Extremo (RE).

Neste último evento de risco ficou visível a preocupação do grupo no que se refere à dificuldade em efetivar o que é dito na Resolução do Conselho Universitário da universidade, que trata sobre as Normas da Política de Segurança da Informação e Comunicação. A Resolução indica que todas as informações produzidas, armazenadas ou recebidas pelos usuários da universidade como resultados da atividade profissional pertencem à universidade. No entanto, o estudo constatou que todos os repositórios identificados na análise do evento de risco pertencem a empresas privadas, revelando quem são os verdadeiros "donos" das informações ali produzidas e registradas. Tudo isso certamente ajudou o grupo a determinar pela classificação deste como um Risco Extremo (RE), como se lê no Quadro 4.

O Risco 4 está contido no contexto da gestão da informação, especialmente na questão sobre ajustar e aliar as atividades gerenciais e organizacionais e os processos informacionais. É

preciso atentar para o fato de que toda prática de gestão de risco precisa de diretrizes, que podem ser expressas em uma política de informação que, segundo Braman (2006), é um conjunto de leis e regulamentos que estabelecem procedimentos e orientações relativas à criação, ao armazenamento, à disseminação e ao uso da informação. Sem diretrizes claras e instituídas, cada usuário gerenciará a informação à sua maneira, elevando ainda mais o grau dos potenciais eventos de risco. Parte disso parece estar acontecendo no objeto de estudo, pois o grupo de discussão confirmou que múltiplos usuários fazem uso constante de repositórios *on-line* diversos para gerenciar suas informações pessoais e de trabalho.

Seguindo com as orientações de Brasil (2018a), esta é a etapa em que o grupo do diagnóstico opta por evitar, reduzir (mitigar), transferir (compartilhar) e/ou aceitar (tolerar) o risco, devendo-se observar que as opções não são mutuamente exclusivas. O Quadro 5 contém as propostas de tratamento dos riscos identificados, geradas a partir do consenso entre os participantes do grupo de discussão criado para fins desta pesquisa.

Quadro 5. Proposta de Tratamento dos riscos

Nº	Eventos de risco	Tratamento dos riscos
1	Usar provedores não oficiais tal como o Gmail para envio, recebimento e armazenamento de informações oficiais.	Evitar
2	Usar o WhatsApp para envio, recebimento e armazenamento de informações oficiais	Tolerar
3	Uso de redes sociais (Facebook, Instagram, Youtube, Twitter, etc.) para disseminação de informações oficiais.	Mitigar
4	Usar repositórios *on-line*, como o Google Drive, OneDrive, Dropbox MEGA e outros, para armazenar arquivos oficiais.	Transferir

Fonte: Adaptado de Lima (2020, p. 65)

Sobre o Risco 1 – Risco Extremo, as Diretrizes para Priorização e Tratamento de Riscos constantes no Quadro 4 apontam que níveis de risco que vão além do apetite ao risco, ou seja, que vão além da quantidade de risco que uma organização está disposta a aceitar na busca de seus objetivos (INTOSAI, 2007 apud BRASIL, 2014), devem ser comunicados à alta administração e também devem ter uma ação tomada em um período determinado. Isto posto, o Risco 1 será colocado na lista de prioridades na etapa de tratamento dos riscos.

Como é possível ver no Quadro 5, o grupo de discussão sugeriu que a unidade acadêmica em estudo e demais partes interessadas trabalhem em prol de evitar tal risco, ou seja, a universidade precisa evitar usar o Gmail para enviar, receber e recuperar informações oficiais. Sem embargo, seguindo o protocolo sugerido nos procedimentos metodológicos, tal risco identificado, com sua análise e avaliação, será enviado à governança e à alta administração da universidade, que, por sua vez, é quem tem autonomia para tomar as medidas necessárias quanto ao tratamento de tal risco.

Entretanto, é válido deixar registrado que a universidade está estudando e comprometida com um plano de migração do Gmail conta pessoal para o uso das contas coorporativas deste mesmo provedor de *e-mail*, passando, dessa forma, a tratá-lo como um cliente oficial e institucionalizado. Tal ação está sendo acordada pela Reitoria e pelo Núcleo de Tecnologia da Informação e, até o final da apresentação dos resultados desta pesquisa em maio de 2020, esse processo encontrava-se em andamento.

O Risco 2 apresenta um nível dentro do apetite de risco. De acordo com a ABNT (2009), esse apetite seria a quantidade e também os tipos de riscos que uma organização está

preparada para buscar, reter ou assumir. Neste caso, geralmente nenhuma medida especial é necessária, porém, requer atividades de monitoramento específicas dos gestores. Então, esse risco pode ser tolerado.

O Risco 3 apresenta características do Risco 1. Isto é, ambos precisam chegar ao conhecimento da alta administração, que deve tomar medidas visando evitar, mitigar, tolerar ou transferir esse risco. O grupo de discussão desta pesquisa sugeriu, no caso deste risco em específico, que o mesmo seja mitigado. Isso quer dizer que a universidade pode usar as redes sociais para disseminar informações oficiais e para contato síncrono com discentes, porém de maneira mais moderada. As redes sociais têm potencial para se constituírem em recursos de divulgação científica, aproximando cientistas e o público fora do alcance dos meios formais de comunicação científica. A informação científica disponível nas redes sociais demanda organização e sistematização, se espera dos pesquisadores a atenção merecida com relação aos leitores que se configuraram em novos grupos de usuários que acessam tais serviços de informação e comunicação científica.

Por último, o Risco 4 é outro risco extremo que requer atenção (Quadro 5). Neste caso, o grupo entendeu que este risco deveria ser transferido ou compartilhado, tendo em vista que o que está posto à mesa são repositórios *on-line*. Entende-se que o Núcleo de Tecnologia da Informação da universidade pode e deve se envolver na resolução dos possíveis impactos relacionados com o referido risco. No entanto, a migração para as contas coorporativas do Gmail, já citadas no texto que faz referência ao Risco 1, ajudará a evitar ou mesmo a mitigar tal risco, tendo em vista que o referido provedor possui um sistema de armazenamento em nuvem mais robusto. Portanto, o Risco 4 será devidamente reportado à alta administração da universidade para tomar as devidas providências, acatando ou não as sugestões aqui apresentadas.

Por fim, todos os dados coletados e analisados foram encaminhados às partes interessadas internas à universidade, de acordo com a matriz RACI apresentada no Quadro 6, de modo que, se houver disposição para dar seguimento ao processo de monitoramento e análise crítica, a alta administração da universidade terá em mãos todos os resultados desta pesquisa.

Quadro 6. Matriz RACI para tratamento dos riscos identificados

Riscos	Lista de ações			
1	A Unidade Acadêmica está comprometida na migração do Gmail conta pessoal para o uso das contas coorporativas deste mesmo provedor. Tal ação está sendo articulada e providenciada pela Reitoria e Núcleo de Tecnologia da Informação (NTI).			
R (Responsável)		A (Autoridade)	C (Consultado)	I (Informado)
Unidade acadêmica de educação a distância		NTI	Comitê de Tecnologia da Informação (CTI)	Todas as unidades acadêmicas
Riscos	Lista de ações			
2	Promover capacitações do correto uso da ferramenta digital, de modo que seu uso não cause impactos na disseminação e recuperação da informação.			
R (Responsável)		A (Autoridade)	C (Consultado)	I (Informado)
Unidade acadêmica de educação a distância		Reitoria	NTI	Todas as unidades acadêmicas
Riscos	Lista de ações			
3	Promoção de treinamento, capacitações que estimulem o zelo e o cuidado no que confere ao uso de tais ferramentas para disseminação e recuperação da informação.			
R (Responsável)		A (Autoridade)	C (Consultado)	I (Informado)

Pró-Reitoria de Gestão de Pessoas (PROGEPE)	Reitoria	NTI	Todas as unidades acadêmicas
Riscos	Lista de ações		
4	Verificar, junto ao NTI, sobre procedimentos para migração para o repositório corporativo, seja ele próprio ou de algum provedor privado, porém, oficialmente registrado e institucionalizado.		
R (Responsável)	A (Autoridade)	C (Consultado)	I (Informado)
NTI	Reitoria	CTI	Todas as unidades acadêmicas

Fonte: Adaptado de Lima (2020, p. 71)

Muitas vezes, na hora de promover mudanças, os gestores se perdem em alguns detalhes e acabam não definindo claramente as responsabilidades. O Quadro 6 destaca quem são os responsáveis pelas ações que precisam ser tomadas, quem tem autoridade sobre elas, quem ou quais setores da universidade devem ser consultados e quem deverá ser informado sobre tais ações.

Tomando como exemplo o Risco 1: a responsabilidade da migração é da unidade acadêmica de educação a distância, mas quem tem autoridade sobre a ação a ser tomada é o Núcleo de Tecnologia da Informação (NTI), pois se trata de mudanças que requerem o uso de tecnologias diversas que demandam conhecimento técnico específico. Porém, é preciso consultar o Comitê de Tecnologia da Informação (CTI), uma vez que tal comitê é justamente um órgão deliberativo e consultivo da universidade nos assuntos referentes às tecnologias da informação. Por fim, a matriz identifica quem ou quais órgãos precisam ser informados sobre tais ações. Em todos os casos analisados no Quadro 8, todas as unidades acadêmicas serão informadas, haja vista que os riscos enfrentados podem ser os mesmos. E, se não for o caso, tal comunicação servirá ainda como um alerta.

5 CONSIDERAÇÕES FINAIS

Esta pesquisa teve como objetivo principal identificar quais os riscos e qual a magnitude desses riscos na recuperação e uso da informação, devido à adoção de meios de comunicação não oficiais na unidade acadêmica de educação a distância de uma universidade federal. Com base nos aspectos analisados e nos resultados obtidos, constatou-se que há muitos riscos envolvidos nesse processo, alguns deles considerados extremos, indicando que medidas precisam ser tomadas para tratá-los. Os resultados apresentados não apenas identificaram os riscos que podem ter algum impacto nos processos de disseminação, recuperação e uso da informação dentro e fora da unidade acadêmica em estudo, como também mensuraram a sua magnitude.

A análise desses riscos revelou que, dos quatro eventos identificados, três (75%) exigem alguma atenção da administração superior da universidade. Isso porque, como os eventos de risco 1, 3 e 4 foram classificados como riscos extremos, a metodologia adotada neste estudo sugere que níveis de risco que forem além do apetite ao risco, que é o caso em ênfase, devem ser comunicados à alta administração e também devem ter uma ação tomada em um período determinado.

As respostas aos riscos identificados visam minimizar os impactos desses eventos sobre a universidade no que se refere à disseminação e recuperação da informação. A matriz consiste em delimitar quem são os responsáveis pelas ações que precisam ser tomadas, qual é a autoridade dessas pessoas sobre as ações, quem ou quais órgãos serão consultados e quem

deverá ser informado. Ao aderir ao referido método, as partes interessadas são igualmente envolvidas na busca por soluções que intentem reduzir os impactos dos eventos de risco identificados.

O estudo também demonstrou que o bom gerenciamento da informação está intrinsicamente ligado ao contexto informacional no qual a universidade está inserida. Nesse contexto está contido um conjunto de veículos inter-relacionados, como *sites*, aplicativos móveis, redes sociais, telefones, computadores, que facilitam o exame das informações em ambientes de comunicação integrados. O estudo também demonstrou o quão importante é construir uma Política de Gestão da Informação clara e abrangente, de modo que ferramentas diversas estejam habilitadas para contribuir e que pessoas sejam capacitadas para usá-las.

Por fim, mesmo sem ser um dos objetivos originalmente propostos para esta pesquisa, o estudo mostrou as práticas informacionais no ambiente de trabalho e o quão influentes são as tecnologias e as mídias sociais sobre o cotidiano de todos. Foi consensual, no grupo de discussão responsável pela identificação de todos os eventos de risco analisados, que boa parte desses riscos provém da intensa e constante utilização de dispositivos eletrônicos que nos mantêm conectados quase que constantemente, como o celular e o computador pessoal, especialmente quando qualquer um desses possui conexão constante com a Internet. A facilidade de uso dessas ferramentas tecnológicas e suas aplicações diversas terminam por influenciar a forma como trabalhamos, como interagimos e, principalmente, como a informação é disseminada e recuperada.

Durante os estudos foi possível identificar alguns limitadores desta pesquisa, no sentido de que, a princípio, o grupo de discussão formado para identificar e analisar os eventos de risco que impactam no objetivo principal analisado neste estudo não tinha autonomia suficiente para tratar os riscos de forma efetiva.

A pesquisa também não tratou do levantamento dos riscos que poderiam ser gerados com a suspensão da utilização dos serviços analisados. Embora não tenha havido levantamento e análise destes riscos secundários, se questiona qual é o grau de risco a que a universidade poderá ficar exposta se a informação estiver indisponível por um período de tempo.

Também seria de grande relevância a reprodução deste estudo e sua metodologia em outros departamentos, unidades acadêmicas e até mesmo em outros órgãos do Poder Executivo. Embora existam fatores culturais, geográficos e organizacionais que podem influenciar o ambiente de informação do trabalho, também existem pontos em comum que ultrapassam essas fronteiras.

CRediT

RECONHECIMENTOS: Não é aplicável.
FINANCIAMENTO: Não é aplicável.
CONFLITOS DE INTERESSE: Os autores certificam que não têm interesse comercial ou associativo que represente um conflito de interesses em relação ao manuscrito.
APROVAÇÃO ÉTICA: Não é aplicável.
DISPONIBILIDADE DE DADOS E MATERIAL: Não é aplicável.
CONTRIBUIÇÕES DOS AUTORES: Conceitualização, Metodologia, Supervisão, Validação, Visualização, Escrita original: Presser, N. H.; Conceitualização, Investigação Metodologia, Supervisão, Validação, Visualização, Escrita original: Lima, J.A.L.; Análise formal; Supervisão; Escrita - revisão e edição: Silva, E.L.

REFERÊNCIAS

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]. Disponível em: http://www.in.gov.br/. Acesso em: 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. Disponível em: http://www.capurro.de/gonzalezdegomez.pdf. Acesso em: 14 maio 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. Disponível em: https://www.ifac.org/publications-resources/bolt-built. Acesso em: 17 de maio 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. Disponível em: https://revistaseletronicas.pucrs.br/index.php/revistafamecos/article/view/4800. Acesso em: 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. Disponível em: https://doi.org/10.20873/uft.2359-3652.2017v4n2p185. Acesso em: 11 maio 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. Disponível em: https://bit.ly/3kwYQuA. Acesso em: 2 ago. 2019.

Artigo submetido ao sistema de similaridade

Submetido em: 24/09/2020 – Aceito em: 10/02/2021 – Publicado em: 27/02/2021