Revista Gestão & Tecnologia
e-ISSN: 2177-6652
revistagt@fpl.edu.br
http://revistagt.fpl.edu.br/

PROPOSTA DE *FRAMEWORK* DE PLANO DE CONTINUIDADE DE NEGÓCIOS PARA A GOVERNANÇA DE TI NAS ORGANIZAÇÕES

PROPOSAL OF A BUSINESS CONTINUITY PLAN FRAMEWORK FOR IT GOVERNANCE IN ORGANIZATIONS

PROPUESTA DE PLAN DE CONTINUIDAD DE NEGOCIO MARCO PARA EL GOBIERNO DE TI EN LAS ORGANIZACIONES

Vanessa Pereira Jasinski
Mestre em Governança e Sustentabilidade pelo Instituto Superior de Administração e Economia - ISAE
vanessa.pjasinski@gmail.com
https://orcid.org/0000-0002-3559-5222

André Francisco Alves
Doutorando em Administração. Professor colaborador do Programa de Pós-Graduação em Governança e Sustentabilidade (PPGS)
andalves@gmail.com
https://orcid.org/0000-0001-9796-5578

Gustavo Rafael Collere Possetti
Doutor e o mestre em Ciências na área de Engenharia Elétrica e Informática Industrial, pela Universidade Tecnológica Federal do Paraná. Gerente de pesquisa e inovação da Companhia de Saneamento do Paraná.
gustavo_possetti@yahoo.com.br
https://orcid.org/0000-0001-8816-5632

Editor Científico: José Edson Lara
Organização Comitê Científico
Double Blind Review pelo SEER/OJS
Recebido em 19.10.2021
Aprovado em 17.03.2022

RESUMO

Objetivo do estudo: Propor um *framework* de Plano de Continuidade de Negócio (PCN) para auxiliar na Governança de Tecnologia da Informação que possa ser aplicado de forma ágil, colaborativa e com rastreabilidade em uma organização;
Metodologia/abordagem: Realizou-se uma pesquisa de natureza qualitativa-descritiva baseada em duas fases, sendo a primeira de natureza bibliográfica e a segunda inspirada nas metodologias *Design Science Research* e *Design* Participativo;
Originalidade/Relevância: Desenvolveu-se um *framework* que pode ser trabalhado colaborativamente por várias pessoas ao mesmo tempo; que permite a coleta dos dados de forma prática; e com facilidade de atualização por meio da integração entre as informações do *framework* e o PCN em si;
Principais resultados: Como principal resultado, obteve-se um novo *framework* para PCN de TI utilizando recursos de uma plataforma gratuita e que pode ser aplicado de forma ágil, colaborativa e com rastreabilidade em uma organização;
Contribuições teóricas/metodológicas: Como contribuição teórica, tem-se a publicação de um *framework* voltado para a TI no meio acadêmico e alinhado às diretrizes do Disaster Recovery Institute International (DRI) de contemplar estratégias de continuidade de negócios; plano de resposta a incidentes; avaliação de riscos e avaliação de impacto no negócio.

Palavras-chave: *Framework*, Plano de Continuidade de Negócios, Tecnologia da Informação, Governança de TI.

ABSTRACT

Study objective: Propose a Business Continuity Plan (BCP) framework to assist in Information Technology Governance that can be applied in an agile, collaborative and traceable way in organizations;
Methodology/approach: A qualitative-descriptive research was carried out based on two phases, the first being bibliographical and the second inspired by the Design Science Research and Participatory Design methodologies;
Originality/Relevance: The development of a framework that can be worked collaboratively by several people at the same time and that enables the collection of data in a practical and easily updated way through the integration between the framework and the PCN itself;
Main results: A new framework for IT PCN was developed using resources from a free platform and which can be applied in an agile, collaborative and traceable way in an organization;
Theoretical/methodological contributions: As a theoretical contribution, there has been the publication of a framework focused on IT in academia, and that is aligned with the guidelines of the Disaster Recovery Institute (DRI) of contemplating business continuity strategies; incident response plan; risk assessment and business impact assessment.

Keywords: Framework, Business Continuity Plan, Information Technology, IT Governance.

RESUMEN

Objetivo del estudio: Proponer un marco de Business Continuity Plan (BCP) para ayudar en la Gobernanza de la Tecnología de la Información que se pueda aplicar de manera ágil, colaborativa y rastreable en una organización;
Metodología/enfoque: Se realizó una investigación cualitativa-descriptiva, basada en dos fases, la primera bibliográfica y la segunda inspirada en las metodologías Design Science Research y Participatory Design;
Originalidad/Relevancia: Se desarrolló un framework que puede ser trabajado en colaboración por varias personas al mismo tiempo; que permita la recolección de datos de manera práctica; y fácil de actualizar a través de la integración entre la información del marco y el propio PCN;
Principales resultados: Como principal resultado se obtuvo un nuevo framework para TI PCN utilizando recursos de una plataforma libre que puede ser aplicado de forma ágil, colaborativa y trazable en una organización;
Contribuciones teóricos/metodológicos: Como aporte teórico, se encuentra la publicación de un framework enfocado en TI en el ámbito académico y alineado a los lineamientos del Disaster Recovery Institute International (DRI) para contemplar estrategias de continuidad de negocio; plan de respuesta a incidentes; evaluación de riesgos y evaluación de impacto empresarial.

Palabras llaves: Marco, Plan de negocios continuo, Tecnología de la informacion, Gobernanza de TI.

1 INTRODUÇÃO

Na área de Tecnologia da Informação (TI), em que o ritmo de mudança nas Tecnologias da Informação e Comunicação (TIC) é acelerado, as inovações incrementais dificilmente se sustentam isoladamente por muito tempo (Tigre & Noronha, 2013). Conforme descrito por Weill e Ross (2006), aqueles que ocupam cargos gerenciais nas áreas de TI não têm capacidade de atender a todas as requisições de investimento e, se tentarem tomar decisões demais, acabarão se tornando um gargalo. Todavia, ao terceirizar essa tomada de decisão é importante garantir que as decisões tomadas por outras pessoas sejam coerentes com a direção que a alta gerência definiu para a organização. Uma Governança de TI deve proporcionar uma tomada de decisão clara, consistente e que represente a visão da alta gerência.

No novo mercado global, a TI possui um papel estratégico nas organizações. Assim sendo, sua governança deve contribuir para uma melhora na governança corporativa da organização com um todo e, nesse sentido, *frameworks* de melhores práticas em TI têm surgido, especialmente nas últimas duas décadas (Neto & Neto, 2013). Considerando que

imprevistos sempre acontecerão, a área de TI precisa saber como agir diante da ocorrência de um desastre, logo, a existência de uma estratégia de continuidade passa a ser de vital importância para a perenidade das organizações. Ter um Plano de Continuidade de Negócios (PCN) elaborado antes que ocorra a interrupção dos negócios é crucial, ou a organização pode não ser capaz de responder com rapidez suficiente à interrupção dos serviços (Wan & Chan, 2008).

A aplicação de um *framework* para elaboração de PCN já foi contemplada por diversos autores, porém, muitas vezes apresentam-se apenas os elementos-chave para um PCN, sem disponibilizar um *framework* estruturado para aplicação, comportamento este que pode ser observado em Svata (2013); ou os resultados da aplicação sem exibir qual foi o *framework* aplicado, como em Magalhães, Oliveira e Oliveira (2014); ou, ainda, expondo apenas trechos dele, como apresentado por Martins, Wangham e Favarim (2009).

Diante do exposto, esta pesquisa tem como objetivo propor um *framework* de Plano de Continuidade de Negócio para auxiliar na Governança de TI e que possa ser aplicado de forma ágil, colaborativa e com rastreabilidade em uma organização. Aplicar um *framework* pronto para a elaboração de um PCN, e que utilize ferramentas que promovam coleta e análise dos dados necessários de forma ágil, colaborativa e com rastreabilidade pode fazer com que as organizações consigam desenvolver uma primeira versão de seu PCN mais rapidamente e garantir que as etapas necessárias sejam apreciadas.

2 REFERENCIAL TEÓRICO

De acordo com Weill e Ross (2006), um modelo eficaz de governança consiste em um conjunto de arranjos e mecanismos alinhados à estratégia, à estrutura e aos resultados desejados da organização. Os autores apresentam que a Governança de TI deve tratar de três questões:

1) Quais decisões devem ser tomadas para garantir a gestão e o uso eficazes de TI?; 2) Quem deve tomar essas decisões? e 3) Como essas decisões serão tomadas e monitoradas? Weill e Ross (2006) apontam também que arranjos de Governança em TI bem concebidos confiam a tomada de decisões sobre TI às pessoas responsáveis pelos resultados, e essas pessoas não necessariamente estarão dentro da área de TI. O conceito de Governança de TI, por meio da adoção de modelos de melhores práticas em Gestão de TI, propõe caminhos para que os

serviços prestados por esta área tragam apoio efetivo ao negócio, tanto do ponto de vista de seus usuários (internos) quanto de seus clientes (externos) (Klumb & Azevedo, 2014). Logo, a importância de um PCN dentro da governança está relacionada à sua capacidade de garantir que as demandas atuais e futuras da organização sejam atendidas.

Conforme a ABNT (2020a, p. 12), Plano de Continuidade de Negócios é a "informação documentada que orienta a organização a responder a uma disrupção e retomar, recuperar e restaurar a entrega de produtos e serviços de acordo com os objetivos de continuidade de negócios". Ou seja, tanto a Governança de TI como um PCN devem ter por finalidade garantir que os objetivos estratégicos da organização sejam alcançados e, nesse contexto, as estratégias de continuidade constituem parte de uma governança corporativa bem estruturada e que apoie a gestão dos controles internos. Tarouco e Graeml (2011) expõem que a preocupação com os riscos de falhas associadas à TI impactarem a saúde das empresas tem sido tanta que alguns conjuntos de práticas têm surgido e sido adotados pelas organizações com o intuito de evitar, ou ao menos reduzir, as chances de percalços com a tecnologia afetarem negativamente os negócios. O *Disaster Recovery Institute International* (DRI), por exemplo, é um instituto internacional sem fins lucrativos fundado em 1988 que tem como missão ajudar organizações a se prepararem para e se recuperarem de desastres (DRI, 2021) e, dessa forma, reduzirem as chances de incidentes relacionados à tecnologia impactarem negativamente os negócios. No conteúdo de seus cursos, o DRI defende que um programa de continuidade de negócios deve abranger: definição das estratégias de continuidade de negócios; plano de resposta a incidentes; avaliação de riscos e avaliação de impacto no negócio.

A análise de impacto no negócio (*Business Impact Analysis* – BIA) é um instrumento do PCN que auxilia no aumento do conhecimento sobre a organização. Svata (2013) pontua que a BIA é parte fundamental da gestão da continuidade, uma vez que consiste em uma análise de todo o negócio que identifica os recursos e as funções críticas e os prazos dentro dos quais devem ser restaurados após uma interrupção. Sob o espectro de TI, Swanson *et al.* (2002) definem a BIA como uma análise dos requisitos, processos e interdependências de TI utilizada para definir prioridades de contingência de sistemas no caso de uma interrupção significativa.

Se o PCN tem por objetivo fazer com que não sejam ultrapassados os tempos em que os impactos de um incidente se tornam inaceitáveis para a continuidade dos negócios de uma

organização, identificar o RTO e o RPO significa descobrir quais seriam esses tempos. De acordo com a ISACA (2011), RTO é o tempo definido para a retomada da entrega do produto, serviço ou atividade após um incidente. Antes dele, o incidente ainda pode ser gerenciado. Depois dele, os planos de recuperação devem ser acionados. Para as áreas de negócio, isso significa executar seus Planos de Continuidade Operacional (PCO), enquanto para a TI, o Plano de Recuperação de Desastres (PRD). A ISO/TS 22317:2020 (ABNT, 2020b, p. 19) apresenta o conceito de RPO como "perda máxima de dados". Logo, é o período máximo de informações que poderiam ser perdidas sem que houvesse prejuízo que impactasse na continuidade de negócio, ou seja, o tempo em que os prejuízos ainda seriam administráveis (Chagas, 2017).

De acordo com Lento e Luz (2014), independentemente do método utilizado para determinar o impacto relacionado a um sistema, os donos dos sistemas e das informações são os únicos responsáveis em esclarecer o nível de impacto em termos de perdas ou degradação de qualquer uma das propriedades de segurança ou pela combinação delas entre si. Isso reforça a necessidade de que a BIA seja feita com envolvimento de representantes das áreas de negócio da organização, e não apenas envolvendo colaboradores de TI.

O item "Planos de resposta a incidentes" preconizado pelo DRI pode ser subdividido em 3 planos principais: Planos de Emergência (PEs); Plano de Gestão de Crises (PGC); e Plano de Comunicação (PCOM). PEs são os procedimentos executados imediatamente após uma interrupção nos negócios (Nonprofit New York, 2013). Possuem foco na proteção de vidas e alguns exemplos de ocorrências que poderiam ser temas para a construção de PEs são: abandono de edificação, combate a incêndio, invasão/roubo/furto, incidentes envolvendo feridos/vítimas, produtos químicos ou materiais perigosos (Daryus Educação, 2020).

Já um PGC aborda o desenvolvimento de uma capacidade de resposta a emergências/desastres eficaz e eficiente em toda a organização. A ISO/TS 22317:2020 (ABNT, 2020b) apresenta algumas estratégias básicas que devem ser avaliadas pelas organizações para permitir resposta e recuperação efetivas de um incidente disruptivo: disposições alternativas do local de trabalho; disposições alternativas da cadeia de suprimentos; opções de recuperação de Tecnologias de Informação e Comunicação (TIC); fontes alternativas de pessoas e fontes alternativas de equipamentos. A principal diferença entre os PEs e um PGC é que este é orientado a cenários de crises ou desastres.

Um PCOM, de acordo com o Plano de Contingência de Tecnologia da Informação e Guia de Planejamento da Universidade de Connecticut (UITS, 2012), serve para fornecer procedimentos para disseminação de comunicações internas e externas, e controlar rumores.

Em TI, os planos de contingência são também chamados de Planos de Recuperação de Desastres (do inglês *Disaster Recovery* – DR). Hearnden (1995) reforça a importância de os PRDs serem relevantes para tratar as questões de negócio identificadas por meio da BIA, ao invés de questões puramente técnicas associadas à recuperação de *hardware*, redes e *software*.

3 METODOLOGIA

Este trabalho teve início no Departamento de TI de uma Instituição de Ensino (IES), motivado pelo interesse desta em identificar as boas práticas existentes no que tange à continuidade de negócios em TI e com o intuito de desenvolver internamente os meios necessários para apoiar os negócios. A pesquisa pode ser classificada como qualitativa e descritiva (conforme Creswell, 2014 e Gil, 2010), uma vez que buscou a análise da realidade operacional pesquisada e de como estão organizadas as atividades dentro dos setores que compunham o Departamento de TI da instituição na qual parte da pesquisa foi realizada. Esta pesquisa também pode ser classificada como empírica, uma vez que foram coletados dados *in loco*, a partir de entrevistas com pessoas com experiência e vivência no tema estudado.

Desta forma, esta pesquisa foi realizada em duas etapas distintas. A primeira se constituiu de um levantamento bibliográfico de *frameworks* para elaboração de PCN existentes, com o intuito de aprofundar o entendimento das características de tais para embasamento teórico e proposição de um novo *framework*. As categorias e os itens considerados para composição do *framework* construído por meio desta pesquisa tiveram origem, em sua maioria, nesta etapa do trabalho.

A técnica empregada para converter os *frameworks* avaliados em itens propostos para a construção de um novo *framework* foi análise de conteúdo (Bardin, 1977), uma vez que a iniciativa consistiu em explicitação e sistematização do conteúdo das mensagens (itens dos *frameworks* avaliados) e da expressão deste conteúdo (formato dos *frameworks* avaliados). Essa abordagem teve por finalidade efetuar deduções lógicas e justificadas, referentes aos modelos levados em consideração, tendo em mente a questão que se buscou resolver.

Seguindo os preceitos do trabalho de Moraes (1999) sobre análise de conteúdo, a atividade de preparação de informações apresentada na Figura 1 correspondeu à identificação dos *frameworks* a serem analisados. Para isso, todos os modelos encontrados foram avaliados quanto à sua pertinência em relação aos objetivos da pesquisa. Os *frameworks* incluídos na amostra foram considerados representativos, abrangentes e pertinentes aos objetivos da análise.

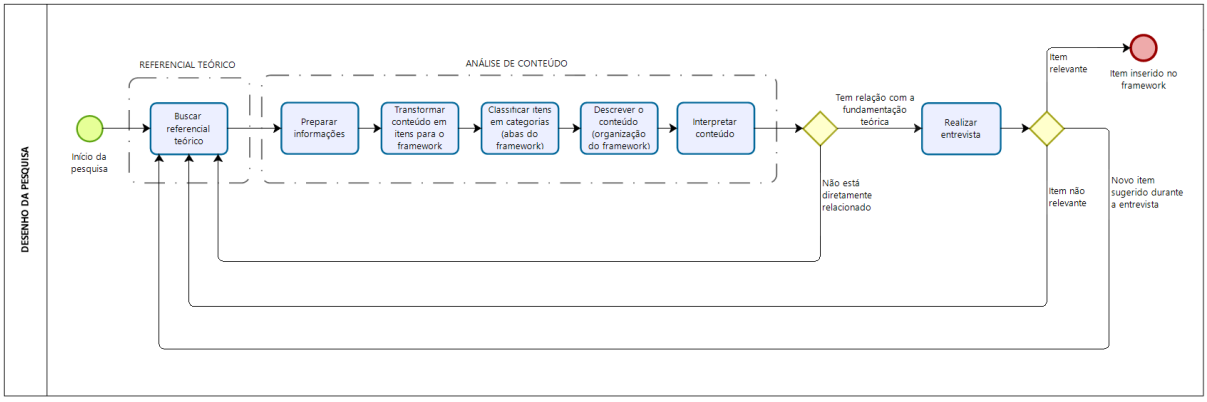

Figura 1 – Desenho da pesquisa
Fonte: Autores.

A segunda etapa se deu por meio de entrevistas não estruturadas com o principal intuito de validar o *framework* em desenvolvimento. O roteiro de entrevista, ou seja, o que norteava a condução das entrevistas era a versão vigente do *framework* em desenvolvimento, com as etapas para construção do PCN (abas do *framework*) e os novos itens sendo expostos um a um até que fossem definidos todos os itens que passariam a compor o *framework*. Nesta etapa utilizou-se como inspiração para a condução desta pesquisa o método *Design Science Research* (DSR), ou "pesquisa *Design Science*". De acordo com Dresch e Lacerda (2016), os produtos gerados pela DSR são chamados de artefatos e devem ter como objetivo a redução do distanciamento entre teoria e prática. Em DSR, até que se obtenha um artefato, a pesquisa deve passar por um ciclo de: 1) Definir o problema, 2) Sugerir, 3) Desenvolver, 4) Avaliar e 5) Concluir. O papel do pesquisador, em DSR, é ser o construtor e/ou o avaliador do artefato.

Conforme Hevner *et al.* (2004), DSR é essencialmente um processo de busca até que se descubra uma solução eficaz para um problema. Ou seja, a ciência por trás de DSR é inerentemente iterativa. Assim sendo, o presente estudo inspirou-se neste método com o intuito de encontrar uma solução prática e viável para um problema, a partir de

fundamentação teórica, buscando reduzir o distanciamento entre teoria e prática, passando por um ciclo de avaliação do artefato (como apresentado na Figura 1) e, assim, obtendo um produto final (*Framework* para PCN de TI), o qual pode ser generalizável para aplicação na área de TI de qualquer tipo de organização.

A pesquisa também se inspirou em *Design* Participativo, um processo que envolve ativamente as partes interessadas para ajudar a garantir que o resultado atende suas necessidades e é utilizável (Hartson & Pyla, 2019). Na maioria das vezes em que é aplicado, *Design* Participativo é usado no modo consultivo, em que os usuários participam na formação de partes do *design*, mas quem está conduzindo o trabalho possui a responsabilidade final pelo *design* geral (Muller & Kuhn, 1993).

Dessa forma, os ciclos iterativos representados na Figura 1 foram realizados entre março e setembro de 2020, sendo que cada entrevista resultou em uma nova versão do *framework*, até que se contemplaram os principais temas necessários para elaboração de um PCN para TI.

Por último neste trabalho, o conteúdo obtido a partir das etapas anteriores foi estruturado utilizando recursos de uma plataforma gratuita e, para tanto, optou-se pela plataforma Google® para tornar o trabalho de elaboração/revisão do PCN mais ágil. Isso porque, além de os recursos da referida plataforma promoverem maior colaboração entre os usuários e permitirem a rastreabilidade do trabalho desenvolvido, eles permitiram também a criação de automações entre os elementos que compõem o *framework* que podem facilitar a análise dos dados obtidos por meio dos questionários desenvolvidos para a coleta dos dados. Desta forma, a metodologia proposta para elaboração e atualização periódica do *framework* desenvolvido utilizou Formulários, Planilhas e Documentos Google®.

4 APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS

Na condução deste trabalho, realizou-se uma análise comparativa entre os seguintes *frameworks*: MyITpros (2020), Interactive (2019), CPA Australia (2020), RiskSOURCE (2020), AIG (2013), FEMA (2018), LUMIFORM (2020), Research and Markets (2020) e Nonprofit New York (2013). Os elementos que compõem cada um dos *frameworks* mostraram-se bastante variáveis, tanto no formato adotado para coleta dos dados quanto em

relação à nomenclatura adotada. Ainda, nenhum dos modelos encontrados empregou o uso de recursos Google®.

Após a realização da pesquisa bibliográfica e das entrevistas, o *framework* para elaboração do PCN para TI foi estruturado em oito fases principais, as quais estão sumarizadas na Figura 2.

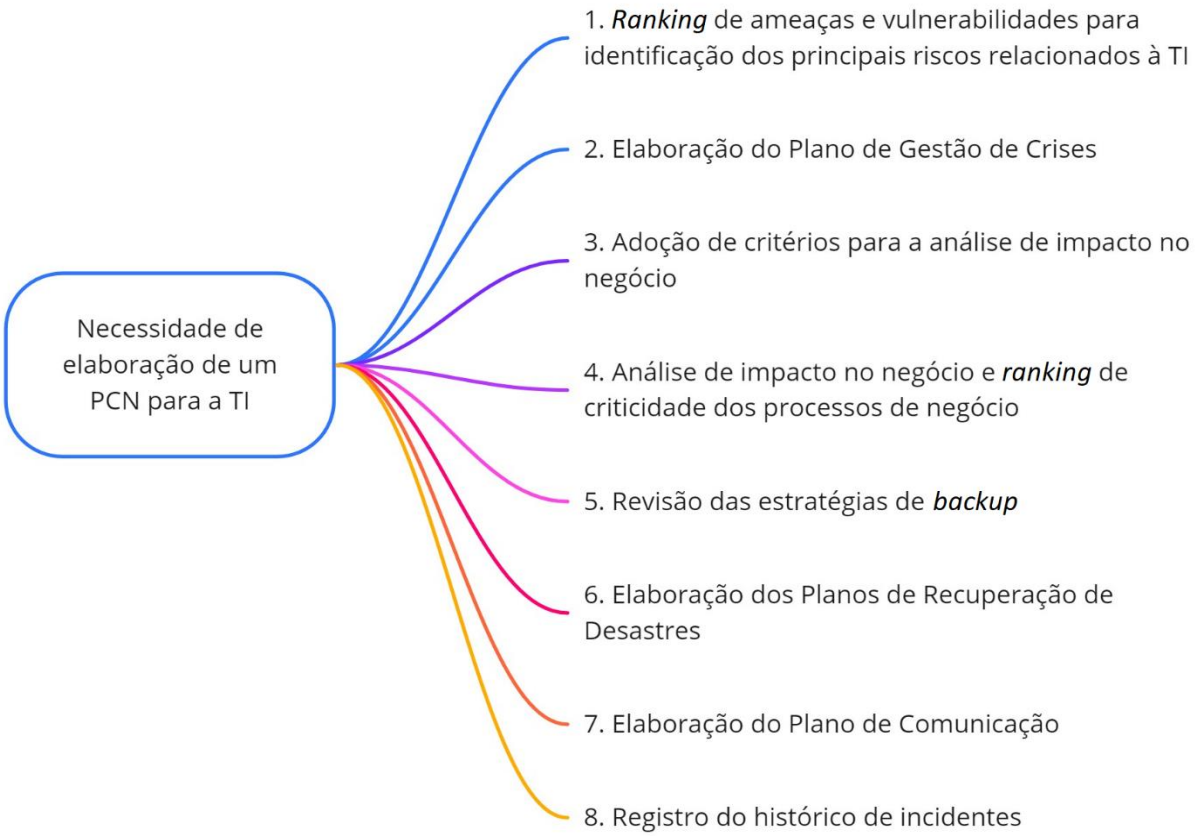

Figura 2 – Fases do *framework* proposto
Fonte: Autores.

Os três primeiros artefatos obtidos são apresentados na Tabela 1. Todos os questionários foram desenvolvidos utilizando os Formulários Google® e com o intuito de coletar dados para preenchimento do *framework.*

Tabela 1
Questionários desenvolvidos para coleta de informações para o PCN de TI

Nº e nome do questionário	*Link* de acesso
Questionário 1 - Identificação dos riscos relacionados à TI	https://docs.google.com/forms/d/e/1FAIpQLSdfFbkU_cn9AuiDwE8uUf0jHJCjcAHt0eNJI68rXdJ0n29kVw/viewform
Questionário 2 - Identificação dos processos apoiados por recursos de TI	https://docs.google.com/forms/d/e/1FAIpQLSeAwZcek6cpI7Xarqys5OMmLnlP9a0G3BMKlh0ffs6wmGjG7w/viewform
Questionário 3 - Identificação dos impactos relacionados aos serviços da TI	https://docs.google.com/forms/d/e/1FAIpQLSejq7CldBy4AaltV4K2XnAqHEb4v-DjHX5_ic3ppnhqkQmGLg/viewform

Fonte: Autores.

As principais ameaças e vulnerabilidades que podem impactar a área de TI e que compõem o Questionário 1 são oriundas de revisão bibliográfica sobre riscos em TI, a saber: NIST (2002), AIG (2013), TechTarget (2017), Martins, Wangham e Favarim (2009) e Daryus Educação (2020), bem como de sugestões provenientes das entrevistas na IES. Todavia, é importante ressaltar que foi prevista no desenvolvimento do questionário a possibilidade de inserção de novos itens durante a aplicação deste, caso alguma ameaça ou vulnerabilidade relevante conforme a realidade de outra organização não tenha sido contemplada, e conforme recomendado por Bannerman (2008).

Após a realização da pesquisa bibliográfica e a análise dos dados obtidos por meio das entrevistas realizadas, identificou-se que, dos três questionários desenvolvidos, o Questionário 1 deve ser aplicado para a TI e os Questionários 2 e 3 devem ser aplicados às áreas de negócio da organização, ou seja, aos responsáveis por cada área organizacional no organograma da empresa. Esse caminho é embasado por Paz (2018), que apontou que para um profissional de TI existem limites do que pode ser feito para criar e implementar um PCN na organização, uma vez que um profissional de TI pode saber como definir permissões para um aplicativo de negócios específico, mas talvez não saiba como os usuários interagem com o aplicativo e qual a real importância dele para o negócio.

Para se chegar a essa proposta de estruturação para o artefato desenvolvido, tomaram-se como base os *frameworks* listados anteriormente. Porém, outros itens também foram inseridos nos questionários e no *framework* a partir de sugestões obtidas conforme o ciclo iterativo já apresentado na Figura 1. Esses itens possuem a origem discriminada como “IES” na Tabela 2. E o resultado final desse trabalho, isto é, a origem de cada um dos itens que compõem o *framework* é apresentada na Tabela 2 bem como o que motivou a inserção de cada um deles.

Tabela 2
Origens dos itens que compõem o *framework* desenvolvido

Aba	Item	Origem	Justificativa da inserção
Riscos	Ameaças e vulnerabilidades percebidas	AIG (2013); Daryus Educação (2020); IES; Martins, Wangham e Favarim (2009); NIST (2002); TechTarget (2017).	Identificar os principais riscos que ameaçam a TI da organização para que possam ser traçados PGCs que mitiguem essas ocorrências.
	Outras ameaças e vulnerabilidades identificadas	IES.	Cobrir eventuais ameaças e vulnerabilidades não identificadas por meio da revisão bibliográfica, possibilitando que os cenários de crise a serem estabelecidos tratem os principais riscos que ameaçam a organização, de acordo com sua realidade.
	Respondente (endereço de *e-mail*)	Registro do *e-mail* de quem respondeu o questionário.	Registrar o histórico das informações e permitir a rastreabilidade.
	Carimbo de data/hora	Registro de data e hora em que o questionário foi respondido.	
Ranking riscos	Ameaças e vulnerabilidades relatadas	Lista as ameaças e vulnerabilidades identificadas pelos respondentes do Questionário 1, bem como outras não previstas inicialmente e por eles relatados.	Ordenar as ameaças e vulnerabilidades relatadas conforme a pontuação dada a cada uma delas, sendo atualizada automaticamente a cada vez que o Questionário 1 é preenchido. Serve para que posteriormente sejam traçados PGCs a partir das ameaças e vulnerabilidades que tiverem a maior quantidade de respostas, considerando impacto e probabilidade de concretização destas.
	Pontuação	Apresenta a quantidade de vezes que cada uma das ameaças e vulnerabilidades foi sinalizada como prioritária pelos respondentes do Questionário 1.	
PGC	Cenário de crise	Deve ter origem nos riscos previstos a partir da avaliação das ameaças e vulnerabilidades previamente realizada por meio do Questionário 1.	Tornar a organização preparada para enfrentar os principais cenários de crise que podem impactar a continuidade do seu negócio.
	Porta-voz	RISKSOURCE (2020); AIG (2013).	Garantir a unicidade das informações divulgadas por meio da definição de um responsável pela comunicação.
	Papéis e responsabilidades	INTERACTIVE (2019); AIG (2013); LUMIFORM (2020).	Expor quem é responsável por executar qual ação e, assim, reduzir os tempos para a tomada de decisões.
	Contatos-chave externos	INTERACTIVE (2019).	Centralizar os meios para contato com os principais parceiros da organização.
	Contatos-chave internos	INTERACTIVE (2019); RISKSOURCE (2020); LUMIFORM (2020a, 2020c).	Explicitar os responsáveis pelo gerenciamento de cada cenário de crise para reduzir os tempos até a tomada de ação.
	PCOM relacionado	AIG (2013).	Fazer a organização refletir antecipadamente

Aba	Item	Origem	Justificativa da inserção
			sobre quem deveria ser comunicado, por que, quando, como e o que comunicar diante de cada cenário de crise.
	PRD relacionado	NONPROFIT NEW YORK (2013).	Explicitar os planos necessários para mitigar a ocorrência dos danos diante cada cenário de crise, bem como eventuais lacunas (planos ainda não existentes que precisam ser desenvolvidos).
	Observações	INTERACTIVE (2019).	Registrar quaisquer outras informações necessárias para que a organização lide adequadamente com os cenários de crise.
Critérios	Tipo de impacto	Tipos de impacto: ISO 22317:2020 (ABNT, 2020b).	Correlacionar os processos de negócio da organização com os impactos previstos para permitir à organização a possibilidade de "calibrar" o peso que determinado tipo de impacto deve possuir sobre seus processos.
	Impacto financeiro	AIG (2013); DARYUS EDUCAÇÃO (2020).	
	Apetite ao risco	AIG (2013).	
PNs	Principais processos realizados pela área	MY IT PROS (2020); INTERACTIVE (2019); RISKSOURCE (2020); AIG (2013); FEMA (2018); LUMIFORM (2020); NONPROFIT NEW YORK (2013).	Identificar quais processos organizacionais precisam ter estratégias traçadas para proteger a continuidade do negócio.
	Sistema/serviço/ recurso de apoio	NIST (2002).	Identificar os recursos de TI que apoiam os processos de negócio, uma vez que os serviços/sistemas/recursos que apoiarem os processos classificados como críticos serão, por consequência, críticos para a TI (NIST, 2002).
	A área tem contingência própria/ Plano de Continuidade Operacional (PCO)?	IES.	Conhecer o quão dependente a área de negócio que irá responder o questionário é dos recursos de TI que apoiam os processos organizacionais.
	Respondente (endereço de *e-mail*)	Registro do *e-mail* de quem respondeu o questionário.	Registrar o histórico das informações e permitir a rastreabilidade.
	Carimbo de data/hora	Registro de data e hora em que o questionário foi respondido.	
Ranking BIA	Processos de negócio (PNs)	Respostas para a pergunta "Quais são os principais processos realizados por sua área?" do Questionário 1.	Identificar os processos organizacionais cujas indisponibilidades possam prejudicar a continuidade do negócio.
	Por quanto tempo o serviço/sistema pode ficar fora do ar (RTO)?	Lento e Luz (2014); LUMIFORM (2020); NONPROFIT NEW YORK (2013).	Identificar o período máximo que um sistema pode ficar indisponível, a fim de evitar consequências inaceitáveis do ponto de vista dos negócios.
	Quanto tempo de informação pode ser perdido (RPO)?		Identificar o período máximo de tolerância em que informações podem ser perdidas ou ficar indisponíveis devido a um incidente, podendo ser representado em minutos, horas ou dias desde a realização do último *backup* (ABRAPP, 2012).

Aba	Item	Origem	Justificativa da inserção
	Probabilidade	MY IT PROS (2020).	Avaliar a probabilidade que determinado impacto tem de se concretizar e efetivamente interromper a continuidade do negócio.
	Financeiro	ISO 22317:2020 (ABNT, 2020b).	Correlacionar o processo com os tipos de impacto previstos pela ISO que trata de Sistemas de Gestão de Continuidade de Negócios, de forma a entender se algum impacto em específico é mais relevante para o processo em questão. É um fator diretamente relacionado ao peso dado para o tipo de impacto na aba Critérios do *framework*.
	Imagem		
	Legal/ regulamentar		
	Contratual		
	Objetivos comerciais		
	Probabilidade x Impacto x Peso	AIG (2013).	Calcular o impacto que cada processo possui na continuidade dos negócios, conforme os tipos de impacto definidos, as probabilidades sinalizadas pelos respondentes e os pesos estabelecidos pela organização na aba Critérios.
	Criticidade do processo	Tem origem nos valores apresentados na coluna anterior do *framework* (Probabilidade x Impacto x Peso).	Ordenar os processos da organização por ordem de criticidade, após a análise do impacto que estes possuem nos negócios e da probabilidade de estes se concretizarem.
	Receita perdida (R$)	AIG (2013); ISO 22317:2020 (ABNT, 2020b); Lumiform (2020b).	Estimar em valores quantitativos qual seria o custo da interrupção em cada um dos processos identificados por meio do Questionário 2.
	Danos à imagem (R$)		
	Não cumprimento de leis/normas (R$)		
	Penalidades contratuais (R$)		
	Não atingimento dos objetivos comerciais (R$)		
	Observações sobre estimativas dos custos dos impactos (multas/contratos)	Tem origem nos valores apresentados nas colunas anteriores do *framework*, para estimativa dos custos relacionados a cada tipo de impacto.	Fornecer ao respondente a possibilidade de detalhar por escrito o que foi considerado para a estimativa do(s) valor(es) apresentado(s) no Questionário 3.
	Respondente (endereço de *e-mail*)	Registro do *e-mail* de quem respondeu o questionário.	Registrar o histórico das informações e permitir a rastreabilidade.
	Carimbo de data/hora	Registro de data e hora em que o questionário foi respondido.	
Backup	Registro, arquivo ou banco de dados essencial	IES; FEMA (2018).	Catalogar todos os ativos de TIC armazenados por meio dos *backups* realizados pela TI.
	Apoia qual(is) PN(s)?	MY IT PROS (2020); FEMA (2018).	Promover maior entendimento sobre quais serviços/sistemas/recursos de TI apoiam quais Processos de Negócio (PNs).
	Periodicidade	IES; FEMA (2018).	Facilitar a comparação entre a periodicidade dos *backups* que está sendo realizada pela TI e o que
	RPO	As informações deste campo	

Aba	Item	Origem	Justificativa da inserção
		serão oriundas da coluna RPO da aba *Ranking* BIA do *framework*, e têm origem na aplicação do Questionário 3.	se espera que seja executado, de acordo com os respondentes do Questionário 3.
	Periodicidade x RPO	IES.	Tornar conhecida a periodicidade de realização dos *backups* realizados pela TI *versus* o tempo de informação que pode ser perdido segundo os donos dos processos, para adequações nas rotinas de *backup*, se necessário.
	Horário de execução	IES.	Mapear e registrar as rotinas de *backup* em prática pela organização.
	Retenção	IES.	
	Locais	IES.	
	Nº de cópias	IES; FEMA (2018).	
	Possui redundância?	IES; NONPROFIT NEW YORK (2013).	
	Tempo para recuperação do ativo (TRA)	INTERACTIVE (2019).	Fazer com que a TI estime o tempo real para recuperação do ativo que suporta o(s) processo(s) de negócio.
	RTO(s) PN(s) x TRA	IES.	Facilitar a comparação entre o tempo de informação que pode ser perdido, conforme o dono do processo, e o tempo que a TI efetivamente leva para recuperar o ativo.
	O que fazer com este risco?	COSO (2007).	Obter uma definição, por alguém com autonomia para tomada de decisão em relação aos investimentos de TI, sobre o que deve ser feito caso sejam identificadas discrepâncias entre o RTO e o tempo estimado para recuperação do ativo.
	Ações para tratar os riscos ou justificativa da aceitação	IES.	Detalhar o que será feito para tratar o risco identificado. Caso opte por aceitar o risco, este campo serve para registro da justificativa.
PRD	Serviço/sistema/ recurso	IES.	Especificar o objeto-alvo do PRD.
	Apoia qual(is) PN(s)?	Deve ter origem nas respostas obtidas para o Questionário 3.	Prover ciência sobre quais processos de negócio são apoiados pelo serviço/sistema/recurso em questão. Devem ser elaborados PRDs para todos os processos classificados como críticos.
	RTO		
	Tempo para Recuperação do Ativo (TRA)?	IES.	Fazer com que a TI estime o tempo-limite para ativação do PRD, de forma que o RTO do processo suportado pelo serviço/sistema/recurso seja garantido.
	Tempo para ativação do PRD	IES.	
	Responsável pela execução - nome, cargo e telefone	AIG (2013); Lumiform (2020d); Nonprofit New York (2013)	Listar os recursos necessários para que a TI consiga restabelecer o serviço/sistema/recurso ao qual o PRD diz respeito.
	Informações e dados necessários		
	Instalações, equipamentos e		

Aba	Item	Origem	Justificativa da inserção
	recursos necessários		
	Tecnologias necessárias (*hardware*, *software*, telecomunicações)		
	Lista de contatos - Fornecedores e parceiros		
	Ações para a recuperação		Listar o procedimento a ser executado para recuperação do serviço/sistema/recurso.
	Data da aprovação	IES.	Garantir que o plano passe por uma aprovação.
	Data de realização do teste	AIG (2013).	Facilitar a identificação de se os planos estão sendo testados e, se sim, com que periodicidade.
	Método de teste	ISO 22313:2020 (ABNT, 2020b).	Estimular uma evolução gradativa na realização dos testes por meio da existência de uma "escala" no nível de complexidade destes.
	Oportunidades de melhoria identificadas	FEMA (2018).	Registrar as oportunidades de melhoria identificadas durante a realização dos treinamentos e testes dos planos desenvolvidos.
	Data de revisão	FEMA (2018).	Explicitar a última vez em que o plano foi atualizado, com o intuito de que não fique longos períodos sem ser revisitado.
	Revisado por		Explicitar o responsável pelas informações para esclarecimento de dúvidas, possibilitando, assim, a rastreabilidade das informações.
PCOM	Situação/ incidente	Deve ter origem nos cenários de crise previstos a partir da avaliação dos riscos críticos previamente realizada.	Vincular os Planos de Comunicação a serem desenvolvidos com os principais cenários de crises identificados anteriormente.
	Por que comunicar?	IES.	Detalhar o motivo pelo qual é importante que o público-alvo tenha ciência da informação.
	A quem comunicar?	IES; ISO 22301:2020 (ABNT, 2020a).	Fazer com que a organização determine as comunicações internas e externas pertinentes à continuidade de negócios.
	Quando comunicar?		
	Como comunicar?		
	Quem vai comunicar?		
	Tipo da comunicação	IES.	Prever cenários para comunicação ativa (quando a TI é quem comunica aos usuários) e reativa (o que a TI deve responder quando procurada pelos usuários) para estabelecer um discurso-padrão entre os colaboradores e reforçar os canais oficiais de comunicação.
	O que comunicar?	IES; ISO 22301:2020 (ABNT, 2020a).	Implementar e manter uma estrutura de resposta que permita aviso e comunicação oportuna às partes interessadas pertinentes.
Histórico	Situação/incidente	ISO 22313:2020 (ABNT, 2020b).	Garantir que a organização possua evidências históricas para monitorar, medir, analisar e avaliar a eficácia das suas estratégias de
	Em que data e horário o incidente		

Aba	Item	Origem	Justificativa da inserção
	foi constatado?		continuidade.
	Quem foi informado sobre o incidente?		
	Quais foram as consequências identificadas para o incidente?		
	Por quanto tempo o sistema/serviço/ recurso e/ou processo deixou(aram) de operar?		
	Itens destruídos ou danificados	CPA AUSTRALIA (2020).	Promover maior conhecimento dos impactos ocorridos a partir de cada tipo de incidente ou crise.
	Estimativa dos custos de recuperação (R$)	CPA AUSTRALIA (2020).	Embasar a alocação dos recursos de forma assertiva, a partir dos incidentes já ocorridos e do conhecimento de quanto já foi gasto para restabelecimento das atividades.
	Lições aprendidas	CPA AUSTRALIA (2020).	Fazer com que as lições aprendidas sejam incorporadas ao PCN após a recuperação do incidente. Também podem servir como argumento para que recursos sejam alocados em medidas preventivas.
	Que ação corretiva (imediata) foi ou está sendo realizada e quem é o responsável?	ISO 22313:2020 (ABNT, 2020b).	Identificar e atuar em aspectos das estratégias de continuidade de negócios que não estejam em conformidade e promover a melhoria contínua.
	Que ação preventiva foi ou será realizada e quem é o responsável?		
	Você agradeceu a todos os envolvidos que ajudaram?	CPA AUSTRALIA (2020).	Agradecer aos que se esforçaram para fazer com que os processos fossem recuperados e a organização voltasse a operar normalmente.
PCN	Política de continuidade de negócios	ISO 22301:2020 (ABNT, 2020a).	Refletir sobre e registrar o que se pretende alcançar com as estratégias de continuidade.
	Papéis e responsabilidades	FEMA (2018); LUMIFORM (2020a).	Facilitar a rastreabilidade dos responsáveis pelas frentes de continuidade de negócios.
	Objetivos de continuidade de negócios	LUMIFORM (2020).	Permitir que a organização acompanhe o progresso de suas estratégias por meio da comparação entre os resultados obtidos e seus objetivos.
	Datas de atualização do plano e responsáveis	FEMA (2018).	Explicitar a última vez em que o plano foi atualizado, com o intuito de que não fique longos períodos sem ser revisitado.

Fonte: Autores.

Assim sendo, tem-se como resultado desta pesquisa um artefato principal: o *framework* para elaboração de um PCN para uma área de TI, e o artefato Documento – PCN de TI, cujos *links* para acesso estão disponibilizados na Tabela 3.

Tabela 3

Principais artefatos desenvolvidos para elaboração do PCN de TI

Nº e nome do questionário	*Link* de acesso
Framework para PCN de TI	https://docs.google.com/spreadsheets/d/13Mz-yGEy7_wI63fE-X6CMB12aFuaVFDp72g842iLd-A/edit?usp=sharing
Documento – PCN de TI	https://docs.google.com/document/d/1PSPBlV4PwlHX_BdB52xk7X5JL4P9qCO2ypTYGZOohus/edit?usp=sharing

Fonte: Autores.

Na aba "Critérios" do *framework*, os pesos devem ser ajustados conforme a importância de cada um dos tipos de impacto, variando em um intervalo de 0 (mínimo) a 10 (máximo). Isso fará com que seja dada maior importância a um processo que possui determinado tipo de impacto (aqueles que foram definidos inicialmente pela organização como sendo impactos de maior peso para ela), ao efetuar os cálculos para determinação da criticidade dos processos e, consequentemente, a classificação destes na aba *Ranking* BIA. O procedimento para parametrização de um critério é demonstrado no seguinte vídeo: https://drive.google.com/file/d/1YLWo66kWgjP1S9wq8UUq-fCoqYxQdGTR/view.

O *framework* foi desenvolvido como uma Planilha Google® por esse recurso permitir que tantas pessoas quanto necessárias possam trabalhar colaborativamente e em paralelo no modelo. Isso também é válido para os Documentos Google®. O Documento – PCN de TI traz, além das tabelas do *framework*, itens para registro de: declaração da política de continuidade de negócios; papéis e responsabilidades quanto à estratégia de continuidade de negócios da organização; objetivos de continuidade de negócios; datas de atualização do plano e responsáveis pela atualização AIG (2013) recomenda que os planos sejam breves e diretos, uma vez que isso reduz o tempo necessário para ler e entender os procedimentos e, portanto, resulta em uma melhor chance de sucesso se o plano precisar ser aplicado.

A Figura 3 é uma representação visual de como o *framework* concebido deve ser aplicado, ilustrando todas as fases previstas até que se tenham todas as informações necessárias para a finalização do PCN de TI.

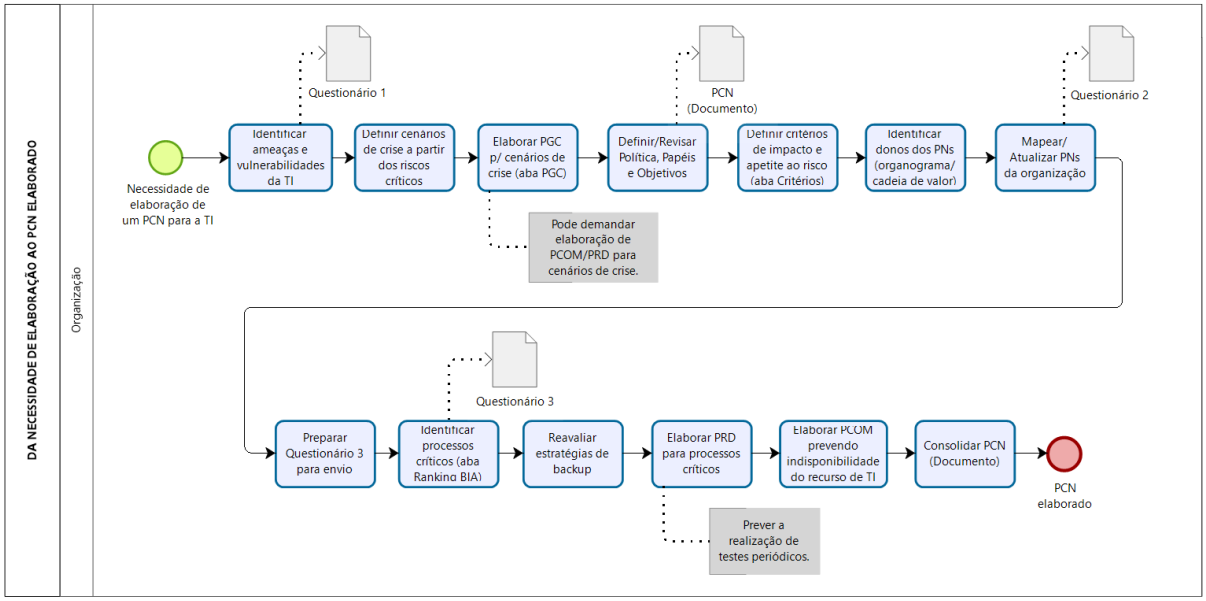

Figura 3 – Etapas para elaboração do PCN de TI aplicando o *framework* concebido
Fonte: Autores.

Uma vez que Formulários, Planilhas e Documentos Google® são preenchidos de forma *on-line*, é possível integrar as informações coletadas por meio dos questionários desenvolvidos ao *framework* e, ainda, o *framework* ao PCN (Documento Google® à parte), permitindo que o PCN possa ser atualizado com facilidade à medida que novas informações forem coletadas. A maneira como as informações estão integradas é demonstrada no seguinte vídeo: https://drive.google.com/file/d/1ofXSbk5zyb_Sx2X3NlMqQQJ71XOoW8Q2/view.

As principais vantagens, desvantagens e diferenciais do *framework* desenvolvido são compilados na Tabela 4.

Tabela 4
Análise do *framework* desenvolvido

Vantagens	Desvantagens	Diferenciais
- Permite que a organização defina os pesos para cada tipo de impacto avaliado conforme a realidade do negócio e o apetite ao risco; - baseado nos processos-chave do negócio; - vincula os processos de negócio aos	- Tem por objetivo tornar a TI resiliente, mas não abrange toda a organização por não contemplar Planos de Emergência (PEs) e Planos de Continuidade Operacional (PCOs) para as áreas de negócio; - ideal para organizações que já	- Integração entre os materiais que compõem o *framework*: questionários, *framework* e modelo de PCN, o que facilita tanto os ciclos de atualização periódica quanto a classificação e a análise dos

Vantagens	Desvantagens	Diferenciais
sistemas/serviços/recursos providos pela TI; - coleta informações por meio de questionários, o que agiliza a obtenção das informações necessárias para o PCN; - contempla cenários de interrupção de negócios/resposta a incidentes, conforme recomendação do DRI; - pode ser útil para aprimoramento da TI tanto de organizações do setor privado quanto organizações não governamentais; - os questionários desenvolvidos são responsivos, pois se adequam à tela de celulares ou *tablets*, permitindo que possam ser respondidos por meio desses dispositivos eletrônicos; - não necessita de aquisição de *software*.	utilizam os recursos da plataforma Google®, embora a não utilização não seja impeditiva. Os questionários precisariam ser refeitos com alguma ferramenta alternativa (preferencialmente *on-line*, para evitar a aplicação de questionários em meio físico), mas o *framework* (por ser uma Planilha Google®), e os Documentos Google® podem ser exportados e utilizados com o pacote Office. Entretanto, ao fazer isso perdem-se as integrações entre os questionários e as abas da planilha, bem como a automação desenvolvida para ordenar automaticamente os riscos (aba *Ranking* riscos) e a criticidade dos processos (aba *Ranking* BIA).	dados coletados por meio dos questionários; - histórico de incidentes como parte do *framework*, para retroalimentação durante a atualização do PCN; - utilização de recursos da plataforma Google®, o que confere ao *framework* uma série de recursos que promovem agilidade, colaboração e rastreabilidade entre os envolvidos na iniciativa de continuidade de negócios na organização e podem facilitar o desenvolvimento do PCN.

Fonte: Autores.

A aplicação desse *framework* para a área de TI pode resultar em um PCN com benefícios percebidos: pelos usuários dos serviços ofertados pela TI; por outras áreas e unidades de negócio da organização que utilizam os serviços, sistemas e recursos disponibilizados pela TI; e pela própria área de TI, em função de uma melhoria da governança obtida por meio do desenvolvimento de um PCN alinhado à estratégia da alta gerência.

5 CONSIDERAÇÕES FINAIS

A realização desta pesquisa resultou na proposição de um novo *framework* de PCN para auxiliar na Governança de TI em organizações, e teve como contribuição prática o desenvolvimento de um *framework* com alguns diferenciais em relação aos modelos já existentes: que possa ser trabalhado colaborativamente por várias pessoas ao mesmo tempo; que permita a coleta dos dados de forma prática, para desenvolvimento da 1ª versão e sempre que uma revisão for necessária; e com facilidade de atualização por meio da integração entre as informações do *framework* e o PCN em si. Como contribuição teórica, tem-se a publicação de um *framework* voltado para a TI no meio acadêmico e alinhado às diretrizes do *Disaster Recovery Institute International* (DRI) de contemplar definição das estratégias de

continuidade de negócios; plano de resposta a incidentes; avaliação de riscos e avaliação de impacto no negócio.

Por meio do *framework* desenvolvido, traçaram-se caminhos para: identificação dos principais riscos relacionados à TI em uma organização; identificação dos processos de negócio de uma organização e os recursos de TI que os apoiam e definição de critérios para avaliação e classificação da criticidade dos processos de negócio. O *framework* permite ainda que sejam conhecidos e ajustados, quando necessário, os tempos de recuperação de dados desejados pelas áreas de negócio e os *backups* realizados pela TI. Também foram definidos quais elementos devem ser considerados ao se elaborar PRDs e um PCOM para a TI e, por último, foi proposta uma forma de acompanhamento dos incidentes ocorridos em TI.

É importante ressaltar que todo PCN precisa estar atrelado aos processos organizacionais e que, por isso, não é possível o desenvolvimento de um PCN sem o envolvimento dos representantes das áreas de negócio da organização. Sem a consulta a aqueles que realmente utilizam os serviços/sistemas/recursos no dia a dia (áreas de negócio), a TI corre o risco de direcionar seus esforços erroneamente, por exemplo, investindo mais tempo e dinheiro protegendo recursos de TI que são menos críticos para a continuidade dos negócios. A única forma de a TI ter certeza sobre quais serviços/sistemas/recursos providos são realmente críticos é a partir do entendimento de quais são os processos críticos da organização. Senão, PRDs poderão ser elaborados, mas não haverá garantia de que os esforços estão sendo focados na direção certa.

Para que a iniciativa possa ser considerada uma estratégia de continuidade de negócios, é preciso realizar a BIA e desenvolver os PRDs em conformidade com a criticidade identificada por meio desta. A consulta às áreas de negócio é de extrema importância não apenas para promover esse entendimento, mas também para que sejam adotadas estratégias de *backup* eficazes. Caso contrário, a área de TI poderá estar prevendo seus *backups* com periodicidade de execução que não atende aos requisitos do negócio, seja para mais (neste caso, recursos estão sendo desperdiçados), seja para menos (neste, requisitos de negócio não estão sendo atendidos).

A aplicação deste *framework* é sugerida para organizações nas quais a área de TI percebe a importância da manutenção dos seus serviços, sistemas e recursos na manutenção dos processos organizacionais, principalmente nos casos em que não há ainda uma iniciativa

de elaboração de um Plano de Continuidade de Negócios para a organização como um todo (por isso, o título PCN "de TI").

Como oportunidade para pesquisas futuras, uma sugestão de aprimoramento seria o desenvolvimento de um aplicativo para uso do *framework*, como o modelo desenvolvido por Lumiform (2020). Isso poderia fazer com que novas funcionalidades fossem incorporadas ao *framework*, por exemplo, a automação de prazos para revisão de planos disparando notificações aos responsáveis por sua atualização.

Independentemente de em que direção este trabalho poderá evoluir, como última consideração, é importante ressaltar que o paralelo traçado por Haes e Gembergen (2008) sobre a aplicação de algum *framework* de Governança de TI em uma organização também é válido para a aplicação de um *framework* de continuidade de negócios: ter desenvolvido um *framework* não significa que a continuidade é realmente trabalhada na organização. Continuidade de negócios também é um processo de negócio, não um evento ou um simples plano de recuperação (Jackson, 2010). Uma vez desenvolvido, o PCN de TI deve, acima de tudo, permitir que a área de TI esteja alinhada às necessidades do negócio.

REFERÊNCIAS

ABNT. (2020a). *ABNT NBR ISO 22301:2020 Segurança e resiliência – Sistemas de gestão de continuidade de negócios – Requisitos.* Associação Brasileira de Normas Técnicas.

ABNT. (2020b). *ABNT ISO/TS 22317:2020 Segurança da sociedade – Sistemas de gestão de continuidade de negócios – Diretrizes para análise de impacto nos negócios (BIA).* Associação Brasileira de Normas Técnicas.

AIG. (2013). *A Guide to the preparation of a Business Continuity Plan*. Acesso em 22 de 6 de 2020, disponível em AIG UK: https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/property-insights/business-continuity-planning-guidelines-for-preparation-of-your-plan.pdf

Associação Brasileira das Entidades Fechadas de Previdência Complementar (ABRAPP). (2012). *Guia de Boas Práticas para Planos de Continuidade de Negócios.* Comissão Técnica Regional Sudeste de Governança da ABRAPP.

Bannerman, P. L. (4 de 2008). Risk and risk management in software projects: A reassessment. *The Journal of Systems and Software*, 2118–2133.

Bardin, L. (1977). *Análise de Conteúdo* (1 ed.). São Paulo: Edições 70.

Chagas, F. d. (2017). *Proposta de Plano de Continuidade de Negócios para uma Empresa Privada de Brasília.* Centro Universitário de Brasília, Brasília.

CPA Australia. (2020). *Disaster Recovery Toolkit*. Acesso em 21 de 6 de 2020, disponível em CPA Australia: https://www.cpaaustralia.com.au/-

/media/corporate/allfiles/document/professional-resources/business/disaster-recovery-toolkit.pdf?la=en&rev=a7ea31bb304641f7ac473914c6a6796a

Creswell, J. W. (2014). *Investigação Qualitativa e Projeto de Pesquisa: escolhendo entre cinco abordagens* (3 ed.). Porto Alegre: Penso.

Daryus Educação. (2020). *Gestão de Continuidade de Negócios - Conceitos e Gerenciamento.* Notas de aula, São Paulo.

Dresch, A., & Lacerda, D. P. (2016). *Design Science e Design Science Research: Método de Pesquisa para o avanço da Ciência e da Tecnologia.* Grupo de Pesquisa em Modelagem para Aprendizagem (GMAP) - Unisinos. Fonte: http://www.gmap.unisinos.br/recursos-didaticos/Design-Science-Research-Aline-Dresch.pdf

DRI. (2021). *Our Mission*. Acesso em 13 de 12 de 2020, disponível em Disaster Recovery Institute International (DRI): https://drii.org/aboutus

Fema. (2018). *Continuity Plan Template and Instructions for Non-Federal Entities and Community-Based Organizations.* Federal Emergency Management Agency, Washington.

Gil, A. C. (2010). *Como Elaborar Projetos de Pesquisa* (5 ed.). São Paulo: Atlas.

Haes, S. D., & Grembergen, W. V. (2008). Analysing the Relationship Between IT Governance and Business/IT Alignment Maturity., (pp. 1530-1605).

Hartson, R., & Pyla, P. (2019). *Background: Design. The UX Book.*

Hearnden, K. (1995). Business continuity planning: Part 4: Establishing business priorities. *Computer Audit Update*, pp. 3-13.

Hevner, A. R. (2004). Design Science in Information Systems Research. *Management Information Systems Quarterly*, pp. 75-105.

Interactive. (2019). *Business Continuity Plan Template*. Acesso em 21 de 6 de 2020, disponível em Interactive - Australia's Largest Privately Owned IT Company: https://www.interactive.com.au/business-continuity-template/

Isaca. (2011). *An Introduction to ICT Continuity Based on BS 25777*. Acesso em 15 de 12 de 2020, disponível em ISACA: https://www.isaca.org/resources/isaca-journal/past-issues/2011/an-introduction-to-ict-continuity-based-on-bs-25777

Jackson, C. B. (2010). Business Continuity Planning: Evolution in Response to Major News Events. *Encyclopedia of Information Assurance*, pp. 377–383.

Klumb, R., & Azevedo, B. M. (8 de 2014). A percepção dos gestores operacionais sobre os impactos gerados nos processos de trabalho após a implementação das melhores práticas de governança de TI no TRE/SC. *Revista de Administração Pública*, pp. 961-982.

Lento, L. O., & Luz, T. A. (2014). *Gestão de Continuidade do Negócio.* Unisul Virtual.

Lumiform. (2020). *Business Continuity Plan (BCP)*. Acesso em 29 de 8 de 2020, disponível em Lumiform Template Library: https://lumiformapp.com/templates/business-continuity-plan-bcp_33009

Lumiform. (2020b). *Business Impact Analysis Template*. Acesso em 29 de 8 de 2020, disponível em Lumiform Template Library: https://lumiformapp.com/templates/business-impact-analysis-template_15877

Lumiform. (2020c). *Business Impact Assessment Template Questionnaire*. Acesso em 29 de 8 de 2020, disponível em Lumiform Template Library: https://lumiformapp.com/templates/business-impact-assessment-template-questionnaire_15876

Lumiform. (2020d). *Business Continuity Plan Template for IT*. Acesso em 22 de 6 de 2020, disponível em Lumiform Template Library: https://lumiformapp.com/templates/business-continuity-plan-template-for-it_16825

Lumiform. (2020e). *Business Continuity Plan Audit*. Acesso em 29 de 8 de 2020, disponível em Lumiform Template Library: https://lumiformapp.com/templates/business-continuity-plan-audit_15861

Magalhães, C. d., Oliveira, L. R., & Oliveira, I. S. (2014). Estruturação do Plano de Continuidade de Negócio: um estudo de caso. *Anais do EATI - Encontro Anual de Tecnologia da Informação e Semana Acadêmica de Tecnologia da Informação*.

Martins, R. F., Wangham, M. S., & Favarim, F. (2009). Plano de Continuidade de Negócios para a TI do Aeroporto Internacional de Florianópolis. *Anais do IX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*.

Moraes, R. (1999). Análise de conteúdo. *Revista Educação, 22*, 7-32.

Muller, M. J., & Kuhn, S. (1993). Participatory design. *Communications of the AC*, 24-28.

My IT pros. (2020). *Business Resumption Plan Template*. Acesso em 21 de 6 de 2020, disponível em My IT pros: https://www.myitpros.com/resumption-plan-thank-you?submissionGuid=7f11b237-9f12-4e0d-ad02-776f88719123

Neto, J. S., & Neto, A. N. (12 de 2013). Metamodelo do Framework COBIT de Governança de TI. *Revista de Gestão da Tecnologia e Sistemas de Informação*, pp. 521-540.

Nonprofit New York. (2013). *Disaster Planning*. Acesso em 21 de 6 de 2020, disponível em Nonprofit New York: https://www.nonprofitnewyork.org/disaster-plan/

Paz, G. T. (2018). *Plano de Continuidade de Negócios de TI em uma empresa de transporte de cargas fracionadas.* Universidade do Sul de Santa Catarina, Farroupilha.

Research and Markets. (2020). *Disaster Recovery Business Continuity - 2020 Edition*. Acesso em 22 de 6 de 2020, disponível em Research and Markets: https://www.researchandmarkets.com/reports/5137121/disaster-recovery-business-continuity-2020#rela0-5137124

RiskSOURCE. (2020). *Business Continuity Planning*. Acesso em 21 de 6 de 2020, disponível em RiskSOURCE: https://risksource.com/wp-content/uploads/2018/06/Sample-Business-Continuity-Plan-Template.pdf

Svata, V. (2013). System View of Business Continuity Management. *Journal of Systems Integration, 4*(2), 19 – 35.

Swanson, M., Wohl, A., Pope, L., Grance, T., Hash, J., & Thomas, R. (2002). *Contingency Planning Guide for Information Technology Systems.* National Institute of Standards and Technology.

Tarouco, H. H., & Graeml, A. R. (3 de 2011). Governança de tecnologia da informação: um panorama da adoção de modelos de melhores práticas por empresas brasileiras usuárias. *Revista de Administração, 46*, 07-18.

Tigre, P. B., & Noronha, V. B. (3 de 2013). Do mainframe à nuvem: inovações, estrutura industrial e modelos de negócios nas tecnologias da informação e da comunicação. *Revista de Administração, 48*, 114-127.

UITS. (2012). *Information Technology Contingency Plan & Planning Guide.* University of Connecticut - University Information Technology Services, Storrs.

Wan, S. H., & Chan, Y. (2008). Improving service management in campus IT operations. *Campus-Wide Information Systems*, pp. 30–49.

Weill, P., & Ross, J. W. (2006). *Governança de TI: como as empresas com melhor desempenho administram os direitos decisórios de TI na busca por resultados superiores.* São Paulo: Makron Books.