FUNDAÇÃO INSTITUTO DE ADMINISTRAÇÃO
FACULDADE FIA DE ADMINISTRAÇÃO E NEGÓCIOS
PROGRAMA DE MESTRADO PROFISSIONAL EM GESTÃO DE NEGÓCIOS

WILSON DE GOES

GESTÃO DE CONTINUIDADE DE NEGÓCIOS – GCN
SUA ORGANIZAÇÃO "ACEITA" FALAR SOBRE ESTE ASSUNTO?
PROPOSTA PARA UMA FERRAMENTA PARA AUTODIAGNÓSTICO ORGANIZACIONAL

São Paulo
2021

WILSON DE GOES

GESTÃO DE CONTINUIDADE DE NEGÓCIOS – GCN
SUA ORGANIZAÇÃO "ACEITA" FALAR SOBRE ESTE ASSUNTO?
PROPOSTA PARA UMA FERRAMENTA PARA AUTODIAGNÓSTICO ORGANIZACIONAL

Dissertação apresentada à Banca Examinadora do Programa de Mestrado Profissional em Gestão de Negócios, mantida pela Fundação Instituto de Administração, como requisito para a obtenção do título de Mestre em Gestão de Negócios, sob a orientação do Prof. Dr. Charbel José Chiappetta Jabbour.

São Paulo
2021

Goes, Wilson de.
Gestão de continuidade de negócios - GCN: sua organização "aceita" falar sobre este assunto? proposta para uma ferramenta para autodiagnóstico organizacional. / Wilson de Goes. São Paulo, [s.n.]: 2022.
147 f.: il., tab.

Orientador: Prof. Dr. Charbel José Chiappetta Jabbour.
Área de concentração: Administração estratégica.
Dissertação (Mestrado Profissional em Gestão de Negócios) – Faculdade FIA de Administração e Negócios, Programa de Pós-Graduação em Stricto Sensu, 2022.

1. Gestão de Continuidade de Negócio. 2. Plano de Continuidade de Negócio. 3. Gestão de crise. 4. Gestão de Continuidade de Negócio - Indústria financeira - Brasil. 5. Estratégia corporativa. I. Jabbour, Charbel José Chiappetta. II. Mestrado Profissional. III. Faculdade FIA de Administração e Negócios. IV. Fundação Instituto de Administração.

DEDICATÓRIA

Segundo Mateus
(23.23 1:2:3:4.)

“Jesus falou então às multidões e aos seus discípulos, dizendo”:
“Os escribas e os fariseus sentaram-se no assento de Moisés. Portanto, todas as coisas que vos dizem, fazei e observai, mas não façais segundo as ações deles, pois dizem, mas não realizam. Amarram cargas pesadas e as põem nos ombros dos homens, mas eles mesmos não estão dispostos nem a movê-las com o dedo.”

AGRADECIMENTOS

Meus agradecimentos vão a todos aqueles que de alguma forma puderam contribuir para a elaboração deste trabalho. Com certeza, sem seus auxílios nos exatos momentos eu teria, de alguma forma, interrompido esta sequência.

Obviamente, não posso deixar de mencionar os nomes que mudaram minha vida: Sandra Eli, minha esposa, Vinícius (20) e Nícolas (19), meus dois filhos.

EPÍGRAFE

Ao braço de Menino Jesus

“O todo sem a parte não é todo,
A parte sem o todo não é parte,
Mas se a parte o faz todo, sendo parte,
Não se diga, que é parte, sendo todo.

Em todo o Sacramento está Deus todo,
E todo assiste inteiro em qualquer parte,
E feito em partes todo em toda a parte,
Em qualquer parte, sempre fica o todo.

O braço de Jesus não seja parte,
Pois que feito Jesus em partes todo,
Assiste cada parte em sua parte.

Não se sabendo parte deste todo,
Um braço, que lhe acharam, sendo parte,
Nos disse as partes todas deste todo.”

“Gregório de Matos
Poeta barroco brasileiro, nasceu em Salvador/BA, em 20/12/1623 e morreu em Recife/PE em 1696.”

RESUMO

As organizações da indústria financeira brasileira são, cada vez mais, pressionadas, por parte dos investidores e acionistas, a aumentarem a eficiência e a eficácia e, consequentemente, tornam-se mais dependentes de plataformas tecnológica. Estas plataformas precisam sempre estar disponíveis, sendo que indisponibilidades potencializa perdas financeiras significativas, promovem degradação da imagem e reputação organizacional no mercado, insatisfação do seu maior patrimônio, seus clientes. Como o objetivo principal da Gestão de Continuidade de Negócios (GCN) é entender como manter a organização ativa (operacional) mesmo em momentos de crise a GCN torna-se, assim, imprescindível. A metodologia adotada neste trabalho foi a pesquisa qualitativa, com entrevista semiestruturada, que permitiu que a entrevista fosse focada e trouxe bastante flexibilidade para aos respondentes. Esta dissertação evidencia que a Gestão de Continuidade de Negócios - GCN – pode ser ferramenta útil e deve prover a continuidade dos processos de negócios considerados críticos, enquanto a organização opera em regime de crise, no menor espaço de tempo possível, com o objetivo de minimizar o impacto de possíveis desastres. As entrevistas foram realizadas com executivos de bancos, com um roteiro inicial de perguntas atendo aos requisitos específicos da ABNT NBR ISO/IEC 22301:2013 e a aplicação de *framework* de boas práticas de gestão aplicados a diferentes cenários de crise. Estas entrevistas ocorreram de forma virtual entre outubro de 2021 a janeiro 2022 e seu resultado é parte constante deste material cujo tema central foi, “Gestão de Continuidade de Negócios – GCN – Sua organização “aceita” falar sobre este assunto? Proposta para uma ferramenta para autodiagnóstico organizacional”. A elaboração de métodos, metodologias, métricas, ferramentas de apoio, e *Know how* são elementos chaves na criação de uma GCN eficaz que permite aumento no nível de resiliência da organização para ações em momentos de crise. Por outro lado, é notório que a GCN não é um dispêndio associado a um evento improvável, mas, sim, um investimento prudente, que reduzirá um possível impacto, tornando-se um recurso corporativo fundamental em tempos de concorrência global. Finalizando esta pesquisa evidenciou que se a organização mantiver uma equipe de profissionais altamente qualificado as definições estratégicas oriundas da GCN poderão compor a estratégia corporativa.

Palavras-chave: Gestão de Continuidade de Negócio, Plano de Continuidade de Negócio, Gestão de crise.

ABSTRACT

Organizations in the Brazilian financial industry are increasingly under pressure from investors and shareholders to increase efficiency and effectiveness and consequently, become more dependent on technological platforms. These platforms always need to be available, and unavailability potentiates significant financial losses, promotes degradation of the organizational image and reputation in the market, dissatisfaction with its greatest asset, its customers. As the main objective of Business Continuity Management (BCM) is to understand how to keep the organization active (operational) even in times of crisis, BCM becomes, therefore, essential. The methodology adopted in this work was qualitative research, with semi-structured interviews, which allowed the interview to be focused and brought a lot of flexibility to the respondents. This dissertation shows that Business Continuity Management - GCN - can be a useful tool and should provide the continuity of business processes considered critical, while the organization operates in a crisis regime, in the shortest possible time, with the objective of minimizing the impact of potential disasters. The interviews were carried out with bank executives, with an initial script of questions meeting the specific requirements of ABNT NBR ISO/IEC 22301:2013 and the application of a framework of good management practices applied to different crisis scenarios. These interviews took place virtually between October 2021 and January 2022 and their result is a constant part of this material whose central theme was, “Business Continuity Management – GCN – Does your organization “accept” talking about this subject? Proposal for a tool for organizational self-diagnosis”. The development of methods, methodologies, metrics, support tools, and know-how are key elements in creating an effective GCN that allows an increase in the organization's level of resilience for actions in times of crisis. On the other hand, it is clear that GCN is not an outlay associated with an unlikely event, but rather a prudent investment that will reduce potential impact, making it a critical corporate resource in times of global competition. At the end of this research, it was shown that if the organization maintains a team of highly qualified professionals, the strategic definitions coming from the GCN will be able to compose the corporate strategy.

Keywords: Business Continuity Management, Business Continuity Plan, Crisis Management.

LISTA DE SIGLAS E ABREVIATURAS

SIGLA	SIGNIFICADO
6W3H	Técnica de Trabalho: **W** = Who; When; Why; Where; What and Which. **H** = How; How much; How many
ABNT	Associação Brasileira de Normas Técnicas
AIN	Análise de Impacto nos Negócios
API	Interfaces de Aplicação de Programas
App	Application
ATMs	Asynchronous Transfer Mode
BaaS	Banking as a Service
BACEN	Banco Central do Brasil
BIA	Business Impact Analysis
BSI	British Standards Institution
CMN	Conselho Monetário Nacional
COBIT	COBIT 5 - **C**ontrol **Ob**jectives for **I**nformation and Related **T**echnology
COVID-19	COVID-19 é a doença causada por um novo coronavírus denominado SARS-CoV-2. A OMS tomou conhecimento deste novo vírus em 31 de dezembro de 2019, após um relatório de um grupo de casos de “pneumonia viral” em Wuhan, na República Popular da China.
DevOps	Desenvolvimento e Operação
DevSecOps	Desenvolvimento, Segurança e Operação
DRII	Disaster Recovery Institute International
DRJ	Disaster Recovery Journal
FEBRABAN	Federação Brasileira de Bancos
GCN	Gestão de Continuidade de Negócios
GDPR	General Data Protection Regulation - Regulamento Geral de Proteção de Dados em tradução livre
GTAG	Global Technology Audit Guide
IA	Inteligência Artificial
IoB	*Internet of Behaviors*
IBGE	Instituto Brasileiro de Geografia e Estatística
IDC	idc.com
IEC	International Electrotechnical Commission

IPA	Automação de Processos Inteligente
ISO	International Organization for Standardization
IT	Information Tecnology
KYC	Know Your Customer
LGPD	Lei Geral de Proteção de Dados
NBR	Norma Brasileira - se destina a uma característica específica da produção acadêmica / científica
ONG	Organização Não Governamental
OSI	Organização Internacional para Padronização
PAC	Plano de Administração de Crises
PC	Plano de Crise
PE	Plano de Emergência
PCN	Plano de continuidade de Negócios
PCO	Plano de Continuidade Operacional
PDCA	**P**lan – **D**o – **C**heck – **A**ction. Metodologia (Planejar, Fazer, Checar, Agir)
PLD	Prevenção à Lavagem de Dinheiro
PPC	Plano Pré Crise
PR4	Metodologia: **P**revenção, **R**esposta, **R**ecuperação, **R**einício, **R**estauração
PRD	Plano de Recuperação de Desastres
PWC	PricewaterhouseCoopers Private
RIV	Relatório de Análise Visual
RPA	Robotic Process Automation
RPO	Ponto Objetivado de Recuperação
RTO	Tempo Objetivado de Recuperação
SaaS	Software as a Service
SARS	Síndrome respiratória aguda grave
SGCN	Sistema de Gestão de Continuidade de Negócio
SIPOC	Técnica de Trabalho: S = supplier (stackholder); I = input; P = Process; O = Output; C = Costumer.
TI ou IT	Tecnologia da Informação
TIC	Tecnologia da informação e telecomunicações
TVM	Títulos de Valores Monetários
WEB	**Web** é uma palavra inglesa que **significa** teia ou rede
UOL	Universo On line

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE TABELA

SUMÁRIO

1. INTRODUÇÃO

A preparação para emergências não é mais a única preocupação das organizações centradas em áreas do mundo mais propensas a terremotos ou tornados. A preparação deve, agora, levar em consideração desastres provocados pelo homem, como ataques terroristas, além de pandemias e desastres naturais.

Durante o primeiro ataque ao World Trade Center, em 1993, a empresa Morgan Stanley aprendeu uma lição importante. Nenhum dos funcionários da Morgan Stanley perdeu a vida, mas foram necessárias quatro horas para que todos os funcionários evacuassem o prédio. Como resultado, a gerência decidiu que o Gestão de Continuidade de Negócios - GCN precisava ser atualizado. A Morgan Stanley examinou atentamente as suas operações comerciais e o risco de possíveis desastres e desenvolveu um novo plano, pois eventos catastróficos afetam grandes e pequenas organizações.

Em 11 de setembro de 2001, o planejamento realizado pela *Morgan Stanley* compensou. Depois que o primeiro avião sequestrado colidiu com a primeira torre do *World Trade Center*, a segurança da *Morgan Stanley* evacuou todos os funcionários. A evacuação levou apenas 45 minutos, permitindo que a *Morgan Stanley* continuasse a recuperar as operações diárias. As melhorias nos recursos de Resposta à Emergência provavelmente salvaram inúmeras vidas e os recursos de GCN também foram aprimorados como parte da revisão. Os ataques terroristas de 11 de setembro de 2001 contra o Pentágono e o *World Trade Center* foram os mais devastadores contra os Estados Unidos desde o bombardeio de *Pearl Harbor*. Além de perturbar os processos militares, os ataques de 11 de setembro também tiveram como alvo os processos civis e as organizações dos Estados Unidos (GTAG, 2008). Aquele evento foi um divisor de águas, no qual se observou que não bastava apenas implementar estratégias de continuidade e planos desenvolvidos e testados, sendo necessário também gerenciar crises, quaisquer que sejam (GUINDANI, 2008).

O surto mundial de síndrome respiratória aguda grave, a SARS (novembro de 2002 a julho de 2003), consistiu em 8.096 casos infectados confirmados e 774 mortes. A quase pandemia causou um declínio significativo de clientes nos restaurantes de culinária chinesa na América do Norte, com uma queda de 90% em alguns casos. Na

época, a maioria das conferências e convenções agendadas nas principais cidades foi cancelada. Além disso, a intervenção do governo interrompeu as funções normais de negócios (por exemplo, viagens, cadeia de fornecimento etc.) para muitas organizações em países com infecções confirmadas (GTAG, 2008)1.

Os atentados de 7 de julho de 2005, em Londres, consistiram em uma série de explosões planejadas por terroristas no sistema de transporte público londrino. Os ataques, responsáveis por mais de 50 mortes e 700 feridos, afetaram seriamente o sistema de transporte público da cidade, bem como o sistema de telecomunicações móveis da Inglaterra (GTAG, 2008).

O furacão Katrina (formado em 23 de agosto de 2005) pode ter sido o desastre natural de maior custo da história dos Estados Unidos. Pelo menos 1.836 pessoas perderam a vida no furacão e nas inundações subsequentes. O Katrina causou danos estimados em US$ 81,2 bilhões, incluindo danos significativos a instalações industriais (principalmente petróleo, refinaria e produtos químicos), comerciais (principalmente de hospitalidade. e agrícolas (GTAG, 2008).

Em reportagem publicada pelo Jornal do Comércio do Ceará (29/09/2020), foi descrito que:

> “De acordo com o Instituto Brasileiro de Geografia e Estatística (IBGE), em torno de 700 mil Organizações fecharam as portas até o momento, e 50% delas devido à pandemia do Covid-19. Um dos principais motivos é a falta de um planejamento estratégico, mesmo que básico, **mas seguido de cuidados e responsabilidades, além de contar com Plano de Continuidade de Negócio (PCN) bem estruturado**, com diretrizes e ações para suportar possíveis impactos externos e até mesmo crises econômicas e políticas inesperadas. Sem estes dois planos, muitas Organizações, independente do segmento ou tamanho, acabam gastando além do necessário, desconhecem as próprias dificuldades e esquecem de criar fundos e ações para momentos mais sensíveis como as crises econômicas e políticas.”

Ainda na mesma reportagem temos:

> “...é relevante lembrar que no Brasil há também um outro tipo de “vírus” que vem importunando muito, são os ataques cibernéticos, que batem recordes todos os anos e cresceram mais de 80% em 2019. A segurança tecnológica no Brasil é muito vulnerável. Exatamente por não existir um ambiente virtual 100% seguro, as Organizações têm aumentado o foco em se preparar para eventos que causam impactos de alta criticidade2 e adotado Planos de Continuidade de Negócios cada vez mais conectado com a Política de

1 GTAG = *Global Technology Audit Guide.*

2 A palavra **“criticidade”** não existe em nosso dicionário, porém, neste trabalho, será utilizada para descrever algo de grande relevância, crítico.

> Segurança e Cibernética. Estes processos podem reduzir e muito os prejuízos da Organização em casos de invasão.”

Segundo o GTAG (2008), desde 1983, agências reguladoras, como a *American Bankers Association e o Banking Administration Institute,* exigiram que seus membros contribuintes executassem práticas de continuidade operacional (posteriormente apoiadas por manuais mais formais de GCN), que protegem o interesse público. As normas mais recentes foram frequentemente baseadas em normas formalizadas, definidas sob o ABNT NBR ISO/IEC 25002.

Muitas vezes, o valor de um programa de GCN não é apreciado até que seja necessário. Talvez isso ocorra porque é difícil calcular o retorno sobre o investimento de um programa de GCN até que um desastre ocorra. A gerência precisa entender que, se tal situação ocorrer, os negócios devem continuar, mas sob circunstâncias muito diferentes. O custo de um desastre pode ser o fim do negócio. Os líderes organizacionais precisam ponderar o custo de se preparar contra o custo de fechar as portas do negócio por uma semana, um mês ou para sempre, dependendo da catástrofe. Muitos governos ao redor do mundo exigem que certas indústrias tenham uma GCN testado em vigor. Nos Estados Unidos, todas as organizações dos setores financeiro, de serviços públicos e de saúde são obrigadas a manter uma GCN atualizado. Existem normas e diretrizes gerais e específicas do setor para uma GCN eficaz.

De acordo com Wheatman (2001), muitas organizações que sofreram uma interrupção de suas atividades devido a um desastre nunca se recuperam. Em percentuais, 40% das organizações que passaram por essa situação encerraram as atividades num prazo de até cinco anos após o evento.

O *Disaster Recovery Institute International (DRII – fundado em 1988)* é a maior e mais antiga organização sem fins lucrativos que ajuda outras organizações em todo o mundo a se prepararem e se recuperarem de desastres. A instituição oferece educação, credenciamento e liderança inovadora em continuidade de negócios, recuperação de desastres, resiliência cibernética e áreas relacionadas. Também, coletou, ao longo de décadas de atividade, estatísticas que afirmam que “de cada cinco companhias que sofrem interrupção nas suas operações por uma semana, duas fecham as portas em menos de três anos” (ALEVATE, 2014, p. 64).

Uma GCN apoia a estruturação da execução de um plano de resposta a eventos de alto impacto, incluindo pontos específicos e documentados acerca da comunicação com o mercado, para *stakeholders* e reguladores, de forma organizada e provendo ferramentas para ações em momentos de crise. Essas ações tornam a reação aos eventos mais estruturada e organizada (GUINDANI, 2011; ALEVATE, 2014).

De acordo com o Instituto Brasileiro de Geografia e Estatística (IBGE), nos últimos tempos, em torno de 700 mil organizações fecharam as portas no Brasil, sendo que 50% dessas ocorrências foram devidas à pandemia da COVID-19. Um dos principais motivos foi a falta de um planejamento estratégico, mesmo que básico, mas seguido de cuidados e responsabilidades, além da ausência de um Plano de Continuidade de Negócio – PCN - bem estruturado, com diretrizes e ações para suportar possíveis impactos externos e até mesmo crises econômicas e políticas inesperadas.

A COVID-19, provavelmente, não afeta a infraestrutura física de uma organização, pois pode ameaçar todas as operações por seu impacto nos indivíduos. Como a área de RH se esforça para garantir a saúde, a segurança e o bem-estar dos colaboradores, em uma crise, essa equipe precisará manter pessoal adequado e monitorar a saúde dos profissionais.

1.1. Contextualização

Em artigo publicado pela revista Exame (13/01/2004), por Michael Porter, encontra-se o seguinte:

> “Sempre me impressionou muito o espírito empreendedor dos administradores brasileiros. O Brasil é um país onde há muitos talentos incríveis atropelados pelo sistema, talentos que têm de lidar com um monte de desvantagens e impossibilidades por causa do ambiente. Mas sempre há essa energia, o espírito empreendedor, criativo. Quando eu vinha ao Brasil, há 20 anos, para falar sobre estratégia, o típico administrador brasileiro me dizia: ‘Ora, eu não posso ter uma estratégia -- tudo é instável demais. Eu nunca sei o que vai acontecer amanhã’.
>
> Mas o Brasil chegou a um estágio no qual todos precisam ter uma estratégia. A estabilidade está chegando, e este é o momento de pensar no longo prazo e em estratégia para os negócios. Muito do sucesso deste país depende de melhorar seu ambiente competitivo.

> Para isso, a comunidade administrativa precisa assumir mais responsabilidade pelas políticas econômicas. Os líderes administrativos têm de desempenhar papel maior, não apenas aconselhando o governo, mas também fazendo coisas por si mesmas."

O sistema bancário brasileiro é altamente regulamentado pelo BACEN, atendendo aos regulatórios nacionais e internacionais. Em junho de 2006, por meio do Conselho Monetário Nacional – CMN, o órgão publicou a resolução 3380:2006, que reflete especificações apresentadas na Basileia II, tratando do risco operacional e substituída pela resolução nº 4557 de 23 de fevereiro de 2017.

A globalização dos serviços financeiros e a sofisticação da tecnologia bancária no mercado brasileiro contribuíram para o aumento da complexidade dos riscos3 envolvendo a Tecnologia da Informação. Por ser fortemente dependente da automação e dos elementos de que lhe dão suporte, a TI está muito vulnerável a falhas operacionais e às consequências que estas podem trazer.

O setor bancário aparece como um dos setores que mais têm investido em TI, tendo grande parte de seus produtos e serviços4 com dependência dessas tecnologias. Com relação ao comportamento global de gastos em TI na América Latina em todos os setores, valores de 1998 apontam a indústria financeira com percentuais entre 20% e 30% do total de investimentos (LARA; PERDÓMO; JIMÉNEZ, 1999).

---

3 **Risco**: efeito da incerteza nos objetivos.
Nota 1: Um efeito é um desvio do que é esperado – positivo ou negativo
Nota 2: Os objetivos podem ter diferentes aspectos (como metas financeiras, saúde e segurança e ambientais) e podem ser aplicados em diferentes níveis (como estratégico, em toda a organização, projeto, produto e processo). Um objetivo pode ser expresso por outros meios, por exemplo, como um resultado esperado, um propósito, um critério operacional, como objetivo da continuidade do negócio, ou pelo uso de outras palavras com significado similar (por exemplo, objetivo, meta ou alvo).
Nota 3: Risco é, muitas vezes, caracterizado pela referência aos eventos potenciais (ABNT ISO Guia 73, 3.5.1.3) e consequências (ABNT ISO Guia 73, 3.6.1.3) ou uma combinação destes.
Nota 4: Risco é frequentemente expressado em termos de uma combinação das consequências de um evento (incluindo mudanças nas circunstâncias) e a probabilidade (Guia 73, 3.6.1.1) de ocorrência associada.
Nota 5: Incerteza é o estado, ainda que parcial, da deficiência de informação relacionada ao entendimento ou conhecimento de um evento, sua consequência ou probabilidade.
Nota 6: No contexto de padrões de gestão de continuidade de negócios, os objetivos de continuidade de negócios são definidos pela organização, de acordo com a política de continuidade de negócios, para alcançar resultados específicos. Ao aplicar o termo "risco" e componentes de gerenciamento de risco, este deve ser relacionado com os objetivos da organização, que incluem, mas não estão limitados aos objetivos de continuidade de negócios, conforme especificado em 6.2.

FONTE: ABNT ISO/IEC Guia 73

4 **Produtos e serviços**: resultados benéficos que uma organização fornece a seus clientes e partes interessadas, como bens manufaturados, seguros automobilísticos, conformidade em regulamentações e benefícios comunitários.

Os bancos investiram R$ 25,7 bilhões em tecnologia no ano passado — alta de 8% em comparação com os aportes feitos no ano anterior (R$ 23,9 bilhões). A informação foi divulgada com base no levantamento de tecnologia bancária 2021 (ano-base 2020) da FEBRABAM (Federação Brasileira de Bancos), durante o evento CIAB FEBRABAN. Com esse aumento, o setor bancário tornou-se o segundo maior investidor em tecnologia no Brasil (14%), atrás apenas dos governos (15%). A mesma situação é vista em âmbito global, o que indica que as instituições financeiras brasileiras têm acompanhado os aportes realizados no mundo todo.

Os bancos brasileiros, por exemplo, investiram, nos últimos três anos, mais de R$ 8,5 bilhões em equipamentos de informática e comunicação e em programas de computador (FEBRABAN, 2002). Já com relação ao número de ATMs, o Brasil aumentou sua rede de caixas automáticas em 32,6%, no período de 1998 a 1999, dispondo de mais de 18.000 salas de autoatendimento (entre postos eletrônicos e tradicionais) (FEBRABAN, 2000).

O computador tem exercido um forte impacto sobre as operações bancárias, sendo que hoje, provavelmente, a indústria bancária é a mais informatizada de todas (DRUCKER, 1999). As transações automatizadas, realizadas sem a intervenção de funcionários, representam uma parcela cada vez maior do total de operações, especialmente porque podem ser realizadas em período muito mais amplo do que o do expediente das agências e em locais mais próximos e cômodos aos clientes. Cada vez menos, os clientes precisam se deslocar às agências bancárias para realizarem seus serviços financeiros, tudo isso graças à tecnologia.

O ano de 2019 terminou com o sistema bancário nacional apostando, ainda mais, na consolidação dos canais *online* e tecnologias móveis como principais meios de interação com seus clientes. A disponibilidade dos serviços digitais passou a ser uma exigência crescente e, nesse aspecto, as organizações do setor bancário competem não apenas entre si, mas com a economia digital como um todo.

Embora a maior parte do sistema bancário invista significativamente em tecnologia, mesmo sendo a indústria mais regulamentada do país, nota-se que muito desse investimento ainda é feito com uma visão de curto prazo, para “apagar incêndios”. A

necessidade de aderir às novas tecnologias é uma constante, mas ela se torna mais efetiva quando há um horizonte estrategicamente definido a ser alcançado.

Os vultosos custos econômicos e sociais resultantes de crises financeiras têm conduzido os esforços de organismos internacionais e autoridades de supervisão para pesquisas sobre o risco sistêmico. O objetivo tem sido buscar características comuns que possam prever a proximidade das crises.

O gerenciamento de crises é um processo em que as organizações buscam gerenciar crises ou eventos de impacto significativo. Esse processo envolve a identificação da crise, as ações de resposta, a resolução e, ao final, a observação das lições aprendidas, o que chamamos de pós-crise. A literatura considera que os estudos e a metodologia adotada atualmente para a gestão de crises iniciaram-se em 1982, com o caso Tylenol ®. Hoje não existem dúvidas de que as crises fazem parte do nosso dia a dia, não podendo mais serem consideradas eventos raros ou imprevisíveis. O gerenciamento de crises eficaz ocorre quando estas são detectadas e tratadas com rapidez, antes que os impactos na organização atinjam níveis inaceitáveis. Existem inúmeros motivos que levam as organizações a investirem tempo e dinheiro no gerenciamento de crises (GUINDANI, 2011).

Nesta linha de pensamento, para as instituições financeiras que pretendem permanecer competitivas no mercado, a GCN passa a ter um peso ímpar. Ela terá que incorporar e combinar seus piores cenários e suas estratégias de recuperação antes, durante e depois dos mais variados tipos de eventos, quer seja em uma crise, paralização do negócio, um desastre ou uma pandemia, como a que se viveu em 2020/2021.

Por outro lado, a GCN está alicerçada em três grandes pilares: negócios, pessoas e tecnologia da informação (TI). O plano de ação de resposta a incidentes visa atender à resolução nº 85 do BACEN5, de 08/04/2021, bem como definir as rotinas, os

---

5 **Alta Direção:** pessoa ou grupo de pessoas que dirige e controla uma organização em nível mail alto.
Nota 1: A Alta Direção tem o poder de delegar autoridade e fornecer recursos dentro da organização;
Nota 2: Se o escopo do sistema de gestão abrange apenas parte de uma organização, então Alta Direção refere-se àqueles que dirigem e controlam parte da organização.

Fonte: ABNT NBR ISO/IEC 22301:2013

procedimentos, os controles e as tecnologias utilizadas na prevenção e na resposta a incidentes. Diante do grande avanço tecnológico observado atualmente, faz-se necessário manter a segurança, a integridade, confidencialidade, disponibilidade, legalidade e autenticidade dos dados e informações, armazenadas pela organização e seus fornecedores.

1.2. Problema de investigação

Diante de tantas alternativas e inovações, as organizações, muitas vezes, focam apenas no *core* de suas atividades, deixando a área de GCN para segundo plano e com orçamento bastante limitado. Diante disso, a questão de pesquisa é investigar, em relação à GCN: “Sua organização ‘aceita’ falar sobre este assunto – Proposta para uma ferramenta para autodiagnóstico organizacional”. Para isso, utilizou-se uma pesquisa semiestruturada, abrangendo 5 perguntas direcionada a 5 executivos de bancos.

Profissionais especialistas precisam estar altamente treinados para que possam desenvolver suas atividades e criar estratégias diante de cenários tão inovadores que, muitas vezes, poderão se deparar com as novas modalidades de negócio e tecnologia. Os processos de negócios considerados críticos, tão vitais para manter o “negócio” da organização em plena atividade, são, muitas vezes, significativamente afetados, requerendo novos e repetidos testes6 em seus *sites* alternativos, nos quais serão ativadas equipes técnicas e de negócios para verificarem e validarem os piores cenários.

1.3. Objetivos

O principal objetivo deste projeto é entender como manter a organização ativa (operacional) mesmo que em momentos de crise. Outros objetivos secundários se destacam: i) compreender se quanto a alta administração7 estiver engajada melhor

---

6 **Teste**: procedimento para avaliação; maneira de determinar a presença, qualidade, ou veracidade de algo.
Nota 1: Teste pode se referir a um “experimento”;
Nota 2: Teste é frequentemente aplicado para suportar planos.

Fonte: ISO 22300

7 **Alta Direção:** pessoa ou grupo de pessoas que dirige e controla uma organização em nível mail alto.
Nota 1: A Alta Direção tem o poder de delegar autoridade e fornecer recursos dentro da organização;

será a qualidade dos resultados / planejamento da crise; ii) verificar se o Planejamento de Crise pode ser executado por meio de: coordenação de parcerias, longevidade e compreensão; iii) identificar se Planejamento da Crise depende da qualidade de recurso: pessoas, TI, negócio;

Além disto é possível dizer que o objetivo final desta pesquisa é responder as proposições, assim como o objetivo geral é manter a organização operacional mesmo em momentos de crise.

1.4. Delimitação do escopo

Este trabalho se propõe a demonstrar a necessidade de desenvolvimento dos planos de continuidade de negócios: Plano de Administração de Crises - PAC, Plano de Continuidade Operacional - PCO e Plano de Recuperação de Desastres – PRD, – Plano Pré Crise - PPC, Plano de Emergência – PE e Plano de Crise – PC, como sendo garantias de sobrevivência para os bancos, independentemente de seus tamanhos. Neste contexto, foca-se no Plano de Crise - PC. Para desenvolvimento dos planos supracitados, pode-se utilizar as melhores práticas e técnicas, tais como: 6W3H, SIPOC, BIA, RIV, PDCA e PR4.

Para efeito desta pesquisa, considerou-se a indústria financeira – bancos - com aplicação de ISO's com todos os regulatórios, circulares expedidas pelo Banco Central do Brasil – BACEN – aplicados apenas aos bancos e outras instituições financeiras.

1.5. Justificativa

Segundo Siqueira (2005, p. 103), a implantação da GCN significa "não permitir a interrupção das atividades do negócio e proteger os processos considerados críticos contra os efeitos de falhas ou desastres significativos". Trata-se de uma das formas de sobrevivência da organização e, por isso, é necessário falar sobre GCN. Mas será que a "alta" administração realmente aceita o que os especialistas da área dizem? Ou o que ocorre é que este assunto ainda é tabu para a grande maioria? Aliás, é possível

---

Nota 2: Se o escopo do sistema de gestão abrange apenas parte de uma organização, então Alta Direção refere-se àqueles que dirigem e controlam parte da organização.

Fonte: ABNT NBR ISO/IEC 22301:2013

afirmar que este tema é tratado com uma conotação negativa, em que a alta administração acredita que os profissionais do ramo somente pensam em problemas, desastres, sinistros, quando a organização teria que pensar em “produtividade”.

No entanto, sabe-se que uma GCN deve prover a continuidade dos processos de negócios considerados críticos ou de informações vitais à sobrevivência, promovendo a longevidade da organização, no menor espaço de tempo possível, com o objetivo de minimizar o impacto de possíveis desastres. Goedert (2004) cita a necessidade de um plano que garanta a continuidade destes processos, enquanto a organização opera em regime emergencial, ou seja, garantir o negócio e as atividades-fim da organização.

Em um mundo dinâmico, em que se desfruta a globalização, é possível comentar poeticamente a indistinção entre parte (Planos) e todo (GCN), resolvendo, ao que tudo indica, essa questão do (des)centramento:

> O todo sem a parte não é todo,
> A parte sem o todo não é parte,
> Mas se a parte o faz todo, sendo parte,
> Não se diga, que é parte sendo todo.
> (Gregório de Matos8).

Em outras palavras, situações adversas acontecem, devem e merecem ser analisadas como um todo e não como uma parte do todo. Ainda existem organizações que encontram dificuldades em manter operacionais processos que envolvem uma parada prolongada e não programada de um aplicativo ou um processo produtivo; perda de um *hardware*; perda de um *software*; “*peopleware”*.

Ainda nesta linha, profissionais da área estão sendo comparados a “bombeiros”, “apagadores de incêndios”, termos comuns na área de Tecnologia da Informação. Estes “bombeiros” são constantemente chamados para apagar tais incêndios que estão consumindo e pondo em perigo a continuidade dos negócios da organização. Nos dias de hoje, isto não deveria mais acontecer.

8 Gregório de Matos – (23/12/1636 – 26/11/1696) – Foi um dos mais expressivos poetas brasileiro do período Barroco.

Felizmente, profissionais da área ou organizações de serviços voltados para este nicho de mercado estão disponibilizando requisições e mudando o cenário, falando de padrões de segurança, conforme ABNT NBR ISO/IEC 22301, que substituiu a ABNT NBR ISO/IEC 25999-2. Estes dois padrões são muito similares, mas a ABNT NBR ISO/IEC 22301 pode ser considerada como uma atualização da BS 25999-2.

A velocidade de processamento, de decisões, e a demanda por disponibilidade de recursos são altíssimas, sendo que a disponibilidade, integridade e confiabilidade das informações são cada vez mais exigida. Grau de Risco, continuidade, normalidade, usabilidade, legalidade, interoperabilidade, entre outros termos que poderiam ser mencionados, passam a ter uma relevância ampliada no mundo corporativo dos negócios, culminando na flexibilidade.

Em pesquisa na internet9, identificou-se que os ataques de 11 de setembro provocaram um baque econômico gigantesco. A Bolsa de Nova Iorque fechou, o que não acontecia desde a Segunda Guerra Mundial. Além disso, nos três dias seguintes aos atentados, o governo dos Estados Unidos injetou US$ 300 bilhões no mercado financeiro para tentar evitar uma crise. Nos meses seguintes, Nova Iorque recebeu US$ 20 bilhões para obras de reconstrução, e os militares viram seu orçamento anual crescer 25% e chegar a avassaladores US$ 500 bilhões (cinco vezes o que o governo federal brasileiro gasta com saúde e educação). Entretanto, a economia continuava paralisada, pois, com medo de novos ataques, ninguém queria investir em nada.

Para o mundo da Continuidade de Negócios, em 2020, novamente tudo mudará. Eventos como do *DRJ – Disaster Recovery Journal* (um dos maiores do mundo sobre o assunto), são realizados duas vezes por ano nos Estados Unidos da América, trazendo muitas novidades quanto à consciência de todos e quanto à maneira de se realizar e rever o planejamento que procura garantir a permanência de uma organização depois do evento incerto.

Um conjunto de ações preventivas torna possível a continuidade das operações das áreas de negócio de uma organização, após a ocorrência de um evento que impossibilite a utilização parcial ou total do ambiente corporativo.

9 https://super.abril.com.br/historia/11-de-setembro-o-que-veio-depois/ - realizada em 21/04/2021

A área de TI passou a ser a mola propulsora para realização por ter, indireta ou diretamente, a centralização das informações, ou seja, um dos bens mais preciosos de uma organização.

A preocupação com a recuperação do Centro de Tecnologia da Informação deve considerar outras áreas vitais para uma organização, tais como logística, *call center*, mesa de operação, linha de produção, centro de engenharia e tantas outras mais.

As organizações ainda mantêm, por questões de segurança, praticidade, instalação e manutenção em um único ambiente para armazenar todos os seus equipamentos de processamento de dados.

Dessa maneira, cabe considerar quais impactos existem para qualquer negócio a parada total ou parcial deste Centro de Tecnologia da Informação. Será que a organização deve prevenir a ocorrência de um evento, identificando riscos e minimizando impactos de eventuais momentos que acarretam perdas ao negócio, com a elaboração de um Plano de Continuidade de Negócio? Ainda, como é possível proteger um Centro de Tecnologia da Informação de um eventual desastre?

Garantir a continuidade dos negócios envolve sempre investimentos ou custos, ação que depende do ponto de vista do gestor em qualquer organização. Com a digitalização de todas as informações relevantes para uma organização e de seus processos, aumenta também a necessidade de melhorar o seu **armazenamento de dados**. Não por acaso, o mercado global de soluções de *enterprise storage* cresceu 13,7% no último trimestre de 2017, segundo o relatório da IDC divulgado em **uma matéria** do *site* da *Computer World*.[10]

Segundo os dados da consultoria IDC, considerando apenas o quarto trimestre de 2017, as vendas do mercado de *enterprise storage* no mundo somaram US$ 13,6 bilhões (cerca de R$ 45 bilhões). Na comparação anual, “os embarques de capacidade total aumentaram 39,3%”, somando 89,2 *exabytes* durante o último

[10] https://www.2cloud.com.br/quanto-custa-investir-em-uma-estrutura-de-ponta-para-o-armazenamento-de-dados/ Artigo: Quanto custa investir em uma estrutura de ponta para armazenamento de dados – postado em 29/05/2018 – TAGS: 2Cloud, Armazenamento de dados, backup

trimestre do ano. Esses dados mostram como as Organizações estão aumentando, cada vez mais, as suas demandas por armazenamento de dados**.**

Empresas investirão mais dinheiro em estratégias de continuidade dos negócios e gestão de risco investigando melhor os terceiros que contratam para reduzir sua exposição[11]

Um elemento da gestão de risco que costuma ser negligenciado e subestimado é a continuidade dos negócios. A pandemia mostrou que as organizações precisam estar preparadas para evitar que clientes e funcionários enfrentem interrupções de serviço. Aliás, isso é ainda mais válido se elas forem uma empresa global exposta a riscos regionais específicos. Esses riscos podem ser cibernéticos ou relacionados à saúde pública, mudanças climáticas, desastres naturais e vários outros.

Além disso, a exposição ao risco vai além das quatro paredes da empresa e inclui os parceiros do ecossistema e os prestadores de serviços. Fica claro que a pandemia foi um teste de fogo para muitos planos de continuidade dos negócios. Portanto, as empresas precisarão rever e auditar regularmente seus planos para terem certeza de que eles cumprem todas as normas aplicáveis e são relevantes.

Um Plano de Continuidade de Negócios deve conter um conjunto de atividades para prevenção de eventos, ações a serem tomadas antes, durante e depois de um evento e processos de retorno a situação anterior ao evento, levando-se em conta a velha fórmula custo *versus* benefício.

Dadas estas considerações, o próximo capítulo traz o referencial teórico que embasou este projeto.

[11] https://www.ecommercebrasil.com.br/noticias/tendencias-de-seguranca-meios-de-pagamentos-digitais-visa/ Artigo: Tendências de segurança para os meios de pagamentos digitais sob olhar da VISA – postado em 16/02/2022

2. REFERENCIAL TEÓRICO

A alta administração, de acordo com a ABNT NBR ISO/IEC 22301:2013, deve demonstrar liderança em GCN. Esta liderança e o comprometimento podem ser demonstrados pela motivação e capacitação de pessoas em contribuir com a eficácia, além de prover evidências de seu comprometimento com o estabelecimento, implementação, operação, monitoramento, análise crítica, manutenção e melhoria do GCN. Por outro lado, Guindani (2008) comenta que a continuidade de negócios é um projeto difícil de ser vendido ou aceito. A grande maioria dos gestores não acredita que algo negativo possa acontecer, então, sob esta ótica, o GCN parece desperdício de tempo e dinheiro.

Já para o GTAG (2008), o apoio da alta administração (Quadro 1) é fundamental para o sucesso da GCN em todas as organizações. A alta administração deve garantir que existam políticas em vigor que exijam que as equipes de gestão implementem um programa de GCN para suas unidades de negócios. Todas as políticas de gestão de emergência devem estar alinhadas, para garantir que a continuidade de negócios, em resposta à emergência, e a GCN trabalhem juntas durante um desastre real. É bom lembrar que GCN não é mera burocracia para atender aos órgãos reguladores e principalmente, que GCN não é despesa, é investimento (GUINDANI, 2008).

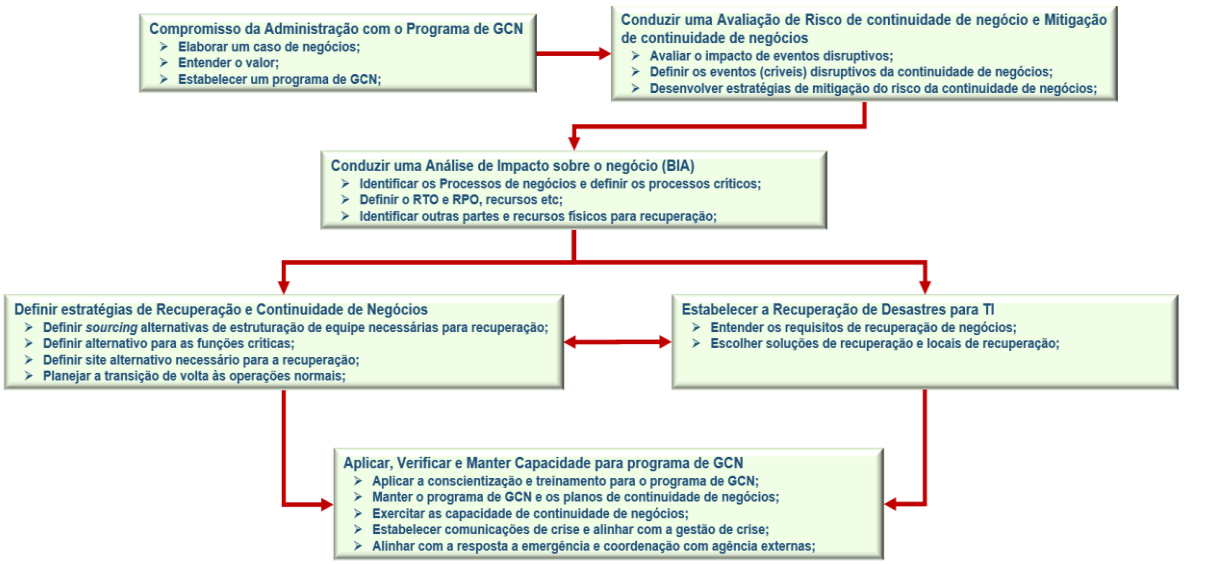
A GCN é o processo pelo qual uma organização se prepara para futuros incidentes, que poderiam comprometer a sua missão central e sua viabilidade em longo prazo. Tais incidentes incluem eventos locais, como incêndios em edifícios, eventos regionais como terremotos, ou eventos nacionais, como doenças pandêmicas. Sendo assim, é possível estabelecer que uma organização possa se preparar para as piores etapas e melhorar suas resistências às ameaças (SILVA, 2010).

Para Guindani (2011), não se pode escolher que tipos de problemas serão enfrentados, mas pode-se escolher a melhor forma de os enfrentar. De acordo com o *Business Continuity Institute - BCI*[12], uma gestão de continuidade de negócio requer que várias disciplinas sejam gerenciadas e administradas, para que um plano seja

12 ***BCI – Thebci.org*** – Sediado na Europa em 2019 marcou 25 anos do BCI, ajudando indivíduos e organizações a se tornarem mais resilientes, por meio das melhores práticas de Continuidade de Negócio.

considerado efetivo dentro dos objetivos de tempo de recuperação esperados pelo negócio.

Quadro 1: Fluxograma de Requisitos de GCN.



Fonte: GTAG
David Everest, key Bank; Roy E. Gerber, Safe Auto Insurance Co., Michael Keating, Navigant Consulting Brian Peterson, Chevron Corp.

Adaptado pelo Autor

A criação de um plano de continuidade é uma das tarefas mais importantes dentro da GCN, sendo que, com esse plano, é possível obter preparo para a tomada de decisão e de ações, tanto para ocorrências boas como para ocorrências ruins. Os planos de continuidade são utilizados, na maioria das vezes, para minimizar os efeitos dos problemas.

A continuidade dos negócios, para ser realmente efetiva, exige mudança cultural (GUINDANI, 2011).

Silva (2011) descreve cinco fases da elaboração de um plano de continuidade: i) identificação ou avaliação do risco; ii) análise de impacto no negócio; iii) desenho, ou seja, definição da estratégia; iv) execução quanto ao desenvolvimento do plano e sua execução; e v) medição de testes[13] e manutenção do plano.

Pode-se ressaltar que os objetivos da GCN transitam entre as áreas: a. jurídica, para proteger a organização e os administradores; b. legal, para atender as legislações e

[13] Medição de testes – método utilizado para medição do teste após seu término.

regulamentações; c. mercado, visando conquistar diferencial competitivo e confiança; e d. sustentabilidade, a qual mantém a disponibilidade do ambiente e garante a continuidade do negócio.

Guindani (2011) cita as etapas para planejamento, implementação e desenvolvimento da gestão de continuidade de negócio, contidas nos guias profissionais *(DRII e BCI)* e normas (BS 25999 e NBR 15999), como referências de modelo que devem ser adaptadas às necessidades e cultura das organizações. São elas: conhecer a organização, definir estratégias, desenvolver uma resposta, manter e testar e gerir o programa de gestão de continuidade de negócios.

Como pode ser visualizado na Figura 1, pode-se dividir o PCN em vários planos: plano de pré-crise, plano de emergência, plano de administração de crise, plano de continuidade operacional, plano de recuperação de dados e plano de crise. Para efeito desta pesquisa, focar-se-á ao plano de crise.

2.1. Gestão de Continuidade de Negócios

Segundo a ABNT NBR ISO/IEC 22301:2013, plano de continuidade de negócios são procedimentos documentados que orientam as organizações a responderem, recuperarem, retomarem e restaurarem, após a interrupção, para um nível predefinido de operação.

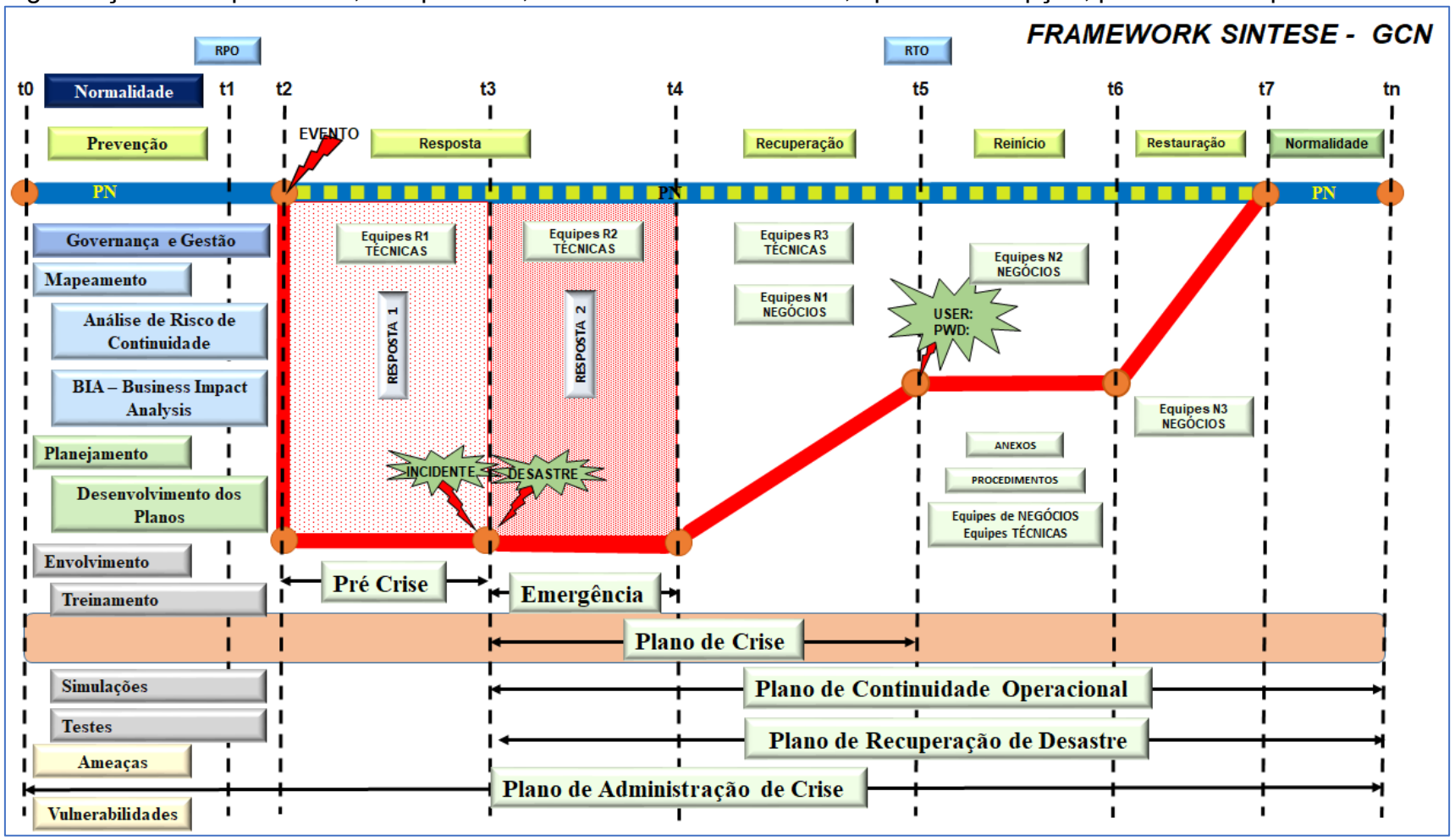


Figura 1: Framework Síntese – GCN
Fonte: Elaborado pelo autor (2021)

Nota 1: Trata-se do ciclo de vida da GCN.

Nota 2: Normalmente, isto abrange recursos, serviços e atividades necessárias para assegurar a continuidade de funções críticas de negócios.

As principais etapas na Gestão de Continuidade de Negócios podem ser descritas de acordo com o *timeline*.

2.1.1 Governança e Gestão Programa

Trata-se do período de normalidade:

- Atualização dos planos, de acordo com mudanças no negócio.
- Registro e reporte dos incidentes e atividades realizadas.
- Definição de canais de emergência e classificação de incidentes e crise.

O COBIT (COBIT[10] 5, p. 34) é um *framework* (Figura 4) e cada organização deverá definir seu próprio conjunto de processos, levando em consideração sua situação específica. Incorporar um modelo operacional e uma linguagem comum para todas as partes da organização envolvidas com atividades de TI é uma das etapas mais importantes e críticas da boa governança. Este modelo divide os processos de governança e gestão de TI da organização em dois domínios de processo principais:

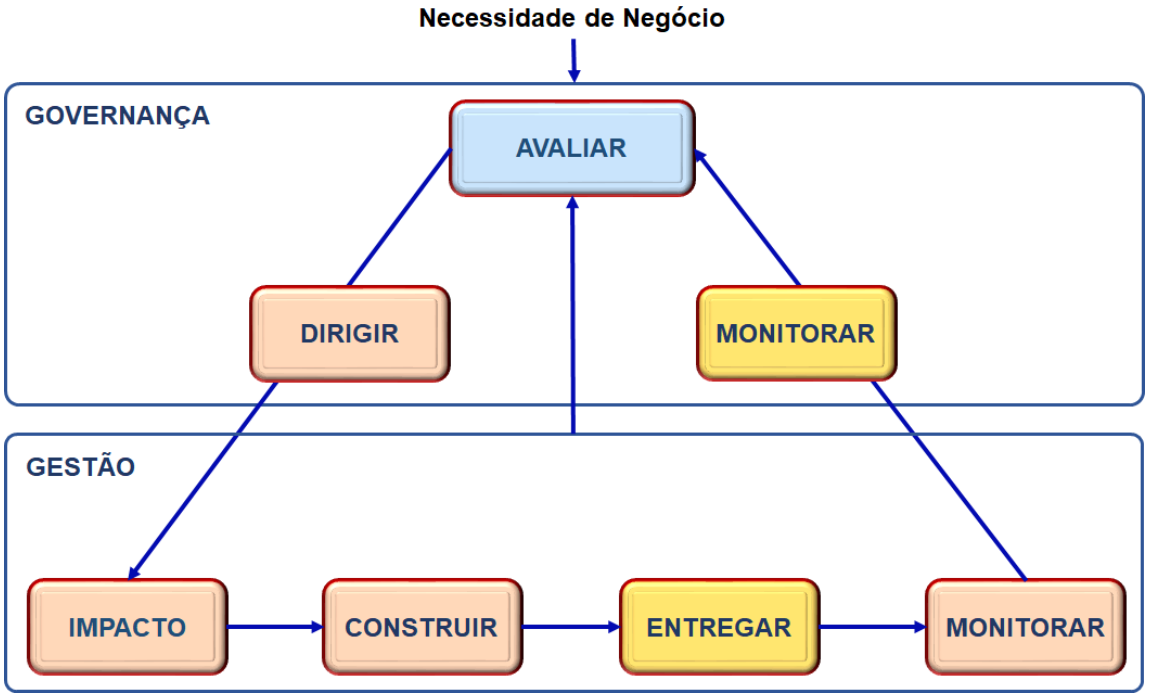


Figura 2 – Modelo - Governança – Gestão
Fonte: Cobit 5 (p. 34)

Governança - contém três processos de governança, sendo que dentro de cada processo são definidas práticas para Avaliar, Dirigir e Monitorar (*Evaluate, Direct and Monitor - EDM).* [14]

Gestão - contém quatro domínios, em consonância com as áreas responsáveis por planejar, construir, executar e monitorar (*Plan, Build, Run and Monitor - PBRM*), e oferece cobertura de TI de ponta a ponta.

2.1.2 Mapeamento

No mapeamento, olham-se os pontos críticos identificados e priorizados.

2.1.2.1 Análise de riscos de continuidade

A análise de riscos de continuidade não fala dos riscos em si, mas sim analisa o grau de exposição deste centro de Tecnologia de Informação, sejam exposições de ação natural (vendaval, inundação, fogo) ou aquelas derivadas da ação do homem (sabotagem, erro ou falha humana). É importante salientar que o crescimento da *internet* fez surgir um novo fator de risco, que expõe eletronicamente o negócio de grandes organizações. Estes riscos podem deixar o Centro de Tecnologia da Informação exposto, vulnerável e até inoperante. Indague-se se prevenir estas falhas, quer seja por meio de recursos de tecnologia de *software*, *hardware*, biometria, ou simplesmente aumentar a segurança física do local, são suficientes para minimizar os riscos desta natureza.

Implementar estas correções requer, em muitas situações, uma ação rápida não deixando de observar aquilo que é economicamente viável à organização e seu principal negócio para o mercado.

14 No contexto do domínio de governança, '**monitorar**' significa avaliar em que o órgão de governança verifica a medida de orientação definida para a gestão e sua efetiva aplicação.

2.1.2.2 Análise de impacto nos negócios ou BIA – *Business Impact Analysis*

A **BIA**, devido a sua complexidade e particularidades, deve ser realizada separadamente de um PCN, pois atuará fortemente nos três seguimentos do PCN. Uma análise BIA verifica o impacto nos processos de negócio da organização.

Uma organização, seja qual for (nosso foco é a financeira), atualmente possui alta dependência de tecnologia, sendo que seus dados/informações estão armazenados em um ambiente computacional. As perdas tangíveis (faturamento, clientes etc.) e intangíveis (reputação, imagem, aceitação no mercado etc.) em algumas organizações podem chegar a cifras altíssimas (milhões, até bilhões de reais). Como exemplo, destaca-se o parlamento europeu, acusando e cobrando multa de US$ 612 milhões da Microsoft. Dependendo do porte da organização ou sua "saúde" financeira, o valor da recuperação pode causar até a extinção total das operações em um curto espaço de tempo.

Nesta pesquisa (BIA), almeja-se identificar as aplicações (*hardware, software, peopleware.* mais críticas para o negócio e o tempo de recuperação necessários para a continuidade de negócio.

2.1.3 Planejamento – Desenvolvimento dos Planos

A ABNT NBR ISO/IEC 22301:2013 define que, ao planejar o GCN, a organização deve considerar as questões de entendimento da organização e seu contexto, "entendendo as necessidades e expectativas das partes interessadas", além de determinar os riscos, conforme figura 3, e oportunidades que devem ser avaliados.

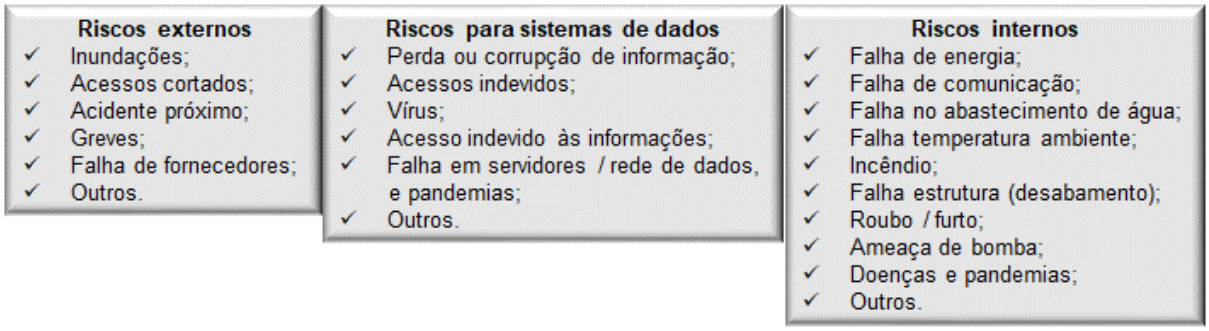


Figura 3 – Cenários de ruptura

Fonte: ABRAPP (2012), adaptado pelo autor.

Em relação às definições das estratégias, planos e ações preventivas, para execução de todas as atividades descritas, faz-se necessário um intenso período de planejamento, criação de equipes de trabalho: equipe técnica, equipe de negócio, equipe de suporte e equipe operacional. Estas equipes, em conjunto com a supervisão do profissional da área, irão desenvolver todas as atividades, tais como: cronograma, plano de teste, tomada de decisão, desenvolvimento de procedimentos e cenários além de uma árvore de acionamento. Na Figura 1 – Framework síntese – GCN, encontramos uma descrição sucinta dos planos no formato gráfico.

O *Disaster Recovery Instituite International* (DRII), órgão que difunde a continuidade de negócios no mundo, situado nos Estados Unidos e no Canadá, coletou, ao longo de décadas de suas atividades, estatísticas que afirmam que “de cada cinco companhias que sofrem interrupção nas suas operações por uma semana, duas fecham as portas em menos de três anos” (ALEVATE, 2014, p. 64).

Em pesquisa realizada por organizações que não tinham um PRD, que passaram por algum tipo de incidente que gerou uma grande perda de dados, aponta-se que 43% interromperam suas operações e nunca voltaram aos negócios, 51% fecharam dentro de dois anos e 6% sobreviveram em longo prazo (CUMMINGS et al., 2005).

2.1.3.1 Plano pré-crise

Na linha do tempo, apresentada na Figura 1, observa-se que o plano de pré-crise acontece entre os tempos “**t2**” e “**t3**”. Deve socorrer a falha com o menor tempo de resposta possível. A ocorrência de um evento15 em “t2” dá início a uma pequena

15 **Evento:** Ocorrência ou mudança em um conjunto específico de circunstâncias.
Nota 1 – Um evento pode consistir em uma ou mais ocorrências e pode ter várias causas;
Nota 2 – Um evento pode consistir em alguma coisa não acontecer;
Nota 3 – Um evento pode, algumas vezes, ser referido como um “incidente” ou um “acidente”;
Nota 4 – Um evento sem consequências pode também se referir a “quase acidente”, “incidente”, “quase colisão” ou “por um triz”.

Fonte: ABNT NBR ISO 22301:2013

crise16, pois, naquele exato momento, ainda não se sabe qual é a dimensão deste evento. Nesse momento, acionam-se imediatamente as equipes técnicas, que já foram previamente treinados para este tipo de cenário. Outra forma, a pré-crise, está entre o evento e a definição pelas equipes técnicas e se trata de um Incidente17 ou Desastre18. Portanto, cada organização necessita ter a sua própria definição de crise e de desastre. Caso seja definido que se trata de um incidente, é finalizado o processo e inicializada a sua formalização.

2.1.3.2 Plano de emergência

Na linha do tempo, apresentada na Figura 1, o plano de emergência acontece entre os tempos “t3” e “t4”.

Com o objetivo priorizar a segurança dos colaboradores, o plano de emergência deve estar sempre em pauta nas organizações, não por apenas ser exigido por órgãos fiscalizadores, mas para garantir a integridade física dos colaboradores em casos **de incidentes.** Por isso, criar um plano de emergência e divulgá-lo entre os colaboradores é tão importante. Esse documento deve ser de acesso a todos, e os treinamentos devem ser constantes, para que os colaboradores saibam como agir em casos emergenciais, como incêndios, abalos, desabamentos, bombas. A ABNT NBR ISO/IEC 15219:2020 pode servir como base para elaborar um plano contra incêndios, mas também convém que se consulte as leis e normativas exigidas pelos órgãos fiscalizadores do seu estado e município.

2.1.3.3 Plano de crise

16 **Crise** é qualquer evento ou situação que implique numa ameaça significativa para a missão, operação, integridade, recursos ou os principais *stakeholders* da organização. Onde *stakeholders* são todas as comunidades com quem a Organização se relaciona: clientes, fornecedores, acionistas, vizinhança, sindicatos, mídia, ONGs, órgãos reguladores;

Fonte: ABNT NBR ISO/IEC Guia 73

17 **Incidente**: situação que pode representar ou levar à interrupção de negócios, perdas, emergências ou crises

Fonte: ABNT NBR ISO 22301:2013

18 **Desastre** é qualquer interrupção nos processos ou funções de negócio que resulta em sérios impactos financeiros, operacionais ou ainda que necessita remanejamento para um *site* alternativo.

Fonte: ABNT NBR ISO 22301:2013

Na linha do tempo, apresentada na Figura 1, o plano de crise acontece entre os tempos **“t3” e “t5”.**

Luecke (2007) define que crise é uma mudança, repentina ou gradual que resulta em um problema urgente que deve ser abordado imediatamente. Para uma organização, uma crise representa qualquer coisa com potencial de causar danos súbitos e graves a seus colaboradores, a sua reputação ou a seu resultado financeiro.

Para Lewis (2006), crise é uma interrupção do estado normal de funcionamento que resulta em turbulência, instabilidade e perturbação significativa de um sistema.

Guindani (2011) diz que não existe uma definição exata para crise, sendo que cada organização terá sua própria definição, de acordo com o contexto e a cultura organizacional. Isto deverá ser feito dentro da política de GCN ou em política específica.

Crises bancárias podem implicar uma alta redistribuição de recursos em uma sociedade. O interesse público em manter os bancos em funcionamento demanda o desenho de regimes eficazes de resolução, pois a falência desordenada desses intermediários pode ser uma fonte de risco sistêmico. O Banco Central do Brasil - BACEN, autoridade responsável por zelar pela rigidez do sistema financeiro, pode se valer de diversos instrumentos para reestruturar ou liquidar um banco em dificuldade financeira.

O Banco Central do Brasil passou a exigir a elaboração de planos de continuidade para as maiores instituições financeiras, por meio da divulgação da Resolução nº 4.502/16, do Conselho Monetário Nacional. Destacam-se, nesta Resolução, o objetivo de “restabelecer os níveis adequados de capital e de liquidez e preservar a viabilidade das instituições, em resposta a situações de estresse, contribuindo para a manutenção da solidez, da estabilidade e de regular o funcionamento do Sistema Financeiro Nacional (SFN)”.

Modelo de gerenciamento de crises

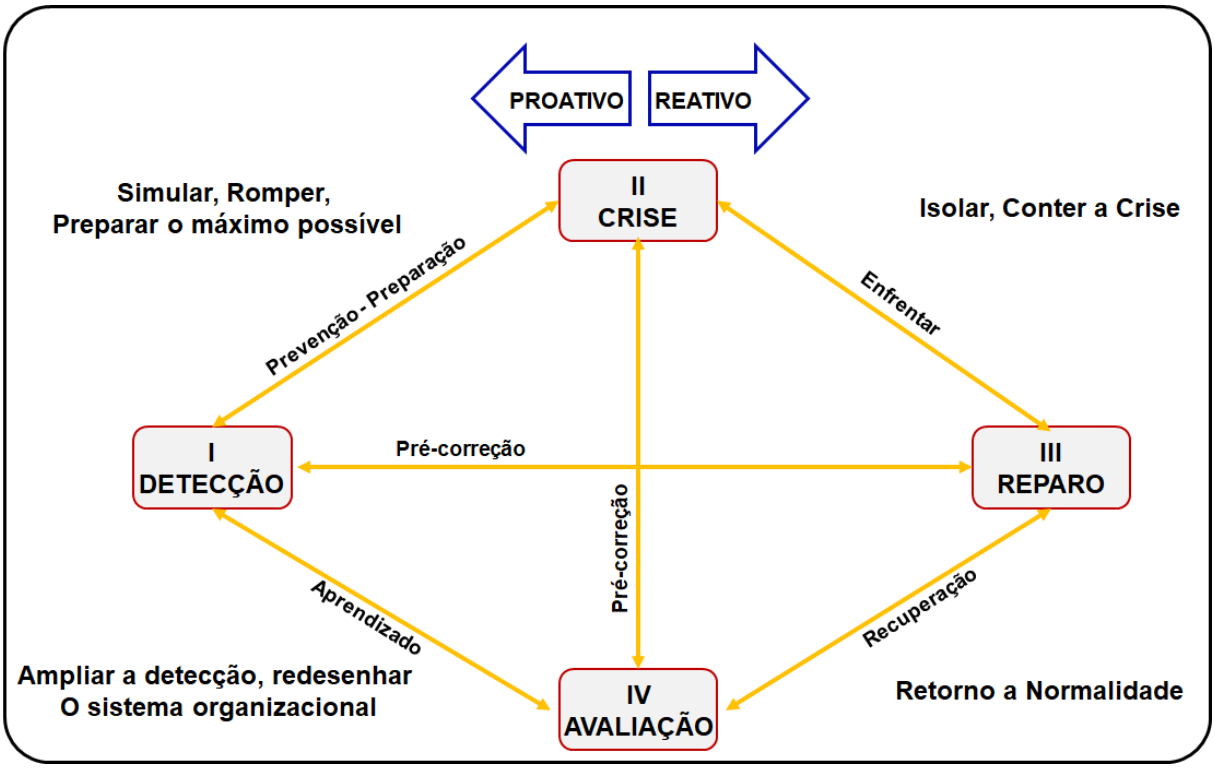


Figura 4 – Modelo de gerenciamento de crises

Fonte: Shrivastava e Udwadia (1987, tradução do autor).

A figura 4 distingue as diferentes abordagens para a gestão de crises e os preparativos para a continuidade do negócio, de acordo com o escopo da atividade projetado para atender a crise sociotécnica, e conforme a atividade seja potencialmente estratégica por natureza. Uma orientação estratégica, para nossos propósitos, é definida como uma abordagem orientada para os negócios, com base em uma combinação de planejamento e gerenciamento, que, potencialmente, leva à criação de valor ao longo prazo e vantagem organizacional. Nesse sentido, vê-se que uma organização com foco técnico operacional tem pouco mais do que capacidade de responder a uma crise, ao invés de antecipar e limitar perdas.

De acordo com a GTAG (2008), a maioria dos planos de gestão de crises são projetados para ser ativados em qualquer incidente, independentemente do impacto. Em muitos casos, são estabelecidos limites específicos antecipadamente para diversos tipos de impactos, para eliminar a subjetividade geralmente associada ao escalonamento de um evento. Esses critérios de escalonamento devem incluir impactos humanos, financeiros e operacionais e serem diretos o suficiente para permitir que os colaboradores de nível gerencial, em qualquer lugar em que a

organização atue, saibam se é necessário escalonar recursos para a equipe de gestão de crises. Da mesma forma, o uso consistente dos limites em toda a entidade ajuda a equipe de gestão de crises a ter certeza de que, se ainda não tiver sido contatada, o evento não excedeu os limites pré-estabelecidos.

Fases da crise

Tempo é um recurso que jamais deve ser desprezado quando se fala dos assuntos aqui abordados, pois o exato momento em que um evento transforma a ameaça em realidade é determinante para o sucesso ou fracasso da organização. Antes, durante e após um evento, a organização passa por momentos importantes, até seu retorno à normalidade19 (GOES, 2005, p. 166).

Por outro lado, a metodologia PR4, apresentada na Figura 1, indica prevenção, responder, recuperar, retomar (reinício) e restaurar (ISO 22301:2013), apresentando cinco fases. É possível compor estas cinco fases em três dimensões, conforme apresentadas por Goes (2005). A fase prevenção adicionada com a detecção pode ser estabelecida como antes da crise ou pré-crise. A fase de contenção, composta por resposta e recuperação, pode delimitar-se como a fase de durante a crise, e as fases de reinício, restauração e aprendizagem podem caracterizar-se como depois da crise ou pós-crise.

Antes da crise

Para Coombs e Laufer (2018), a fase da pré-crise é destinada à prevenção e à preparação para um possível momento de crise, a fim de minimizar erros. Deveney (2018) defende que a organização deve estabelecer um plano de contingência para que possa responder rapidamente às partes interessadas. Nos primeiros passos, são traçados os riscos e previsões de possíveis rupturas, de diversas motivações e, também opções de respostas e níveis de gravidade. O primeiro passo ainda especifica outras ações que podem ser tomadas, como a análise das redes sociais, opiniões dos *stakeholders* e a criação de uma *landing page* específica para tratar do assunto.

19 **2º CONTECSI** – Congresso Internacional de Gestão de Tecnologia e Sistemas de Informação. 01-03 de junho 2005 – FEA USP São Paulo Brasil

Durante a Crise

A organização é foco de observação de setores e da sociedade neste momento, sendo que a transparência é fundamental (DEVENEY, 2018). A fase que ocorre durante o problema é o momento crucial, que representa a estratégia de resposta e de posicionamento da organização aos *stakeholders* (COOMBS; LAUFER, 2018).

Esta fase se caracteriza pelo esforço de conter e limitar o problema e evitar que se espalhe ainda mais (FEARN-BANKS, 2017). Avaliar o volume, a intensidade e a significância são os primeiros procedimentos a serem tomados, assim como colocar em prática o que foi definido na fase anterior (DEVENEY, 2018). É importante perceber, de forma clara e objetiva, o que ocasionou o problema, a natureza da adversidade e as acusações, para assim responder corretamente aos eventos (BENOIT, 2012).

Depois da Crise

Uma crise nunca deve ser enfrentada sem que haja lições aprendidas. Esta é a fase de avaliar, mensurar as perdas e ganhos e documentar os fatos acontecidos (DEVENEY, 2018).

Benoit (2012) cita que o segredo para desenvolver uma boa estratégia de resposta e reparar a imagem vem da atitude de perceber a natureza dos ataques que provocaram a situação de crise, que podem ter duas vertentes: i) quando a Organização é responsável pelo infortúnio; ii) ou quando o ato é considerado ofensivo. O reparo da imagem é pensado com o objetivo de reduzir os efeitos negativos que a situação pode causar à uma organização. Coombs (2015b. formulou essa estratégia de resposta em quatro grupos, nos quais cada componente desenvolve uma estratégia de resposta diferente: i) negação; ii) redução de ofensas; iii) reforço; e iv) reparação.

Comunicações da Crise

Esse tópico é um dos principais fatores para o sucesso da gestão de crise (GUINDANI, 2011).

O planejamento da comunicação de crise é parte integrante de um programa holístico de GCN e é mais frequentemente coordenado pela comunicação interna, relações públicas ou outro departamento com profissionais de comunicação. Planos de comunicação de crise, quando existem, abordam como gerenciar as mensagens de mídia após um evento de crise. Em todos os casos, o processo de comunicação de crise deve ser uma função subordinada ao processo geral de continuidade de negócios, em vez de um esforço autônomo (GTAG, 2008).

É necessário avaliar criteriosamente tudo o que foi divulgado durante as situações de crise, bem como os possíveis meios de comunicação que minimizem os impactos para a organização, seus empregados e familiares, clientes, fornecedores, investidores e gestores corporativos.

Planos eficazes de comunicação de crise são projetados para comunicar, de forma proativa, uma mensagem integrada a vários *stakeholders*, de uma maneira que seja relevante para as audiências individuais. Pontos de comunicação relevantes para a comunidade financeira podem não ser tão relevantes para funcionários ou vizinhos, no entanto, a mensagem principal deve ser consistente. Embora seja impossível antecipar todos os aspectos das comunicações de crise a serem implementadas durante um evento, alguns públicos devem ser abordados nos planos e nos esforços de preparação. Estes incluem:

a) Membros da equipe de resposta da organização;
b) Gerentes responsáveis pela continuidade das operações e pelo contato direto com os colaboradores;
c) Colaboradores de linha cuja compreensão dos problemas mais amplos possa ser menos completa do que a da equipe de administração;
d) Membros da família de colaboradores, especialmente os familiares dos colaboradores diretamente impactados pelo evento ou pela resposta da organização;
e) Mídia nacional, incluindo a mídia financeira, cujo interesse na organização esteja focado principalmente na gestão do evento atual;

f) Mídia local, impressa e transmitida, que cubra a organização regularmente em uma ampla variedade de tópicos;
g) Investidores, especialmente investidores institucionais, que desejem transparência nas consequências de curto e longo prazo de um incidente;
h) Governos locais e estaduais que estejam interessados na viabilidade a longo prazo da base tributária e outros benefícios que a organização traga para seus constituintes;
i) Agências reguladoras responsáveis por garantir a conformidade contínua, mesmo operando em modo de recuperação;
j) Vizinhos que possam ser afetados negativamente pelo evento, pela resposta da organização ou pelos esforços das autoridades para minimizar o impacto geral sobre a comunidade (GTAG, 2008).

A necessidade de uma equipe multidisciplinar para administrar as crises

A gestão de crises precisa ser estudada e abordada de forma integrada, para que as suas ações tenham maior eficácia. Os profissionais têm-se organizado em grupos de ação, preparados para evitar que os eventos súbitos desencadeiem as ameaças às organizações, mas que tenham também capacidade de agir durante essa fase da gestão de crises e saibam transformar as dificuldades enfrentadas em aprendizados e mudanças para evitar futuras crises.

A atuação isolada pode, além de perder a sua eficácia, provocar resultados que prejudiquem ainda mais a organização.

2.1.3.4 Plano de Recuperação de Desastre

Na linha do tempo, apresentada na Figura 1, o plano de recuperação de desastre acontece entre os tempos “**t3**” e “**tn**”.

O planejamento de recuperação de desastres (*Disaster Recovery Planning – PRD)* é um termo usado para descrever a recuperação de TI. Algumas organizações usam termos diferentes, para incluir a recuperação de sistemas de TI, dados, sistemas e processos de gestão de informações e outros sistemas relacionados. O documento

de recuperação de desastres deve descrever as estratégias de recuperação dos sistemas de gestão de informações e TI.

Para o GTAG (2008), o PRD deve incluir instruções detalhadas de recuperação, que podem englobar referências: a procedimentos, de fornecedores, diagramas do sistema e outros materiais de recuperação relacionados. Os procedimentos detalhados de recuperação devem ser atualizados sempre que os processos do sistema e de negócios forem alterados.

Shrivastava e Somasundaram (2009, p. 254) descrevem métricas para dimensionar disponibilidade, por meio de porcentagens de tempo em que seu ambiente está operacionalmente ativo.

Tabela 1. Porcentagem de disponibilidade e tempo inativo permitido

%	% Downtime	Downtime por Ano	Downtime por Semana
98,0000	2	7,3 dias	3h22 min
99,0000	1	3,65 dias	1h41 min
99,5000	0,500	1,82 dias	50 min 53 seg
99,8000	0,200	17h 30min	20 min 10 seg
99,9000	0,100	8h 45min	10 min 5 seg
99,9900	0,010	52,5 min	1 min
99,9990	0,001	5,25 min	6 seg
99,9999	0,00001	31,5 seg	0,6 seg

Tabela 1 – Porcentagem de disponibilidade e tempo inativo permitido.
Fonte: Evento DRII – Orlando Set/2000 – adaptado pelo autor.

O plano visa assegurar a continuidade do processamento dos sistemas aplicativos de tecnologia da informação, que suportam as funções e os processos de negócios da organização, durante um período de contingência declarada, devido à ocorrência de um evento que impossibilite a utilização do seu *site* principal.

Devido às muitas variáveis e combinações de possibilidades uma interrupção (incluindo o tempo médio de reparo de estragos, substituição de peças, componentes ou equipamentos), as equipes (técnicas, suporte e de negócio) devem estar preparadas para tomar a decisão de declarar ou não a contingência, segundo níveis de severidade pré-definidos. Isto minimiza análises subjetivas e decisões precipitadas em situações de desastre.

Logicamente, é impossível prever todas as situações de problemas, emergências ou desastres que podem ocorrer. No entanto, neste tópico, são apresentados alguns exemplos e um critério, em forma de níveis, para a tomada de decisão, quando necessário.

Os três Níveis de Severidade relacionados a interrupções pequenas, médias e grandes, sendo que cada nível corresponde a uma situação, específica:

- **Nível 1:** normalmente são incidentes relacionados com infraestrutura ou com parte dos equipamentos. Numa situação de incidente desse tipo, normalmente não é declarada contingência, pois ele é resolvido com ações operacionais.
- **Nível 2:** estão englobadas situações que causem uma paralisação das aplicações críticas. A equipe deverá analisar o momento do desastre (se é período crítico de processamento), a previsão para retorno, à situação normal, outros fatores relativos à situação e declarar ou não contingência.
- **Nível 3:** enquadram-se, neste nível, todas as ocorrências que, pelas suas dimensões, causarão a paralisação das aplicações críticas ou algum ambiente operacional da organização por um período maior do que RTO (horas). Sem previsão de retorno à situação normal a equipe poderá declarar a contingência: i) a declaração de entrada em contingência pode ser tomada em caso de interrupção total do Data Center - *site* principal; ii) no caso de ocorrência de um problema ou desastre, em que outros fatores devem ser considerados (por exemplo, dia, horário, fatores operacionais); iii) as definições apresentadas acima são conceituais e têm como objetivo auxiliar no processo de tomada de decisão pela declaração ou não de contingência.

2.1.3.5 Plano de Continuidade Operacional

Na linha do tempo, apresentada na Figura 1, o plano de emergência acontece entre os tempos **“t3” e “tn”.**

O papel do Plano de Continuidade Operacional - PCO - é listar os processos considerados críticos e garantir a continuidade das atividades-chave de uma organização nos cenários mais desastrosos. A tecnologia e as ferramentas digitais, cada vez mais, ganham um papel central dentro das organizações, independentemente do porte ou segmento de atuação destas.

Por essa razão, muitas vezes, problemas como servidores danificados ou um site fora do ar podem afetar diretamente a rentabilidade e os negócios. Desastres podem ser causados pelas mais diferentes razões — desde falhas no *hardware* até catástrofes naturais, como temporais e alagamentos.

A identificação de cenários de ruptura é necessária para a determinação do ponto de recuperação e de seleção das estratégias de continuidade.20A variedade de causas também leva a um leque de consequências que podem afetar mais ou menos as operações das organizações, a depender de quais são as atividades-chave de cada uma.

Em pesquisa realizada no ano de 2004, pela revista *Continuity Insights* e pela KPMG, com a participação de 410 organizações, foram apontadas as sete maiores causas de interrupção das operações. São ocorrências normais e que podem afetar os negócios de grandes corporações: 81% das organizações foram afetadas por falta de energia; 65% por desastres naturais; 62% por falhas na rede de telecomunicação; 61% por falhas de hardware; 58% por vazamento de informações; 57% por erro humano; 56% por falha de *software*. Para 64% das organizações entrevistadas, as paralisações ocorridas nos 12 meses anteriores ao período da pesquisa e causaram prejuízo médio na ordem de US$ 100,000 e, para 24% delas, de até US$ 500,000 (GUINDANI, 2008).

PCO’s são elaborados de formas diferentes de acordo, com cada uma das possíveis ameaças para os processos operacionais mais relevantes e críticos, definindo

20 **Guia de Boas Práticas para PCN** – Comissão Técnica Regional Sudeste de Governança da ABRAPP – outubro de 2012.

detalhes operacionais para cada uma das falhas de segurança e consequências possíveis em um desastre.

É preciso criar um planejamento de acordo com o contexto e com as necessidades de cada organização. Primeiro, é preciso definir quais são as prioridades do seu negócio em caso de emergência. No PCO, por meio de um passo a passo, pode-se alinhar um fluxograma com todas as tarefas que devem ser executadas por ordem de importância para a continuidade das atividades-chave.

No plano, é possível priorizar as maiores necessidades e programar quais ações são necessárias para garantir a sua continuidade, mesmo em cenários desastrosos. Essas são as suas “funções críticas aos negócios”. O plano identifica também em quais tarefas serão alocados os esforços, seja internamente ou para atender demandas de clientes.

2.1.3.6 Plano de Administração de Crise

Na linha do tempo, apresentada na Figura 1, o plano de emergência acontece entre os tempos “**t0**” e “**tn**”. O PAC pode ser considerado o plano dos planos, pois dentro dele estão todos os outros planos apresentados.

Para diferenciar um PAC de um PRD, importa definir que, segundo o glossário para a resiliência do DRII (2018). Este último trata-se de um plano que visa a recuperação de um ou mais sistemas, num local alternativo como resposta a um evento, que tenha causado a interrupção das operações, ao passo que o PAC atua a partir do instante “**t0**”.

O BCI, em 2017, em parceria com o *Disaster Recovery Journal* (DRJ), referiu os termos de PCN no glossário. A definição de *Disaster Recovery* (DR) aponta o processo como políticas e procedimentos relacionados com a preparação para recuperação e continuidade das infraestruturas tecnológicas, sistemas e aplicações que são vitais para a organização após a ocorrência de um desastre. Como nota, é ainda referido que a DR está focada na informação ou sistemas tecnológicos, que são a base para o funcionamento da organização. Enquanto isso, a Administração de Crise implica em

um planejamento, que visa manter todos os aspetos essenciais do negócio em funcionamento, antes, durante e depois da ocorrência de um desastre. De acordo com o BCI, a recuperação de um desastre é um subconjunto do Plano de Administração de Crise.

A distinção da Continuidade de Negócio está em que esta não visa apenas a recuperação das funcionalidades, mas sim garantias de que, no caso de um evento disruptivo, as funcionalidades previamente definidas como cruciais continuam a operar, mesmo que a um nível mínimo de capacidade.

É comum para os bancos atribuírem ao diretor responsável pelo atendimento dos itens requeridos pela Resolução 3380:2006 a incumbência de fazer com que o plano de recuperação seja aprovado e revisado pela alta administração anualmente. Ou sempre que julgar haver mudanças significativas nas estratégias de operação, nos modelos de negócio, na estrutura organizacional ou nos processos vinculados às funções críticas e serviços essenciais. Cabe também ao diretor garantir que o plano seja remetido ao BACEN com a mesma frequência. O diretor responsável deve ainda garantir que, ao menos a cada três anos, o plano seja submetido à revisão por unidade, independente das áreas responsáveis pela sua elaboração.

2.1.4 Envolvimento

Nesta seção, descreve-se o envolvimento dos *stakeholders* e a capacitação dos times.

Para Guindani (2008), o treinamento é item fundamental para o sucesso do GCN, que deverá receber treinamento aprofundado no tema, bem como os conhecimentos básicos deverão ser disseminados na organização. Hoje, no Brasil, existem poucos cursos disponíveis; pode ser necessário realizar um curso *in-company,* ou então aguardar as oportunidades oferecidas pelo mercado. O DRII ministra vários cursos sobre o assunto, normalmente realizados nos Estados Unidos, preparatórios para os exames de certificação existentes. Atualmente (2021), os treinamentos já podem ser realizados no Brasil – São Paulo.

Os planos de continuidade somente podem ser considerados efetivos após a validação por meio de treinamentos, simulação e testes. O processo de validação, treinamento, simulação e teste dos processos de negócio considerados críticos é essencial para o desenvolvimento do trabalho em equipe, melhoria da competência, confiança e conhecimento de todos os envolvidos. Os testes devem abranger, no mínimo, os seguintes tópicos: i) avaliação de aspectos tecnológicos, logísticos, administrativos e dos procedimentos previstos nos planos; ii) avaliação da infraestrutura especificada nas estratégias de recuperação; iii) validação da estratégia de recuperação dos recursos de TIC (tecnologia da informação e telecomunicações), inclusive quanto aos aspectos de disponibilidade e necessidade de mudança do local de trabalho das pessoas designadas para sua operacionalização.

Os planos de continuidade precisam incluir um conjunto de ações que permite avaliar a capacidade que todos os planos e procedimentos têm para responder aos requisitos de desempenho previamente definidos. É observável que, em situações muito específicas, é possível que todos os ativos dos planos não sejam testados. Os ativos são os componentes que suportam os processos de negócios. É tudo que tenha valor e que necessita de algum tipo de proteção ou cuidado por conta disso. A identificação dos ativos que necessitam de proteção é passo fundamental para o estabelecimento de qualquer estratégia.

Classificação de ativos.

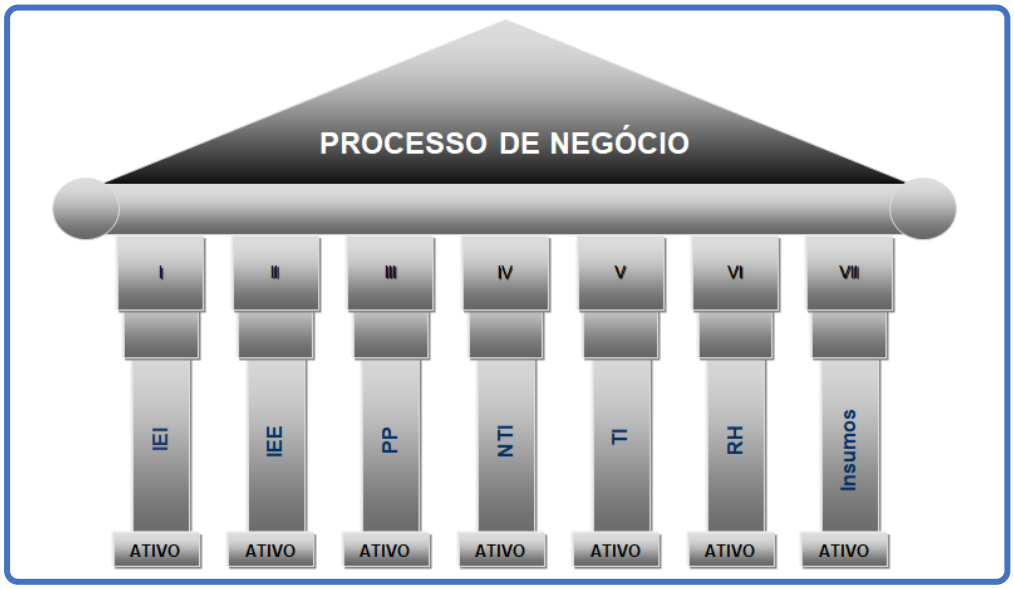


Figura 5a – Tipo de Ativo - como suporte de processos de negócios

Fonte: Elaborado pelo autor

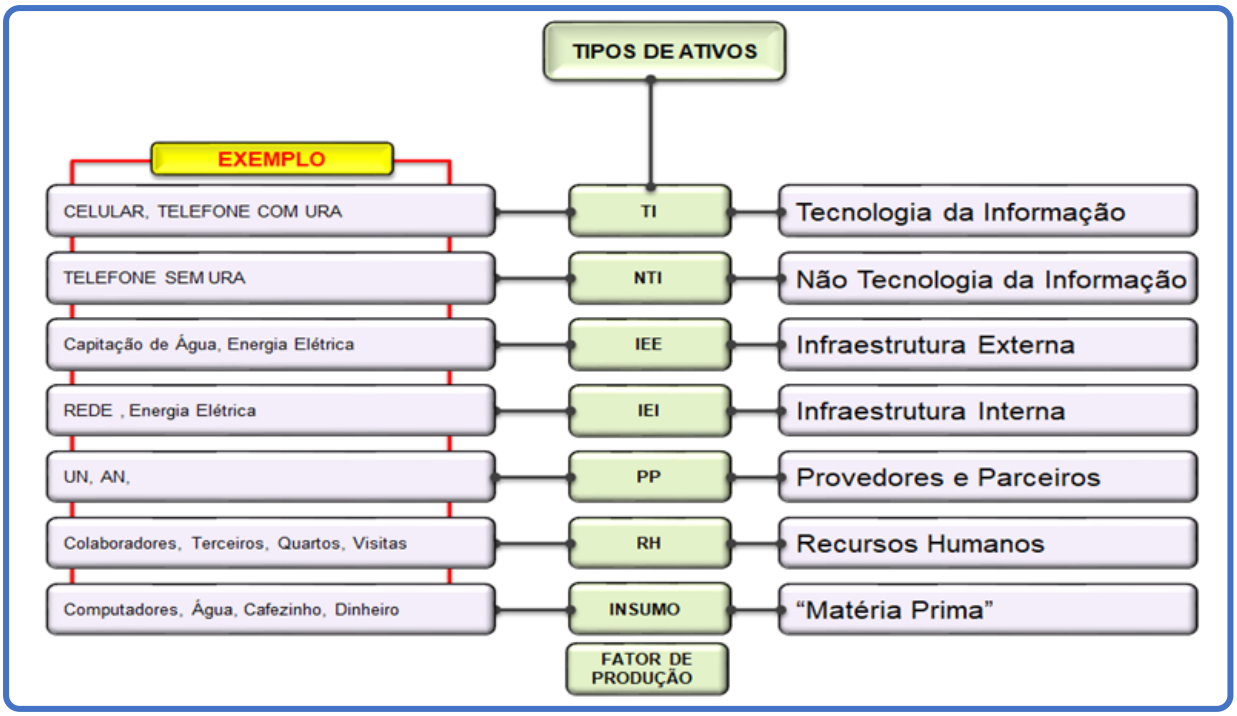


Figura 5b – Classificação de Ativos

Fonte: Elaborado pelo autor

Contudo, os testes têm por finalidade indicar um grau de segurança suficiente de que seus procedimentos endereçarão corretamente os eventuais problemas que venham a surgir, nos casos de necessidade de sua ativação.

Os testes têm como objetivo estratégico treinar, simular e assegurar aos clientes, acionistas, fornecedores e empregados que todos os processos considerados críticos da organização e a infraestrutura que as suportam sejam capazes de operar sob as mais severas circunstâncias. Sua meta, ao testar e exercitar os planos, não é apenas verificar se funcionam, mas determinar que ações e medidas corretivas serão adotadas em caso de necessidade.

Os objetivos específicos são: i) testar a funcionalidade dos procedimentos; ii) assegurar que as estratégias de recuperação atendam às necessidades do negócio; iii) capacitar todos os envolvidos; iv) identificar os pontos de falha e corrigi-los; v) manter elevados os níveis de conscientização de todos os envolvidos e aplicar para todos – pessoas, processos – a atividade de lição aprendida, bem como avaliar o grau de maturidade da organização. Sua periodicidade de realização deve ser definida em função de fatores específicos de cada organização (natureza, tamanho e

complexidade. e das características do plano e recursos envolvidos. É importante que esteja alinhado às características dos processos de negócios a que os planos são vinculados.

Várias são as categoria e tipos de planos, nos quais se destaca: *walkthroughs* ou teste de mesa, simulações, modular ou por componente, funcional (por linha de negócio), teste geral, teste programado e teste não programado. Destaca-se que, independentemente do tipo de teste, o importante é que sejam avaliadas a qualidade, eficiência e efetividade do plano e a competência e capacidade dos envolvidos na execução dos procedimentos.

Como requisitos mínimos, aponta-se: i) definir escopo e objetivos de cada teste; ii) estabelecer critérios de avaliação da efetividade dos planos; iii) que sejam mensuráveis e quantitativos e qualitativos; iv) estabelecer limites aceitáveis para considerar o teste bem-sucedido; v) definir premissas e esclarecer o que não será testado; vi) identificar os recursos necessários; vii) identificar e envolver todos os participantes, garantindo que compreendam os objetivos do teste e seus papéis e responsabilidades; viii) declarar e formalizar o roteiro de teste (sequencialmente e com os resultados esperados de cada etapa.; ix) garantir que seja de conhecimento de todos os envolvidos; e x) estabelecer mecanismos que permitam abortar o teste e retornar à situação de normalidade, no caso de ocorrência de eventos ou resultados imprevistos ou indesejados.

Após a realização de testes, as seguintes atividades devem ser analisadas: i) traslado até o site alternativo com tempos de espera, deslocamento, entrada e retornos; ii) avaliação dos resultados alcançados; iii) esperados *versus* obtidos; iv) resultados inesperados; v) análise dos pontos de falha e identificação de alternativas de correção; vi) identificação de oportunidades de melhoria, por meio de lições aprendidas; vii) definição de plano de ação e responsáveis pela correção de falhas e implementação das melhorias identificadas; viii) elaboração de relatório, detalhando os procedimentos executados, duração, envolvidos, resultados alcançados, pontos de falha, oportunidade de melhoria, necessidade de revisões nos planos e roteiros de testes.

2.1.4.1 Análise e avaliação de vulnerabilidade

A técnica de análise de vulnerabilidade busca encontrar e eliminar qualquer brecha ou falha que possa ser utilizada por *hackers* ou demais pessoas mal-intencionadas, para terem acesso a dados e informações confidenciais.

A origem das vulnerabilidades, na maioria das falhas e brechas de segurança, são frutos de determinadas situações ou ações que podem ser evitadas por meio de uma identificação e de tratamento. Entre as principais origens, estão a falha humana, na qual colaboradores sem treinamento acabam por clicar em *links* suspeitos ou baixar documentos indevidos, erros de programação, isto é, falhas no desenvolvimento de sistemas que mantêm brechas que podem ser utilizadas por *hackers* para realizar invasões, ou ainda a má configuração: aplicativos de segurança que são aplicados, mas não contam com a configuração correta e não garantem um funcionamento adequado.

Pode-se elencar, como objetivo da análise de vulnerabilidades, o processo de levantar falhas ou ausências em um conjunto de proteções21, ao passo que avaliação de vulnerabilidade é a combinação da análise com uma lista de ameaças, no intuito de avaliar a probabilidade de elas ocorrerem.

2.1.4.2 Ameaças

Segundo o DRII – *Disaster Recovery Institute International* (2007), a ameaça está intimamente ligada com a Relação de Causa e Efeito, conforme Figura 6. Ameaça é tudo aquilo que tem potencial de causar algum tipo de dano aos ativos.

21 **Proteção:** É prática, **procedimento ou mecanismo que pode proteger** os ativos contra ameaças, reduzir ou eliminar vulnerabilidades, limitar os impactos de um incidente ou ajudar na sua detecção, facilitando a correção e a recuperação dos estragos causados.

Fonte: ABNT NBR ISO 22301:2013

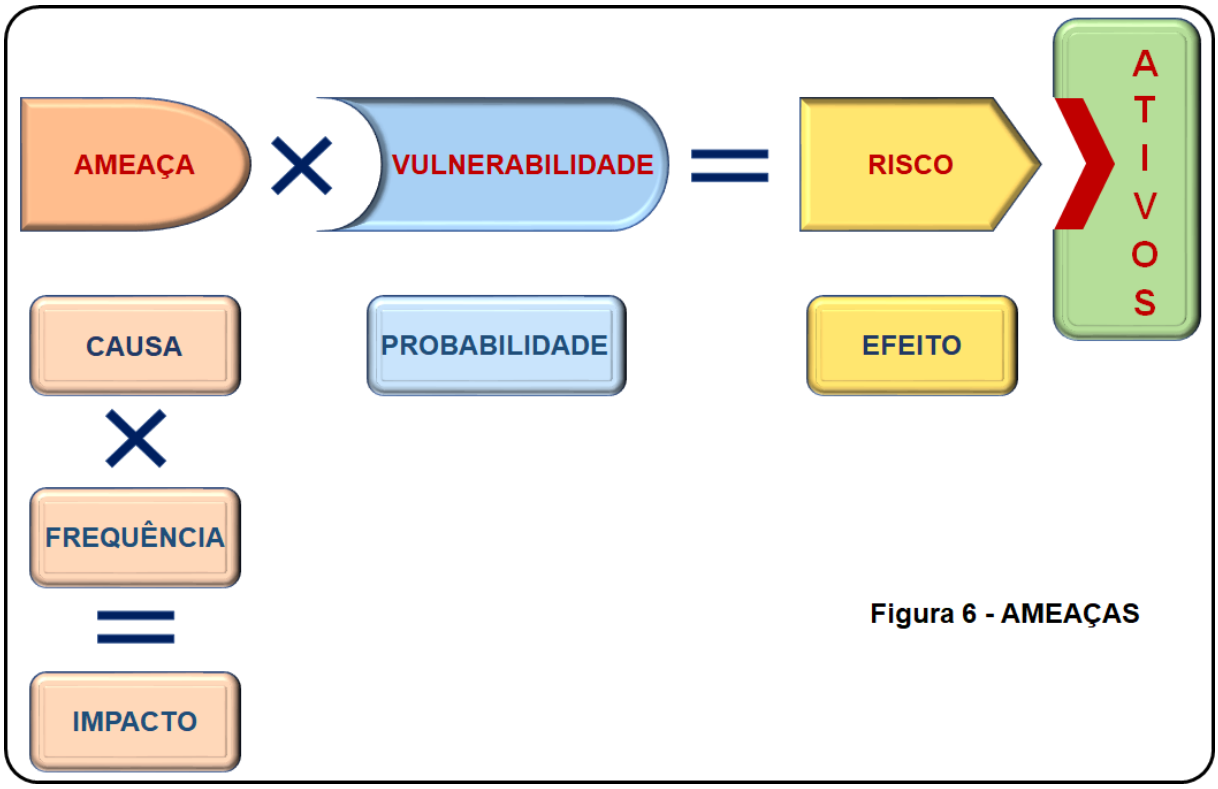


Figura 6 – Ameaças.

Fonte: DRII – 2007 – adaptado pelo autor

Os prejuízos causados por uma ameaça se enquadram, basicamente, em duas categorias: danos diretos aos ativos e danos causados por situações inesperadas. Tem-se, como origem ambiental – fenômenos naturais, interrupção de serviços básicos, ou ainda, eventos que não causam prejuízos sem o envolvimento direto de pessoas, como incêndios ou quedas de aviões. Outro tipo, são as humanas - causadas diretamente pela ação de pessoas. Estas estão divididas em ameaças humanas **acidentais** (erros de operação ou manipulação de informações) ou **intencionais**, como inserção de vírus, roubo de informações e invasão de sistemas.

A ameaça pode ser usada para identificar ações de mitigação, abordagem para coleta de dados e identificar quais planos são necessários.

Quanto aos tipos de ameaça, cada organização pode criar sua lista: i) naturais: furacões, deslizamentos, tempestades, tsunamis, enchentes, raios, secas; ii) infraestrutura: energia; recursos tecnológicos, infraestrutura predial, transporte; iii) recursos humanos: incêndios, explosões, terrorismo, greves e paralisações, fraudes, erros operacionais; iv) tecnológicos (WEB.: vírus, *hacker, spyware*, cavalo de Tróia,

spim, spam, *phishing, malwares, hijacks, ransomware*; v) químicos: corrosão, drogas, toxidade, contaminação com produto químico.

Desastres externos: são catástrofes naturais (enchentes, fogo, queda de raio, vendaval); desastres causados por pessoas (incêndio, explosão, exposição química.; terrorismo (ameaça de bomba, sabotagem, crime organizado, rapto, outras ameaças intencionais); acidentes em geral (explosões, queda de aeronave.; impedimentos de acesso ao local de trabalho.

Desastres internos: são falhas prolongadas em: equipamentos, infraestrutura ou nas instalações físicas de TI; problemas operacionais graves (erros ou problemas causados por profissionais intencionalmente ou não, situações imprevistas); desastres causados por pessoas (incêndio, explosão, exposição química); greves; sabotagem Interna.

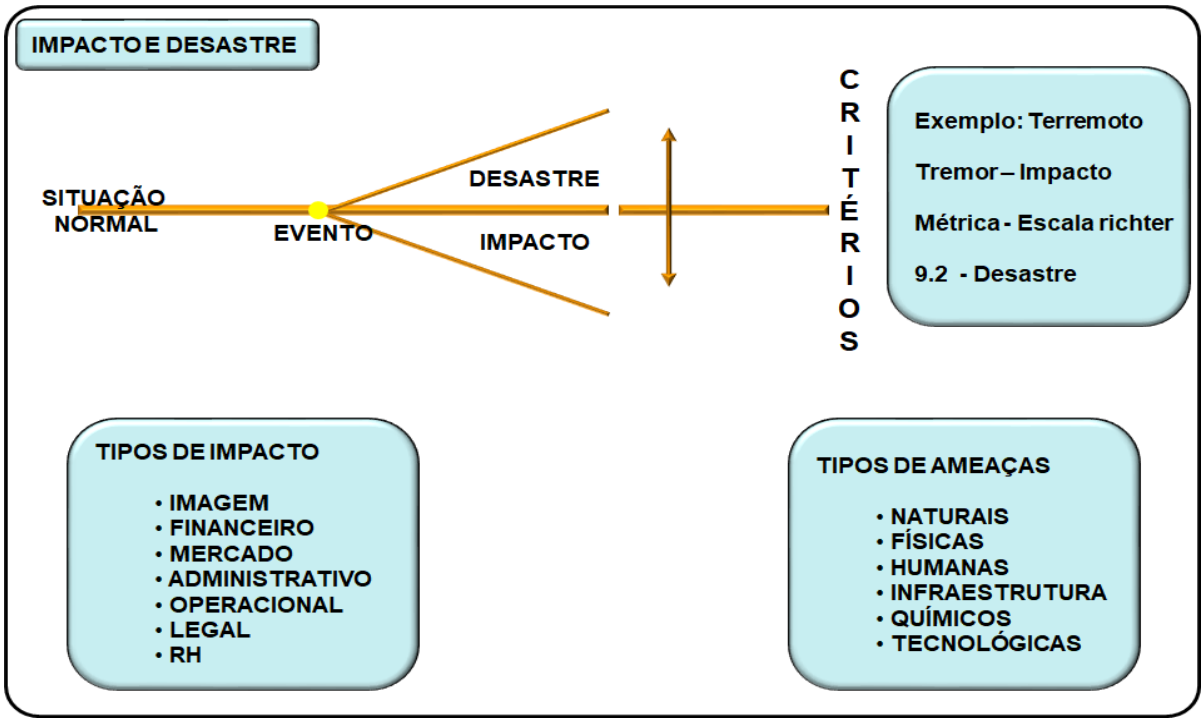


Figura 7 – Critérios para definição de Impacto - Desastre

Fonte: Elaborado pelo autor

Cenários fora do escopo: estão relacionados aos desastres em *sites* não contemplados no contrato. São falhas físicas ou lógicas, que permitam a recuperação

no *site* principal num prazo inferior que o RTO definido no plano contratado; falhas que afetem ambientes, aplicações vitais ou serviços fora de escopo.

2.1.4.3 Cenário

A indisponibilidade de acesso físico, indisponibilidade de tecnologia da informação, e indisponibilidade de pessoas são exemplos de cenário para GCN, entretanto não se limitando a estes. Cenário engloba um desastre natural ou causado por pessoas, que afete habilidades e localidades previstas em contrato, falta de entrega de seus serviços, por meio de seu *site* principal, resultando na necessidade de transferi-los para o *site* contratado/estabelecido pela organização. Inclui ainda parada planejada no *site* principal, com duração superior ao tempo para virada (RTO, veja item 2.1.4.5) e retorno do ambiente à situação normal, resultando na necessidade de transferir seus serviços para o *site* alternativo.

Tipos de *Sites* Alternativos

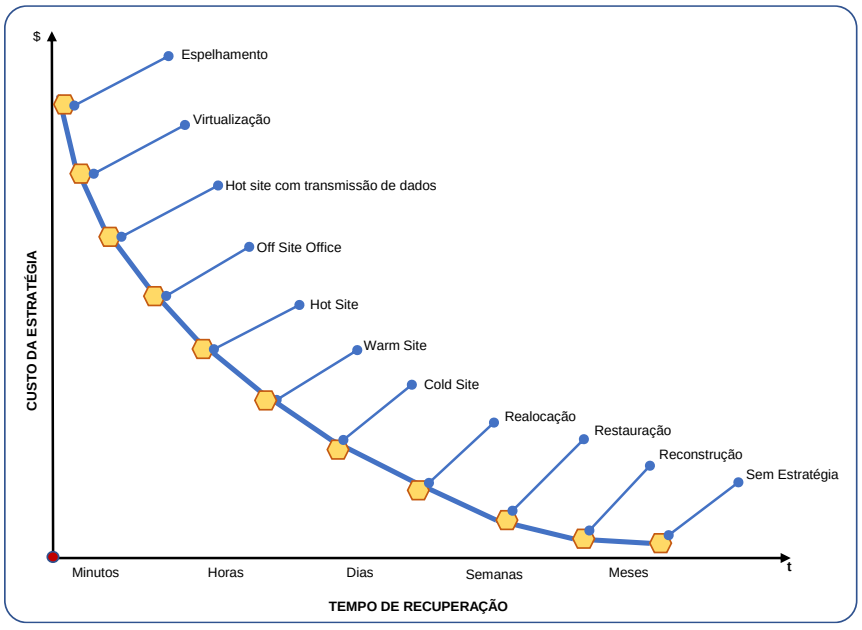


Figura 8 – Tipos de ***Sites*** Alternativos

Fonte: Guindani (2011), adaptada pelo autor.

2.1.4.4 Equipes

Todas as atribuições referentes a uma simulação, teste e exercício devem ser distribuídas e ordenadas adequadamente, para que não haja sobreposição de atividades entre as equipes. O mesmo ocorre para o momento em que se fizer necessário, quando acontecer um evento, independente do seu tamanho.

Para que um planejamento seja realizado e documentado de forma realmente eficiente e eficaz, as atividades referentes à sua recuperação devem ser específicas. Esse planejamento é executado em caso de emergência, prevalente sobre quaisquer outros que estejam fora dos procedimentos de continuidade (Guindani, 2011).

Os papéis e responsabilidades das equipes podem ser vistas na Figura 9 a seguir.

Distribuição de Equipes.

Figura 9 – Distribuição de Equipes.
Fonte: elaborado pelo autor (2021).

Equipe de Gerenciamento de Crise ou Equipe EGC.

Esta é a equipe mais volátil entre todas, pois é composta por colaboradores internos, pertencentes a áreas de negócios envolvidas. Também fazem parte desta equipe

colaboradores do corpo diretivo, além de, em alguns casos, terem participantes externos à organização, como, por exemplo: bombeiros, policiais, agentes hospitalares, entre outros.

A EGC tem por atividades: i) avaliar e analisar, juntamente com o “Responsável PCN”, todo e qualquer potencial de risco de interrupção, e o impacto que este poderá gerar na continuidade dos processos críticos de negócios; ii) gerenciar as demais equipes de ação e atuar como interface com os colaboradores e demais órgãos ou organizações que serão comunicadas, caso a área de negócio necessite acionar a sua contingência; iii) prover informação atualizada para Assessoria de Imprensa, juntamente com a EGC; iv) definir a necessidade ou não de acionamento do PCN; v) declarar que entrou em contingência; vi) definir a necessidade ou não de acionamento do site alternativo; vii) definir e formalizar a todos os colaboradores e áreas de negócio que farão parte desta equipe.

Equipe de Pessoal Generalista ou Equipe EPG.

Esta é a primeira equipe a entrar em operação após seu acionamento.

A EPG deve estar preparada para responder imediatamente a um chamado/declaração de contingência. É composta por um colaborador eleito como líder, que é o ponto focal, e por colaboradores que possam, num primeiro momento, desempenhar mais de uma função. Esses colaboradores devem ter capacidade técnica, iniciativa e ampla visão do processo de negócio considerados críticos, e estarem voltados à recuperação dos processos.

Nota: A EGC avisa o líder da EPG que, por sua vez inicia, a “árvore de acionamento”. Alguns colaboradores serão contatados e terão a incumbência de transmitir as instruções recebidas aos demais, previamente separados em subgrupos.

Equipe de Pessoal Especialista ou Equipe EPE.

O principal objetivo desta equipe é suprir a necessidade de recurso humano - colaboradores para a equipe EPG.

A EPE é um grupo de colaboradores que poderão ser acionados pela EGC ou EPG num segundo momento, após o restabelecimento dos processos de negócios considerados críticos no site alternativo pela EPG. A função é suprir a crescente demanda após o evento e desempenhar tarefas e atividades que não foram executadas num primeiro momento, devido a uma *criticidade* menor.

Equipe de Pessoal de Plantão ou Equipe EPP.

Seu principal objetivo é suprir a necessidade de recurso humano - colaboradores para a equipe EPE.

A EPP é um grupo de colaboradores que serão acionados pela EGC, EPP ou EPE num terceiro momento, em que os processos de negócios considerados críticos já estão operando em contingência, mas que necessitam de mais mão-de-obra para operar.
Outra característica que pode ser atrelada a esta equipe é o raio de ação (20 km de sua residência, por exemplo), dentro do qual os colaboradores podem atuar, lembrando que estão de plantão e devem responder imediatamente se forem chamados.

Equipe de Pessoal de "*Stand by*" ou Equipe EPS.

O principal objetivo da equipe EPS é suprir a necessidade de recurso humano para a equipe EPP.

A EPS é um grupo de colaboradores que serão acionados pela EGC ou EPS ou EPE ou EPP, e que aguardarão, em local pré-definido, os procedimentos que deverão ser seguidos.
Outra característica que pode ser atrelado a esta equipe é o raio de ação (50 km de sua residência, por exemplo, dentro do qual os colaboradores podem atuar, lembrando que estão de plantão e devem responder imediatamente se forem chamados.

Matriz de mobilização dos colaboradores entre equipes.

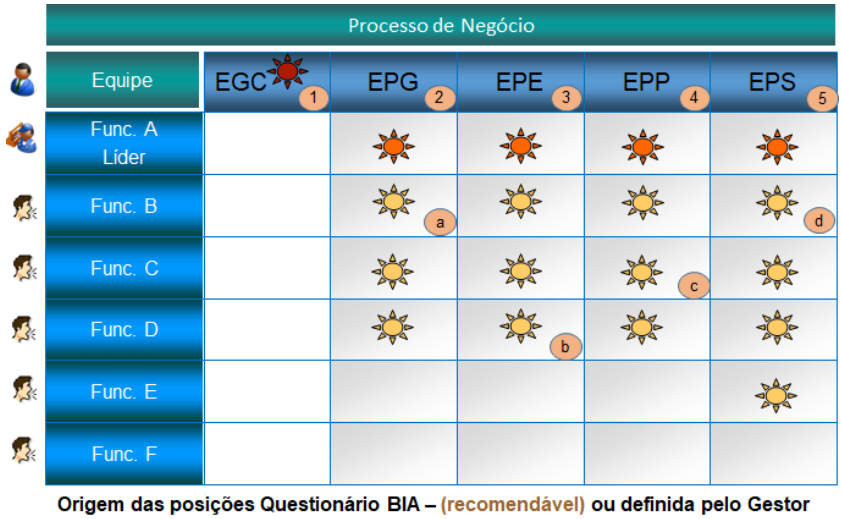


Figura 10: Matriz de mobilização dos Colaboradores entre as Equipes.
Fonte: desenvolvida pelo autor (2021)

A dinâmica de utilização da Matriz de Mobilização dos Colabores entre as Equipes é bastante simples, sendo que basta que se sigam as regras validadas para todas as áreas de negócios.

Regras

i. Todas as equipes devem ser compostas por um líder, que é considerado ponto focal;
ii. Todas as equipes devem possuir colaboradores das respectivas áreas de negócios.

Dinâmica

- O líder (1) da Equipe EGC entra em contato com o líder (2) da Equipe EPG, líder (3) da Equipe EPE, líder (4) da Equipe, EPP e líder (5) da Equipe EPS.
- O líder (2) da Equipe EPG entra em contato com os colaboradores da sua equipe. Caso algum colaborador(a) não responda ao seu chamado em tempo hábil, o referido líder entrará em contato com o líder EPE (3).

  O líder (3) entra em contato com colaborador (b) de sua equipe e o encaminhará para fazer parte da equipe (2) EPG. Por outro lado, o líder (3) entrará em contato com o líder (4), solicitando um colaborador para compor sua equipe.

O líder (4) entra em contato com colaborador (c) de sua equipe e o encaminhará para fazer parte da equipe (3) EPE. Por outro lado, o líder (4) entrará em contato com o líder (5), solicitando um colaborador para compor sua equipe.

O líder (5) entra em contato com colaborador (d) de sua equipe e o encaminhará para fazer parte da equipe (4) EPG. Por outro lado, o líder (5) apenas cede colaboradores, isto é, em sua equipe não se repõem colaboradores.

Nota: Este processo se repete tantas vezes quantas forem as faltas de colaboradores nas respectivas equipes.

2.1.4.5 Recovery Point Objective e Recovery Time Objective

A ABNT NBR ISO 22301:2013 define:

- ***R**ecovery **P**oint **O**bjective* – **RPO** (acontece em "**t1**" – conforme descrito na Figura 1) – em português: ponto objetivado de recuperação - ponto em que a informação usada por uma atividade deve ser restaurada, para permitir a operação da atividade na retomada.

  Nota: Também pode ser referido como "perda máxima de dados".

  Observação: o termo RPO é muito conhecido/confundido no mercado como sendo *backup*, porém esta é uma forma parcialmente errada de se entender este termo. Deve haver cautela em sua utilização.

- ***R**ecovery **T**ime **O**bjective* – **RTO** (acontece em "**t5**" – conforme descrito na Figura 1) – em português: tempo objetivado de recuperação – tempo após um incidente em que o produto ou serviço deve ser retomado, ou a atividade deve ser retomada, ou os recursos devem ser recuperados (NBR 2 3,45).

  Nota: Para os produtos, serviços e atividades, o tempo objetivado de recuperação deve ser menor do que o tempo em que os impactos negativos surgirão como resultado de não fornecimento de um produto/serviço ou da realização de uma atividade inaceitável.

2.2. Benefícios

Como benefícios, pode-se destacar: i) capacidade de identificar proativamente os impactos de uma interrupção operacional; ii) capacidade de resposta eficiente às interrupções, o que minimiza o impacto à organização; iii) capacidade de gerenciar os riscos que não podem ser segurados; iv) oportunidade de promover o trabalho entre equipes; v) capacidade de demonstrar uma resposta possível, por meio de um processo de testes; vi) capacidade de melhorar a reputação; vii) ganhar vantagem competitiva por meio da capacidade demonstrada de manter seus produtos e serviços disponíveis frente a uma situação de crise; viii) redução de custos financeiros, derivados da parada dos seus processos de negócios considerados críticos e redução dos riscos e impactos inerentes a eventos; ix) redução do tempo de resposta, frente à indisponibilidade de componentes/ativos que suportam os principais processos de negócios; e x) possibilidade de negociação de redução do Prêmio de Lucros Cessantes.

2.3. Regulamentação

Quadro 2 – Regulamentação

Ano	Norma	Descritivo
2004	ANZ HB 221	Business Continuity Handbook
2006	ANZ HB 292	A Practioners Guide Business Continuity Management
2006	ANZ HB 293	Executive Guide to Business Continuity Management
2017	DRII	Melhores práticas – 10 Capítulos
2017	BCI	Melhores práticas - 10 Capítulos
2006	BS 25999:1	Desenvolvido a partir das melhores práticas do mercado (DRII e BCI.
2007/ 2008	NBR 15999	A NBR parte 1 estabelece o processo, os princípios e a terminologia da gestão da continuidade de negócios; A NBR parte 2 especifica os requisitos para planejar, estabelecer, exercitar, manter e melhorar o SGCN dentro do contexto dos riscos de negócios de toda a Organização.
2009	NC nº 06/IN01/DSIC /GSIPR	Estabelece diretrizes básicas para GCN.
2008	BS 25777	Ajuda a definir um modelo de governança mais efetivo, integrando a Continuidade dos serviços de TIC com a GCN corporativa.
2008	ISO/IEC 24762	Apresenta os requisitos para a implementação, operação, monitoramento e manutenção de estratégias de Recuperação de Desastre para os serviços e *sites* de TIC.
2005	ISO/IEC 27001	Visa estabelecer um referencial para as organizações desenvolverem, implementarem e avaliarem a gestão de segurança da informação.
2006	High-level principles for business continuity	Busca apoiar as organizações e as autoridades financeiras nos esforços para melhorar a resiliência dos sistemas financeiros a interrupções significativas.
2003	Acordo de Basileia II	Trata da gestão de riscos22 em instituições financeiras. Deve demonstrar práticas eficazes de gerenciamento e supervisão de tais riscos. Em 2003, em seu princípio nº 7: “Bancos deverão ter planos de contingência e de continuidade dos negócios para assegurar sua capacidade de operar de maneira contínua e com perdas limitadas na eventualidade de interrupção significativa nas suas operações de negócio.”
2002	Lei Sarbanes-Oxley	Aumenta as responsabilidades dos presidentes e diretores e as exigências dirigidas a auditorias e advogados responsáveis pela fiscalização dos relatórios contábeis das organizações.
2006	Resolução nº 3380	A estrutura de risco operacional deve prever a “existência de plano de contingência contendo as estratégias a serem adotadas para assegurar condições de continuidade das atividades e para limitar graves perdas decorrentes de risco operacional.”
2013	ABNT NBR ISO/IEC 22301:2013	Especifica requisitos para estabelecer e gerenciar um eficaz SGCN

Fonte: Guindani (2011) - adaptado pelo autor

22 **Gestão de risco**: atividades coordenadas para dirigir e controlar uma Organização no que se refere a riscos.
Fonte: ABNT ISO Guia 73

2.4. Esquema geral da dissertação

Este trabalho foi estruturado de maneira a apresentar o problema de pesquisa, o levantamento bibliográfico, a exploração de método e tipo de pesquisa e a análise e detalhamento dos resultados alcançados. O Quadro 3, a seguir, detalha as etapas que compõem este trabalho.

Quadro 3 - Estrutura da Dissertação

ESTRUTURA DO TRABALHO			
PARTE 1 – FUNDAMENTAÇÕES			
FASE TEÓRICA	INTRODUÇÃO	Contextualização	**CAP. 1**
		Problema de investigação	
		Objetivos	
		Delimitação do Escopo	
		Justificativa	
	REFERENCIAL TEÓRICO	Gestão de Continuidade de Negócios	**CAP. 2**
		Benefícios	
		Regulamentação	
		Esquema Geral da Dissertação	
	MÉTODO DE PESQUISA	Caracterização da Pesquisa	**CAP. 3**
		Matriz de Amarração	
		Delineamento das etapas da pesquisa	
		Dados da pesquisa	
		Instrumentos de pesquisa e procedimentos de análise de dados	
PARTE 2 – RESULTADOS			
FASE ANALÍTICA	DESCRIÇÃO DOS RESULTADOS	Descrição da coleta de dados Delineamento do foco da coleta de dados: resgatando a questão de pesquisa Aspectos Descritivos dos Atores e Organizações Perfil amostra - Entrevistas	**CAP. 4**
	ANÁLISE DOS RESULTADOS E CONSIDERAÇÕES FINAIS	Limitações da pesquisa e sugestões para estudos futuros	**CAP. 5**
		Principais resultados encontrados na pesquisa de campo	
		Considerações finais	
	REFERÊNCIAS		
	APENDICE		

Fonte: elaborado pelo autor (2021)

3. MÉTODO DA PESQUISA

Este capítulo descreve os procedimentos que foram adotados na fase empírica do estudo e como foram estruturados o trabalho e o foco empírico, após pesquisa pertinente da teoria.

3.1. Caracterização da pesquisa

A técnica de coleta de dados empíricos na pesquisa qualitativa é discutida por vários autores, entre os quais Haguette (1995), Minayo (1994), Triviños (1987), Lüdke e André (1986). Como forma de captar a realidade empírica, a qualitativa é considerada por Goode e Hatt (1979) como a mais antiga e, ao mesmo tempo, a mais moderna das técnicas de pesquisa. Para que se torne válida e fidedigna, requer planejamento com relação ao que observar e como observar.

A entrevista é um processo de interação social, no qual o entrevistador tem a finalidade de obter informações do entrevistado, por meio de um roteiro contendo tópicos em torno de uma problemática central (HAGUETTE, 1995).

Para Minayo (1994), a entrevista privilegia a obtenção de informações, por meio da fala individual, a qual revela condições estruturais, sistemas de valores, normas e símbolos e transmite, com um porta-voz, representações de determinados grupos.

Optou-se, nesta pesquisa, pela entrevista semiestruturada, na qual o entrevistado tem a possibilidade de discorrer sobre suas experiências, a partir do foco principal proposto pelo pesquisador. Ao mesmo tempo, a técnica permite respostas livres e espontâneas do entrevistado, além de valorizar a atuação do entrevistador. As questões elaboradas para a entrevista levaram em conta o embasamento teórico da investigação e as informações que o pesquisador recolheu sobre o fenômeno social (TRIVIÑOS, 1987).

Essa técnica possibilita conhecer a perspectiva dos agentes quanto ao trabalho realizado. As entrevistas traduzem a representação dos agentes sobre o seu trabalho e, dessa forma, constituem-se sempre em uma aproximação do concreto vivido. Considerando que não é possível reduzir a realidade à concepção dos homens, a

entrevista foi utilizada para complementar e fazer o contraponto com os dados obtidos por meio da observação.

3.1.1 Vantagens da entrevista semiestruturada

As vantagens da entrevista semiestruturada são: flexibilidade e a chance de rápida adaptação. Esse tipo de entrevista pode ser ajustado tanto ao entrevistado quanto às circunstâncias. Ao mesmo tempo, um pequeno roteiro de perguntas contribui para a reunião das informações apuradas. São ainda vantagens da entrevista semiestruturada:

a) mais direcionamento para o tema da entrevista;
b) possibilidade de testar a capacidade de o entrevistado se ajustar a novas situações, ao levantar questões inesperadas;
c) oportunidades de conhecer os entrevistados, já que, enquanto em uma entrevista totalmente guiada por roteiros, torna-se mais difícil obter respostas muito diferentes. Na entrevista semiestruturada, você pode saber a percepção real do entrevistado e, assim, obter uma boa amostra de candidatos;
d) favorecimento de respostas espontâneas.

3.1.2 Desvantagens da entrevista semiestruturada

Algumas desvantagens da entrevista semiestruturada são:

a) requer grande habilidade do entrevistador para a sua condução;
b) exige a demonstração de confiança e o emprego de grande experiência, por parte do entrevistador, para o atingimento dos objetivos.

A credibilidade das pesquisas qualitativas tem aumentado, e se torna legítima por incorporar alguns critérios positivos que validam e generalizam o estudo (RICHARDSON et al., 1999).

Entrevistas qualitativas, de forma semiestruturada, foram realizadas como parte do trabalho de campo deste trabalho, compondo o método de pesquisa através de entrevistas, com uma investigação empírica que aborda profundamente um evento em sua realidade, para se explicar “como” e “por que” quanto à realidade estudada

(SEVERINO, 2007; YIN, 2015). As entrevistas foram roteirizadas para uma maior interação, utilizando entrevistas nas quais as perguntas foram listadas. Como parte da composição de uma entrevista qualitativa, mesmo com as perguntas listadas, a relação entre o pesquisador e o entrevistado não seguiu um aspecto rígido para a investigação dos contextos pesquisados.

Nas etapas iniciais desta pesquisa, o pesquisador recorre à formulação de hipóteses, baseando-se na revisão da literatura existente sobre o assunto a ser investigado. Dessa forma, os questionamentos são vistos e reformulados, ajustando-se os referenciais e constructos analisados ao que se visa obter com os dados da parte empírica da pesquisa (BARDIN, 1977; OLIVEIRA, 2008).

Na etapa de entrevistas, deve-se considerar que a abordagem qualitativa é usada como um relacionamento social e embasa a análise e interpretação dos resultados que serão obtidos (OLIVEIRA, 2008).

A análise de conteúdo é uma possibilidade de investigação de pesquisa nas ciências sociais aplicadas e designa a verificação23 dos conteúdos obtidos durante os processos de coleta de dados. Este tipo de análise traz a descrição desses dados, que podem ser conseguidos por meio de falas, documentos e textos (COOPER; SCHINDLER, 2016; OLIVEIRA, 2008).

A análise de conteúdo, com abordagem qualitativa tem suas origens marcadas nas ciências sociais e nas literaturas de críticas acadêmicas. Suas características principais estão relacionadas à: i) necessidade de uma leitura mais próxima e aprofundada de uma relativa porção de referencial teórico, que trará os construtos específicos da pesquisa pretendida; ii) reinterpretação de textos já consolidados, com novas perspectivas ou aplicações a novas realidades; e iii) sua natureza interativo-hermenêutica, visto que circula em seu próprio espaço e considera seus próprios entendimentos social e culturalmente autocentrados. Sobre essa última característica, pode-se dizer que a análise de conteúdo é de natureza hermenêutica e de interação, na qual o pesquisador interpreta os dados dentro de um contexto condicionado, porém

23 **Verificação**: confirmação, por meio de evidência, que os requisitos especificados foram cumpridos.
Fonte: ABNT NBR ISO/IEC 22301:2013

com vistas a realizar descobertas amplas ou específicas de um universo (KRIPPENDORF, 2004).

A análise de conteúdo é uma metodologia de tratamento e segue com a análise de informações, que pode ser aplicada a qualquer tipo de comunicação que deverá ser decifrada por meio de técnicas, de modo a se constituírem padrões, tendências ou relações, além das descritas e explicitadas nos documentos.

Para Bardin (1977), as categorias definidas e pré-verificadas na literatura são escoradas em um quadro teórico relevante, mas também podem ser direcionadas, em sua construção, por uma interpretação criteriosa dos dados obtidos. Assim, realizada a etapa de coleta dos dados, verifica-se sua adequação em relação às interpretações e análises. Observam-se, nesse momento, algumas inferências que não estavam preditas quando da etapa inicial, sendo que a interpretação criteriosa proporcionará novos apontamentos e, provavelmente, um aprofundamento posterior tanto do referencial teórico como das próprias análise e metodologia. É importante observar novas possibilidades e realizar mais leituras e interpretações, nessa fase da pesquisa, sendo que se deve procurar estabelecer uma validação dos resultados, o que contribui para a caracterização da relevância da pesquisa.

Para fornecer um modelo de visualização mais sintetizado da pesquisa, indicando com mais precisão as conexões entre as dimensões da pesquisa, uma matriz de amarração foi determinada, para apresentar os vínculos entre referencial teórico, objetivos, hipóteses de pesquisa e técnicas de análise dados. Esse conceito subsidia o exame da qualidade metodológica da pesquisa. Para melhor visualização da estruturação desta dissertação, o Quadro 4 e o Quadro 5 apresentam uma síntese deste trabalho.

3.2. Matriz de Amarração

Quadro 4 – Matriz de Amarração

COMPONENTES		DESCRIÇÃO E ORIENTAÇÕES METODOLÓGICOS		
INTRODUÇÃO		O todo sem a parte não é todo, A parte sem o todo não é parte, Mas se a parte o faz todo, sendo parte, Não se diga, que é parte sendo todo.		
Fonte: Gregório de Matos				
Questão de Pesquisa:		**Gestão de Continuidade de Negócios – sua Organização "aceita" falar sobre este assunto?** **Proposta para uma ferramenta para autodiagnóstico organizacional.**		
Metodologia:		➢ **Qualitativo semiestruturado:** Entrevistas com 5 executivos que atuam na área (setor bancário) – com 5 perguntas.		
		Método de Pesquisa: Entrevistas	**Instrumento de Pesquisa:** Questionário	**Método de Coleta:** Aplicação de Entrevista
Objetivos	**Primário:**	**Manter** a Organização ativa (operacional) mesmo que em momentos de crises.		
	Secundário:	• **Compreender** se quanto mais a alta administração[24], estiver engajada melhor será a qualidade dos resultados / planejamento da crise; • **Verificar** se o Planejamento de Crise pode ser executado por meio de: coordenação de parcerias, longevidade, compreensão; • **Identificar** se Planejamento da Crise depende da qualidade de recurso: pessoas, TI, negócio;		
	Final:	**Responder as proposições de pesquisa.**		
	Geral:	**Manter a Organização operacional.**		
Fonte: Elaborado pelo autor.				

24 **Alta Direção:** pessoa ou grupo de pessoas que dirige e controla uma organização em nível mail alto.
Nota 1: A alta direção tem o poder de delegar autoridade e fornecer recursos dentro da organização;
Nota 2: Se o escopo do sistema de gestão abrange apenas parte de uma organização, então Alta Direção refere-se àqueles que dirigem e controlam parte da organização.
Fonte: ABNT NBR ISO/IEC 22301:2013

PROPOSIÇÃO	CONSTRUCTOS/VARIÁVEL	REFERÊNCIAS
P1. Quanto mais a alta administração estiver engajada, melhor será a qualidade dos resultados / planejamento da crise.	Proatividade; aprendizado; boa gestão humana;	ABNT NBR ISO 22301:2013 Segurança e resiliência — Sistema de GCN — Requisitos;
	Qualidade dos testes; qualidade da equipe de testes; Simulações realizadas;	**Artigo:** GCN de pequenas e médias empresas: Provas da Tailândia. Mio Kato, Teerawat Charoenrat;
	Liderança em momentos de Crise, Planejamento de Crises;	
P2. Planejamento de Crise pode ser executado por meio de: Coordenação de parcerias, longevidade, Compreensão.	Coordenação de parcerias, longevidade, Compreensão;	BS 11200:2014 Crisis management. Guidance and good practice;
	Cooperação;	**Artigo:** Estudo de Impacto da Governança de TI no desempenho das Empresas Brasileiras: uma Análise a partir da Perspectiva dos executivos, usuários e membros de equipes de TI; Rogério F. da Costa e Alessandro M. Rosini – Future Journal.
P3. Planejamento da crise depende da qualidade de recursos: Pessoas, TI, Negócio.	Redução de recursos, TI, Negócios, Pessoas;	ISO/IEC 27000:2018 Segurança da Informação
	Redução de recursos, TI, Negócios, Pessoas;	**Artigo:** GCN: hora de um papel estratégico? Brahim Herbane, Dominic Elliott e Ethne' M. Swartz;

Fonte: elaborado pelo Autor

Constructos	Liderança em momentos de crise;
	Planejamento da Crise;
	Coordenação de parcerias, Longevidade, Compreensão;
	Pessoas, TI e Negócios;

Definições	**Liderança:**	Para simbolizar a importância atribuída ao GCN pela alta administração;
	Coordenação de parcerias:	Para refletir a natureza complexa e acoplada das cadeias de abastecimento das Organizações;
	Longevidade:	Para evitar que a continuidade dos negócios seja considerada um projeto temporário;
	Propriedade:	Para gerar compromisso e responsabilidade com o processo;
	Compreensão:	Para facilitar uma maior compreensão das implicações estratégicas de uma crise empresarial;
	Infraestrutura de Gerenciamento:	Para gerar links e apoiar o trabalho comunicativo entre o GCN e as equipes funcionais de gerenciamento.

Fonte: Gestão de Continuidade de Negócios: hora de um papel estratégico? Brahim Herbane, Dominic Elliot and Ethne M. Swartz	
Relevância	Provê uma caracterização sobre ameaças, riscos e de vulnerabilidades da indústria financeira brasileira, que é de suma importância para toda a sociedade no país. A pesquisa pode ser usada como base para a aplicabilidade de análise dos controles na gestão de crise e continuidade de negócio, não só da indústria financeira, mas também para qualquer indústria que tenha missão crítica em suas operações e busque mitigar potenciais riscos inerentes25 as suas operações.
Justificativa	Executar a análise da gestão de continuidade e capacidade de resposta em tempo adequado a eventos de alto impacto em instituições financeiras, reduzindo perdas potenciais em suas operações, sem que isso traga risco de liquidação financeira, ou de imagem para estas organizações, ou até mesmo um problema sistêmico, mantendo um sistema financeiro resiliente e saudável para atender a sociedade brasileira, assegurando a estabilidade das transações bancárias no Brasil.
Objeto de pesquisa	Refere-se à gestão de continuidade de negócios das organizações da indústria financeira brasileira, conectando a utilização de controles e governança. Desta forma, prioriza-se a identificação de processos considerados críticos ao negócio, identificando-se ameaças significativas e planejando uma estratégia coordenada de resposta a um alto impacto operacional, assegurando uma efetiva e eficiente resposta durante um evento de crise, garantindo a sobrevivência (longevidade. da organização e o atendimento aos seus compromissos junto a clientes, reguladores e investidores.
Problematização da pesquisa	As organizações que compõem a indústria financeira brasileira atuam com a gestão de continuidade de negócios e se preparam para responder a incidentes e eventos de alto impacto operacional quanto aos requisitos específicos da ABNT NBR ISO/IEC 22301.
Contribuição social da pesquisa	Se dá pela execução da análise de como a indústria financeira no Brasil atua na gestão da continuidade de seus negócios e na sua capacidade de resposta em tempo adequado a eventos de alto impacto operacional. Assim, consegue-se mitigar perdas potenciais em suas operações, sem que isso traga risco de liquidação financeira, ou de imagem para estas organizações, ou até mesmo um problema sistêmico mantendo um sistema financeiro resiliente e saudável para atender a sociedade brasileira, assegurando a estabilidade das transações bancárias no Brasil.
Contribuição acadêmica da pesquisa	Por se tratar de um trabalho que envolve segurança da sociedade e descrição da abrangência da fundamentação teórica de Gestão de Continuidade de Negócios, que é composta por disciplinas como Segurança da Informação, Tecnologia da Informação, Governança Corporativa e Risco Operacional Corporativo, a proposta da pesquisa pode ser uma referência para outros estudos relacionados ao tema.
Fonte: Elaborado pelo Autor	

25 **Risco Inerente:** representa a quantidade de risco que existe com os controles existentes no momento da identificação dos riscos.
Risco residual: é a quantidade de risco que permanece ou que aparece após a inclusão dos controles adicionais e/ou ajustes dos controles existentes.

3.3. Delimitação e amostra da pesquisa

A delimitação deste pesquisa considerou, como parte do que se deve observar, unidades para análise e coleta de dados, a relação de instituições financeiras informadas no *site* do Banco Central do Brasil, que somam 600 (seiscentas) instituições financeiras brasileiras, as quais encontram-se divididas em: i) conglomerados; ii) bancos comerciais, múltiplos e caixa econômica; iii) cooperativas de crédito; iv) bancos de investimento, bancos de desenvolvimento, sociedades corretoras de TVM - Títulos de Valores Monetários, sociedades distribuidoras de, TVM, sociedades de crédito, financiamento e investimento, sociedades de crédito imobiliário e APE, sociedades de arrendamento mercantil, sociedades de investimento, sociedades de crédito ao microempreendedor, agências de fomento, Companhias Hipotecárias e Instituições de Pagamento; v) Administradoras de consórcios.

Há, nessa relação, 155 instituições financeiras do tipo bancos comerciais, múltiplos e Caixa Econômica no Brasil.

Para melhor compreensão da capacidade de resposta aos eventos, buscou-se a avaliação dos modelos de plano de crises, quanto à sua comprovação e validação. Segundo Yin (2006), a escolha de um determinado projeto de caso único ou múltiplo depende diretamente da organização do plano de pesquisa com o qual o pesquisador busca obter respostas. Neste caso, a pesquisa visa identificar se as organizações possuem um Plano de Crises, dentro de um diagnóstico de contexto da análise desta disciplina. Assim, busca-se estabelecer um comparativo quanto à existência de um Plano de Crise nas organizações da indústria financeira, que utilize como melhores práticas aspectos da norma ABNT NBR ISO/IEC 22301, na qual se verifica se há aderência em partes deste *framework*. Esta pesquisa utiliza múltiplos casos, incluindo organizações nacionais e multinacionais, indicadas para representar o fenômeno no universo das instituições financeiras no Brasil.

Segundo Gil (1991), a opção pela pesquisa se dá pela necessidade da exploração mais profunda dos objetos a serem pesquisados, de maneira que possibilitem um amplo e mais detalhado conhecimento. Isto dará a oportunidade para que os aspectos do problema de pesquisa sejam estudados em maior profundidade dentro de um período limitado (VENTURA, 2007). Além disso, esse método parece ser apropriado

para investigação do Plano de Crise, tema complexo, em que existe uma grande variedade de fatores e relacionamentos. Estes podem ser diretamente observados, sendo que não existem leis básicas para determinar quais são os de maior relevância, pois as instituições atuam em diferentes formas com diferentes apetites ao risco.26

Dessa forma, para a realização desta pesquisa, serão abordadas 05 organizações (bancos, Quadro 5) de perfis e portes diferentes, com operações distintas, mas que seguem as regulamentações estabelecidas pelo regulador principal. A diversificação das unidades-caso a serem pesquisadas foi considerada como fator fundamental para a ampliação da visão do tratamento do risco.

26 **Apetite ao risco é** a quantidade de risco que a organização deseja assumir para conseguir atingir seus objetivos. Ou pode-se dizer também que apetite a risco é a quantidade de riscos, no sentido mais amplo, que uma organização está disposta a aceitar em sua busca para agregar valor. O apetite a risco reflete toda a filosofia administrativa de uma organização e, por sua vez, influencia a cultura e o estilo operacional desta.
A fixação do apetite ao risco permite determinar na organização o binômio risco x benefício, controlar e manter os riscos em níveis desejados. Para tanto, para possibilitar a concretização de geração de valor nas organizações, estas devem fazer um balanço entre riscos x oportunidades x apetite ao risco, e, servir de guia para a tomada de decisões, alocação de recursos e a definição do alinhamento de toda organização para a busca dos objetivos fixados, permitindo fazer um monitoramento das ações, resultados e dos níveis de riscos associados.
Fonte: ABNT NBR ISO/IEC 31000, COSO I e II
Prof. Dr. Antonio Celso Ribeiro Brasiliano, CRMA, CES, DEA, DSE, MBS. *D*outor em Science et Ingénierie de L'Information et de L'Intelligence Stratégique, pela Université East Paris - Marne La Vallée – Paris – França, é presidente da Brasiliano INTERISK – Gestão de Riscos Corporativos. CEO da Brasiliano INTERISK Gestão de Riscos Corporativos.

Quadro 5 – Resumo das características das organizações entrevistadas

Organização	Organização_1	Organização_2	Organização_3	Organização_4	Organização_5
Gênero	Financeiro	Financeiro	Financeiro	Financeiro	Financeiro
Sustentabilidade	sim	sim	sim	sim	Sim
PCN	sim	sim	sim	sim	sim
Capital	Fechado	Fechado	Aberto	Aberto	Organizado sob a forma de sociedade de economia mista, de capital aberto, cujo acionista majoritário detém (80,33%)
Funcionários	84.952 (2019)	219.000 (2020)	3564	89.575 (2020)	3280
Lucro Líquido (2019 - bilhões)	R$ 21,1	R$1,5	R$ 2,7	R$ 25,887	R$ 0,4123

Fonte: Elaborado pelo autor.

3.4. Dados da pesquisa

O objeto desta pesquisa é a continuidade de negócios em organizações da indústria financeiras, que possuem governança corporativa. Depois de aprofundada pesquisa sobre os constructos e temas pertinentes, foi estabelecida a pergunta: **Gestão de Continuidade de Negócios – sua organização "aceita" falar sobre este assunto? Proposta para uma ferramenta para autodiagnóstico organizacional.**

A coleta de dados, do tipo entrevista aberta, será realizada junto à amostra e considerará o envolvimento e análise de documentos, políticas, evidência de processos de validação de testes de contingência, planos, dados primários e secundários.
O roteiro de entrevistas categorizado pode ser visualizado no Quadro 6, a seguir, e o protocolo das entrevistas está apresentado no Apêndice.

Quadro 6 – Categorização - Roteiro de Entrevista – Parte 1

Roteiro de Entrevista
01. A Organização considera GCN como um ponto importante para alcançar seus objetivos de negócio? Como GCN se encaixa na estratégia de negócios? Qual é a importância estratégica do GCN para sua organização? Quais foram e tem sido os principais “marcos” da GCN na sua organização? Quais as principais conquistas e desafios?
02. A organização possui uma equipe ou comitê de mudança que garanta que todas as atualizações feitas no ambiente de produção também sejam realizadas no site alternativo? Explique como se dá? A organização possui a revisão e a coleta dos resultados dos testes e prática de lições aprendidas? Como ocorrem essas análises?
03. A organização possui um processo de monitoração e manutenção da GCN?
04. A organização possui um mapeamento da sua cadeia de principais fornecedores? Esses fornecedores possuem classificação de "criticidade"? Os fornecedores críticos participam dos seus testes de continuidade de negócios? Descreva como isso ocorre.
05. A sua Organização monitora *stakeholders* que podem influenciar GCN? Como ocorre esse monitoramento? Quais são os principais *stakeholders*?

Fonte: Criado pelo Autor

Quadro 7 – Categorização - Roteiro de Entrevista – Parte 2

Roteiro Entrevista	Método Pesquisa: Coleta:	GCN – ISO 22301	Objetivo Específico	Proposição Constructo	Autores / Normas
01. A Organização considera GCN como um ponto importante para alcançar seus objetivos de negócio? Como GCN se encaixa na estratégia de negócios? Qual é a importância estratégica do GCN para sua Organização? Quais foram e tem sido os principais "marcos" da GCN na sua Organização? Quais as principais conquistas e desafios?	Entrevistas; Entrevistas; **Instrumento:** Questionário	Entendendo a organização e seu contexto; Liderança e comprometimento; **PDCA: PLAN, DO,** Planejamento e Suporte; Operação; Melhoria	**a.** Qual a importância das estratégias de GCN para a corporação. **b.** Identificar as organizações que possuem GCN com regulatórios e ISO's. **c.** Maturidade corporativa	**P1** Liderança, Longevidade	Guindani (2011); ABNT NBR ISO 22301:2013 - Segurança e resiliência — Sistema de GCN — Requisitos; **Artigo:** GCN de pequenas e médias empresas: Provas da Tailândia. Mio Kato, Teerawat Charoenrat;
02 A Organização possui uma equipe ou comitê de mudança que garanta que todas as atualizações feitas no ambiente de produção também sejam realizadas no site alternativo? Explique como se dá? A Organização possui a revisão e a coleta dos resultados dos testes e	Entrevistas; Entrevistas; **Instrumento:** Questionário	**PDCA: PLAN** Planejamento e Suporte; Operação; Melhoria	**a.** Qual a importância das estratégias de GCN para a corporação. **b.** Identificar as organizações que possuem GCN com regulatórios e ISO's. **c.** Maturidade corporativa	**P1,** Liderança, Longevidade **P2** Coordenação de parceiras, Longevidade, compreensão	Guindani (2011); ABNT NBR ISO 22301:2013 - Segurança e resiliência — Sistema de GCN — Requisitos; BS 11200:2014 Crisis management. Guidance and good practice. **Artigo:** Estudo de Impacto da Governança de TI no desempenho das Empresas Brasileiras: uma Análise a partir da Perspectiva dos executivos, usuários e membros de

prática de *lições aprendidas*? Como ocorrem essas análises?					equipes de TI; - Rogerio F. da Costa e Alessandro M. Rossini – Future Journal
03. A Organização possui um processo de monitoração e manutenção da GCN?	Entrevistas; Entrevistas; **Instrumento:** Questionário	**PDCA: CHECK** Avaliação de Desempenho; Monitoramento, medição, análise e avaliação;	**a.** Qual a importância das estratégias de GCN para a corporação. **b.** Identificar as organizações que possuem GCN com regulatórios e ISO's. **c.** Maturidade corporativa	**P3** TI, Negócios, Pessoas	Guindani (2011); ISO/IEC 27000:2018 Segurança da Informação; **Artigo:** GCN: hora de um papel estratégico? Brahim Herbane, Dominic Elliott e Ethne' M. Swartz;
04. A organização possui um mapeamento da sua cadeia de principais fornecedores? Esses fornecedores possuem classificação de "criticidade"? Os fornecedores críticos participam dos seus testes de continuidade de negócios? Descreva como isso ocorre	Entrevistas; Entrevistas; **Instrumento:** Questionário	**PDCA: PLAN, DO, CHECK, ACT** Avaliação de Desempenho; Monitoramento, medição, análise e avaliação; Operação; Melhoria.	**a.** Qual a importância das estratégias de GCN para a corporação. **b.** Identificar as organizações que possuem GCN com regulatórios e ISO's. **c.** Maturidade corporativa	**P2** Coordenação de parceiras, Longevidade, compreensão	Guindani (2011); ABNT NBR ISO 22301:2013 - Segurança e resiliência — Sistema de GCN — Requisitos; BS 11200:2014 Crisis management. Guidance and good practice. **Artigo:** Estudo de Impacto da Governança de TI no desempenho das Empresas Brasileiras: uma Análise a partir da Perspectiva dos executivos, usuários e membros de equipes de TI;
05. A sua Organização monitora *stakeholders* que podem influenciar GCN?	Entrevistas; Entrevistas;	**PDCA: PLAN, DO, CHECK, ACT** Avaliação de Desempenho; Monitoramento, medição, análise e avaliação;	**a.** Qual a importância das estratégias de GCN para a corporação. **b.** Identificar as organizações que possuem GCN com regulatórios e ISO's.	**P3** TI, Negócios, Pessoas	Guindani (2011); ISO/IEC 27000:2018 Segurança da Informação;

Como ocorre esse monitoramento?	**Instrumento:** Questionário	Operação; Melhoria.	**c.** Maturidade corporativa		**Artigo:** GCN: hora de um papel estratégico? Brahim Herbane, Dominic Elliott e Ethne' M. Swartz;

Fonte: Elaborado pelo autor.

3.5. Instrumentos de pesquisa e procedimentos de análise de dados

Para manter o equilíbrio entre os métodos da entrevista, no que tange às vantagens e desvantagens entre os referidos métodos, optou-se pelo modelo híbrido.
A entrevista aplicada foi composta por cinco perguntas abrangentes, que envolvem todos os tópicos da ISO 22301:2013. Seu tempo médio de respostas é de uma hora aproximadamente. A entrevista foi preparada previamente e por meio de e-mail encaminhado aos gestores respondentes, ao passo que a entrevista foi encaminhada por solicitação com *invite* via aplicativo Teams da Microsoft, cujo aceite do gestor respondente consolida a solicitação de entrevista. As entrevistas ocorreram dentro do prazo estipulado.

Inicialmente, foram realizadas perguntas para caracterização do profissional entrevistado, para posteriores análises dos resultados, tais como:

a) Formação Acadêmica;
b) Possui certificações na área de Gestão de Continuidade de Negócios;
c) Cargo que ocupa atualmente na organização;
d) Há quanto tempo ocupa o cargo;
e) Principais atividades que exerce;
f) Possui alguma experiência em Segurança da Informação, Gestão de Risco Operacional ou Governança Corporativa.

4. DESCRIÇÃO DOS RESULTADOS

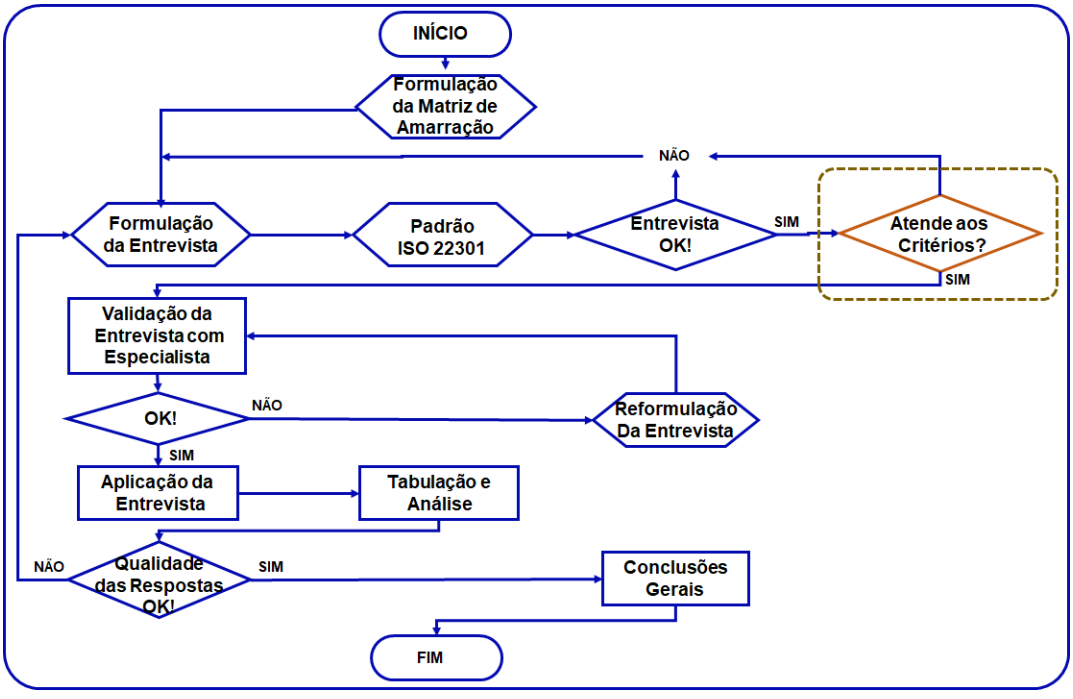
As organizações do sistema financeiro brasileiro estão sendo, cada vez mais, pressionadas. De um lado, o BACEN exige dos acionistas, investidores e executivos a implementação dos marcos regulatórios e, por outro lado, os reguladores internacionais, representados pelas ISO's, exigem a adoção das melhores práticas. Como consequência disso, temos o aumento da eficiência e eficácia operacional das companhias que, desse modo, tornam-se, cada vez mais, dependentes da tecnologia da informação.

A dependência da eficácia da tecnologia das organizações volta-se aos seus ambientes operacionais e suas plataformas tecnológicas, que precisam sempre estar disponíveis, pois o risco operacional decorrente de uma suposta indisponibilidade potencializa perdas significativas, inclusive financeiras, devido à interrupção de serviços ou à ineficiência ou ineficácia das operações.

4.1. Descrição da coleta de dados

Através da figura a seguir o autor demonstra como foi o processo decisório praticado para realização/elaboração das perguntas que foram incluídas no programa.

Figura 11 – Processo de elaboração e coleta de dados.



Fonte: Camila Silvestre de Melo (2018), adaptado pelo Autor

Em primeira análise não havia necessidade de se questionar sobre critérios, e assim foi feito, foi elaborado uma entrevista com 15 perguntas, conforme descritas a seguir:

Quadro 8 – Roteiro de entrevista – Inicial

Gestão de Continuidade de Negócios – Roteiro de entrevistas
01. A Organização possui uma **Área específica** de Gestão de Continuidade de Negócios?
Se afirmativo. Com qual Diretoria está a responsabilidade de GCN?
Por quê?
Explique o ponto.
02. A Organização considera GCN como um ponto importante para alcançar seus objetivos de negócio?
Como GCN se encaixa na estratégia de negócios da empresa?
03. A Organização possui **políticas(s) específicas** para o cumprimento de ações relacionadas a gestão de continuidade de negócios? Sim ou Não?
Todas as Áreas de Negócios foram contempladas nesta política?
04. A Organização possui um **centro de processamento de dados de produção** ou principal e um centro de processamento secundário ou alternativo para acionamento em caso de um impacto operacional em suas operações? Sim ou não?
Explique como se dá o acionamento de contingência para o *site* alternativo.
05. Em caso afirmativo, a Organização possui uma equipe ou comitê de mudança (Change Management) que garanta que todas as atualizações feitas no ambiente de produção também sejam realizadas no centro de processamento secundário ou alternativo? Sim ou não?
Explique como se dá?
06. A Organização possui **duplicação de abordagem de link** de telecomunicação de dados entre seus principais sites de negócio?
Em caso afirmativo, essa duplicidade de conectividade de links de dados ocorre com operadoras de telecomunicações diferentes ou não?
07. A Organização possui um processo de monitoração e manutenção dos planos de continuidade de negócios *(Plan – Do – Check - Act)*? Sim ou não?
08. GCN é valorizado ou mesmo exigido pelo mercado/acionistas/Bolsa?
O que a Organização tem feito nesse sentido?
As iniciativas de GCN são comunicadas ao mercado e aos investidores?
Qual o retorno disso?

09. A Organização considera GCN como um ponto importante para alcançar seus objetivos de negócio?
Como GCN se encaixa na estratégia de negócios da empresa?
10. A Organização possui um mapeamento da sua cadeia de principais fornecedores?
Esses fornecedores possuem classificação de criticidade?
Os fornecedores críticos participam de testes de continuidade de negócios? Sim ou não?
Descreva como isso ocorre.
11. A Organização possui a revisão e a coleta dos resultados dos testes e a criação de planos de ação para corrigir os problemas ocorridos durante as manobras de recuperação (Lições Aprendidas)? Sim ou não?
Como ocorrem essas análises?
12. GCN faz parte do treinamento de todos os colaboradores da empresa?
Por quê?
De que forma?
Foi possível medir algum resultado? Quais?
13. A Organização possui um mapeamento de conexão de entidades externas (B2B), (B2C)?
Essas entidades externas (B2B), (B2C) possuem classificação de criticidade?
As entidades externas participam de testes de continuidade de negócios? Sim ou não?
Como isso ocorre?
14. É feito algum tipo de mensuração sobre a adoção de GCN? Quais?
Que nova iniciativa surgiu após análise dos dados?
15. GCN é valorizado ou mesmo exigido pelo mercado/acionistas/Bolsa?
O que a Organização tem feito neste sentido?
As iniciativas de GCN são comunicadas ao mercado e aos investidores?
Qual o retorno disto?

Porém, ao sair a campo, aplicou-se a entrevista para o ATOR_1, ficou evidenciado que o tempo de entrevista estava muito acima do esperado, isto é, aproximadamente 2h30 (duas horas e meia) quando a expectativa era de 1h00 (uma hora). De posse desta informação foi realizado uma análise em nosso questionário de entrevista, onde se verificou que a quantidade que perguntas era muito grande, 15 (quinze) até aquele momento. Assim optou-se pela redução da quantidade de perguntas com o compromisso de não perder a essência e sequência lógica, cujo foco principal estava na de redução do tempo.

Com isto efetuou-se uma melhoria no fluxo representado pela figura 11, onde foi acrescentado a questão: “Atende aos Critérios” destacado por linhas pontilhadas.

Após os ajustes, a entrevista passou a ter 5 (cinco) perguntas principais, ao invés de 15 (quinze) e, cada uma contendo perguntas secundárias que dariam suporte para o questionamento principal, ficando assim, conforme Quadro 6 – Categorização - Roteiro de Entrevista – Parte 1.

Com este novo formato de entrevista, reaplicamos a entrevista com o ATOR_1 onde se constatou o atingimento que foi previamente estabelecido, isto é, entrevista de aproximadamente 1h00 (uma hora).

Vale a pena lembrar que a entrevista que durou 2h30 (duas horas e meia) não foi descartada, isto é, foi mantida como parte integrante da pesquisa.

4.2. Delineamento do foco da coleta de dados: resgatando a questão de pesquisa

A criação de uma área de GCN efetiva permite o aumento no nível de resiliência das organizações, indicando métodos, métricas, planos de simulação e testes, criação de estratégias, além de ferramentas e equipes altamente preparadas e treinadas para ações em momentos de crise. Assim, esta pesquisa analisou a capacidade dessas organizações para responderem a eventos de crises, que variam desde pequenas paralisações, até uma total parada nas operações críticas, atendendo aos requisitos específicos da ABNT NBR ISO/IEC 22301, além da utilização das boas práticas

realizadas no mercado nacional. Por meio de uma pesquisa qualitativa semiestruturada, realizou-se a coleta de informações, fazendo-se uso de entrevistas, com uma amostra composta por cinco entrevistados, cada qual aqui chamado de ATOR, e de cinco organizações distintas do segmento financeiro e que possuem aplicação de *framework* de boas práticas de gestão de governança corporativa. Inicialmente, um pré-teste do instrumento de entrevista foi realizado, com uma organização que foi usada como parâmetro para este trabalho.

Ocorreu interação total entre entrevistados e entrevistador, contando-se com o fato de que a entrevista proporcionou ganho para ambos os lados. Uma exigência sistemática em ouvir e compreender o entrevistado foi observada, para que os temas pudessem ser concluídos. A abrangência e profundidade das perguntas e respostas foram adequadamente comportadas pelo instrumento de entrevista e permitiu a elaboração de um roteiro com observações focadas nos pontos relevantes. O entrelace de eventos relacionados aos aspectos de gestão de continuidade de negócios e as perguntas realizadas em campo foram bem-sucedidas. A entrevista com o ATOR_1 da organização_1 foi realizada em outubro de 2021, sendo que as demais entrevistas foram realizadas no período de outubro de 2021 até janeiro de 2022.

Por meio das entrevistas, buscou-se responder à seguinte questão de pesquisa: “Gestão de Continuidade de Negócios – sua Organização “aceita” falar sobre este assunto? Proposta para uma ferramenta para autodiagnóstico organizacional”. Assim, também se atenderam as proposições: **P1.** Quanto mais a alta administração estiver engajada melhor será a qualidade dos resultados / planejamento da crise; **P2.** Planejamento de Crise pode ser executado por meio de: coordenação de parcerias, longevidade, compreensão; **P3.** Planejamento da crise depende da qualidade de recursos: pessoas, TI, negócio.

Com a definição dos objetivos (primário, secundário, final e geral), descritos no Quadro 4 - Matriz de Amarração, foi possível estabelecer os procedimentos adequados para obtenção das informações desejadas, uma vez que a metodologia deve se adequar aos problemas de investigação e aos dados trabalhados (CARVALHO, 2014).

4.3. Aspectos Descritivos dos Atores e Organizações

O grau de maturidade e a resiliência expressados mediante a possibilidade de um evento causado por ameaças naturais, ambientais, biológicos, químicos, cibernéticos, erros humanos e incidentes, que possam impactar os principais *sites* de operações, foram determinantes para a análise das cinco organizações, todas atuantes na indústria financeira brasileira, que foram selecionadas para compor os parâmetros desta pesquisa. Para cada organização, no mínimo um *expert* foi entrevistado, sendo aqui chamado de “ATOR”.

Por outro lado, ao se realizar a entrevista com o ATOR_1, a pandemia do coronavírus - COVID-19, que modificou os hábitos ao redor do mundo, apresentava índices e indicadores baixos ou com perspectiva de queda. Porém, o mesmo não aconteceu até a conclusão da execução das entrevistas, pois, o surgimento da nova variante, Ômicron, do coronavírus (cepa B.1.1.529), confirmada em regiões da África, passou a preocupar especialistas internacionais de saúde. A variante Ômicron surgiu em meados de novembro de 2021 e, segundo a Organização Mundial da Saúde (OMS), pode se tornar responsável pela maior parte de novos registros de infecção pelo novo coronavírus.

Por causa da pandemia da COVID-19, não se considerou a possibilidade de encontros presenciais para a realização das entrevistas. A entrevista com o ATOR_1 se deu em ambiente virtual, por meio do aplicativo Microsoft Teams, e teve duração de, aproximadamente, duas horas, nas quais foram aplicadas 14 perguntas. Esta entrevista foi concedida diretamente pelo gestor da área de Continuidade de Negócios da organização.

4.3.1. Perfil dos especialistas

O tema gestão de continuidade de negócios na indústria financeira brasileira, ou mesmo a determinação de aplicação de controles relacionados ao tema por órgãos reguladores, no Brasil, apresenta uma série de determinações e normas para a aplicação em alto nível de boas práticas e especializações técnicas. Essas especificações relacionam-se aos aspectos específicos de análise de uma

estruturação para preparar, responder, recuperar, retornar e restaurar a continuidade operacional, crise ou desastres em operações. Apresentam uma série de determinações e normas para a aplicação em alto nível de boas práticas e especializações técnicas.

Entretanto, este não é um tema com grande abrangência acadêmica e, por este motivo, aspectos corporativos e de mercado contaram significativamente para definição da experiência de quem pode ser considerado um especialista, para atender à análise especializada sobre a investigação.

Para a fundamentação teórica, foram utilizados, como referências, autores de livros sobre a abordagem de tema para investigar as proposições. Além disso, foram usados artigos e, mais especificamente, ISO's, juntamente com a ABNT NBR ISO/IEC 22301.

A partir dessa prerrogativa, as escolhas dos profissionais para fazer parte da etapa de entrevistas de especialistas em Gestão de Continuidade de Negócios e Gestão de Crises foram efetuadas em primeira análise. Levou-se em consideração a disponibilidade de acesso a esse tipo de profissional, o nível de certificação nas entidades DRII e BCI, a experiência profissional em atuação em gestão no mercado para a indústria financeira brasileira e a participação em *workshops* e congressos relacionados aos temas supracitados. Os profissionais contatados possuem essas características e, por isso, a coleta dos seus depoimentos mostrou-se crucial para a investigação do tema e a devida fundamentação de uma conclusão.

Outro ponto importante a mencionar é que profissionais que são certificados por institutos, como o Disaster Recovery International Institute – DRII, passam por um rigoroso processo seletivo para a obtenção de qualquer nível de certificação na entidade. Estar certificado neste instituto significa que o profissional precisou demonstrar bom nível de conhecimento variado nos temas de GCN e a devida confirmação da experiência nas disciplinas. Inclusive, é feita uma verificação dessa experiência com evidências requisitadas pelo instituto, juntamente com o conhecimento para diferentes atuações.

As práticas profissionais para os objetivos de GCN são:

a) iniciação e gestão do programa - estabelece a necessidade de um programa de continuidade dos negócios: obter suporte e financiamento para o programa de continuidade dos negócios; estrutura organizacional para o programa de continuidade dos negócios; introduzir conceitos-chave, como a gestão do programa, conscientização sobre riscos, identificação de funções/processos críticos, estratégias de recuperação, treinamento e conscientização e exercícios/testes;

b) avaliação de risco - identificar os riscos que possam prejudicar sua imagem: proteger os recursos da organização; avaliar os riscos para determinar os potenciais impactos para a organização, definir a forma mais eficaz dos recursos para reduzir esses impactos;

c) análise de impacto nos negócios - identificar e priorizar as funções e os processos de organização, visando quais são as principais causas de impacto: avaliar os recursos de impacto nos processos de análise de negócios; analisar as características para atender a tais requisitos;

d) estratégias de continuidade dos negócios - seleciona as estratégias com melhor custo-benefício, para reduzir as características identificadas e o processo de benefício durante a avaliação de risco de análise de impacto nos negócios;

e) resposta a incidentes - desenvolver e auxiliar a implantação de um sistema de gestão de incidentes que: defina os papéis, linhas de autoridade e de autoridade na organização; defina os requisitos para desenvolver e implementar o plano de resposta a incidentes da organização; garanta que haja a resposta rápida à incidência e a necessidade de coordenação com as agências externas, quando necessário;

f) desenvolvimento e implementação do plano - documentar planos para utilização durante um incidente, permitindo que a organização se mantenha em funcionamento;

g) programa de conscientização e treinamento - estabeleça e mantenha programas de treinamento e conscientização para capacitar o pessoal a responder a incidentes de maneira calma e eficiente;

h) exercício, avaliação e manutenção do Plano de Continuidade dos Negócios: estabelecer um programa de exercícios, avaliação e manutenção para manter o estado de prontidão;

i) comunicação em crise: fornece um modelo para o desenvolvimento de um plano de comunicação em crise: garantir que o plano de comunicação em crise irá fornecer comunicação com eficácia como partes internas e externas;

j) coordenação com agências externas: estabelecer políticas e procedimentos para coordenar as atividades de resposta a incidentes com entidades públicas.

Levando-se em consideração este importante aspecto da investigação para uma alta contribuição deste trabalho para a pesquisa, por meio de contatos utilizados na FEBRABAN, no comitê de gestão de risco desta entidade, foi possível contatar os profissionais:

- **ATOR_1**. Com mais de 15 anos de experiência, atualmente, exerce a função de gerente executivo responsável pelo Programa de Continuidade de Negócios. Possui MBA em Gestão de Segurança da Informação, pós-graduação em Gestão de Crises Corporativas, possui a certificação CBPC - *Certification Business Continuity* Professional, do instituto americano DRII (*Disaster Recovery Institute International*). Possui ainda a certificação MBCI - *Master of Business Continuity Institute*, do instituo britânico BCI (*Business Continuity Institute*), que é a escola inglesa para gestão de continuidade de negócios.

É ISO 22301- *Technical Expert* – BSI e ISO 27001 *Lead Auditor*, é membro da Subcomissão de Gestão de Continuidade dos Negócios na FEBRABAN - Federação Brasileira dos Bancos no Brasil. Membro do GT Infraestruturas Estratégicas Finanças, ligado à presidência da república, autor de livro, relacionado ao tema, considerado o registro único sobre a disciplina no país. Ainda, é responsável por manter o *site* exclusivo para temas de GCN, com ampla experiência em palestras, *workshops* e eventos no Brasil. As credenciais deste profissional para o assunto de gestão de crise e continuidade de negócios no Brasil são relevantes, considerando que não há muitos profissionais com este nível de experiência na indústria financeira brasileira.

- **ATOR_2**. Atualmente, é o gerente de tecnologia da informação – gerenciamento regulatório de segurança cibernética, responsável pelo Programa de Continuidade de Negócios de uma organização financeira de capital privado de serviços bancários múltiplos (varejo e corporativo) no Brasil. Possui mais de 20 anos de carreira em Cibersegurança, Tecnologia da Informação, Governança de TI, Risco e Controle, Privacidade de Dados, Gestão de Fornecedores, Operações de TI, Suporte ao Usuário Final, Auditoria de TI, Gestão de Estratégia de Desastres e *Failover*, projetos e

experiência em TI Merge. Está há mais de 15 anos gerenciando diferentes equipes, e experiência na gestão de equipes de alta *performance* e exposições globais internacionais. É formado em Sistemas de Tecnologia da Informação, com MBA em Gestão de Tecnologia da Informação, mestrado em Administração – Governança Corporativa, e cursos de extensão em Gerenciamento de Riscos, Liderança em Cyber Security.

Possui a certificação em *Certified Data Privacy Solution, Information Security Office, Information Security Management Professional based on ISO/IEC 27001, Information Security Management 27001 Foundation, Privacy &Data Protection; Cloud Computing Foundation, Agile Scrum Master; Cyber & IT Security, Business Continuity Management, COBIT 5 Foundation, ITIL Foundation level*, com ampla experiência em palestras, *workshops* e eventos no Brasil. As credenciais deste profissional para o assunto de gestão de continuidade de negócios no Brasil são relevantes, considerando que não há muitos profissionais com este nível de experiência na indústria financeira brasileira.

- **ATOR_3.** Atualmente, está como gerente de Gestão de Continuidade de negócios e Gestão de Crises, sendo graduada em Administração de Empresa e com mestrado em Administração de Empresas. Possui certificação na área de atuação, com mais de 15 anos de experiência em gestão das disciplinas, equipe e coordenação de times multidisciplinares.

- **ATOR_4.** Atualmente, atua como gerente de Crises e Continuidade de Negócios – graduada em Publicidade & Marketing, Administração com ênfase em marketing e pós-graduada em Gestão de Crise corporativa. Possui certificações internacionais CBCP pelo DRII e MBCI pelo BCI. Tem como atividade principal toda rotina que envolve o ciclo GCN e Governança de Gestão de Crises. Atua há mais de 10 anos na área de Business Continuity Management (BCM). Atualmente, é responsável pela implementação e governança do GCN na sua organização, atuando também na coordenação, análise e avaliação dos riscos do negócio para definição e implementação de estratégias.

- **ATOR_5**. Atualmente, é Analista Sênior na área e o processo de GCN nasceu na área de Segurança da Organização. Tem ampla experiência nesta área, mas lidando com continuidade de negócios. Hoje, trabalha no processo de GCN e encontra-se na Gerência de Risco Operacional, com 9 anos e 8 meses na função. É graduado em Administração de Sistemas de Informação, e possui certificações internacionais CBCP pelo DRII. Tem vários treinamentos na área de GCN, todos eles em São Paulo, na Sthroll System, Daryus, Brasiliano e um na *in Company*, conduzidos então pelo falecido já Fernando Marinho, autor de alguns livros sobre GCN. De forma geral, são essas as atividades que o profissional executa: a) realização de Análise de Impacto nos Negócios em novas áreas; b) revisão de dados dos processos críticos já identificados; c) revisão dos Planos de Contingência Operacionais das áreas negociais e de TI; d) revisão dos normativos de GCN (Manual de Gestão de Continuidade de Negócios e Política de GCN); e) participação no teste de Recuperação de Desastres de TI (PRD-TI); f) elaboração de matérias para aculturamento em GCN; g) Ministrar treinamentos em matérias diversas em GCN; h) revisões periódicas da metodologia de GCN já implantada; i) participação em treinamentos externos de Continuidade de Negócios; j) realização de testes de contingência das áreas críticas identificadas; k) análise dos relatórios de Incidentes Cibernéticos do ponto de vista da continuidade de negócios; l) suporte às empresas do conglomerado (Organização DTVM, Financeira e Seguros Organização), relativamente à continuidade de negócios; m) suporte às atividades de risco operacionais relativamente aos riscos de terceiros.

4.3.2. Perfil da organização

As organizações que participaram desta pesquisa, representadas por seus gestores de Continuidade de Negócios, dispuseram-se a responder a pesquisa pela plataforma Microsoft Teams. As respostas tornaram possível identificar os pontos descritos a seguir.

A GCN das organizações estudadas conta com a atuação de profissionais dedicados para a gestão de continuidade de negócios e gestão de crises. Apesar de apresentar diferenças em suas operações, no tangente ao volume de processamento realizado, a aplicabilidade da gestão de continuidade de negócios e gestão de crises são

semelhantes. Os colaboradores são igualmente certificados e treinados na disciplina de GCN. As organizações utilizam diferentes tipos de indisponibilidades, inclusive, há cronogramas anuais estabelecidos para execução de testes para validar a tolerância a falhas e possíveis cenários, em um mínimo de três, que podem causar a total indisponibilidade das operações. Em geral, as organizações possuem tipos de testes em que suas estratégias são validadas.

A GCN e gestão de crise nas organizações demonstraram estrutura dentro dos padrões similares ao aplicado pelo mercado analisado por este trabalho. Detêm o mesmo modelo de interseções com as disciplinas de gestão de problemas e incidentes e gestão de mudanças. Atuam de forma integrada com as áreas de Governança Corporativa.

As organizações detêm um *site* alternativo, com posições de trabalho capacitadas com a infraestrutura tecnológica necessária para operacionalização de colaboradores. Os servidores e os equipamentos críticos, indispensáveis para realização dos planos de continuidade de negócios, são ativos da organização. Este modelo conta, hoje no mercado de tecnologia da informação, com um modelo de *PaaS*, ou, *Plataform as a Service*.

A gestão das plataformas no *site* alternativo fica a cargo da própria TI de cada organização, permitindo a atualização de versões entre o *site* principal e do *site* alternativo, de forma sincronizada e adequada à manutenção de todos os PCN's. Assim sendo, há um rigoroso controle sobre os fornecedores e sobre os contratos estabelecidos, para mitigar qualquer risco à segurança e aos planos de continuidade de negócios da organização. Há, ainda, cláusulas específicas e passíveis de multa sobre a confidencialidade de informações, LGPD[27], além da instalação de processos altamente complexos para criptografia de todo e qualquer dado trafegado.

[27] LGPD – Lei 13.709/18, alterada pela Lei 13.853/19). Considera que dados pessoas pertencem a pessoas, e não a empresas, e que cabe aos responsáveis pelas diversas etapas dos tratamentos de dados protegê-los. A lei também cria a necessidade de comunicação, por parte das organizações de vazamentos ou violações de dados pessoais para a ANPD e impõe penalidades como multas de até 2% do faturamento da pessoa jurídica. Mais detalhes estão no Anexo D.

O grau de maturidade das organizações, promovido pela governança de processos de TI, também pode ser considerado alto, dada a aplicação de políticas para continuidade de negócios e segurança da informação, disseminados em todos os níveis hierárquicos das companhias. Tal ação possibilita o desenvolvimento de testes que validem toda a cadeia de processos de negócios de cada organização, considerados críticos pelo time de gestão, propiciando o tempo de resposta requerido no RTO – Recovery Time Objetive (Objetivo de Tempo de Recuperação). Esse mecanismo atende às expectativas dos executivos e acionistas no contorno de um evento de crise de grandes proporções.

A identificação dos processos de negócios considerados críticos e o mapeamento dos possíveis impactos financeiros são encorajados pelo nível de maturidade da GCN, que conta com a aplicação cíclica de testes de contingência para analisar e documentar os resultados obtidos. Assim, identificam-se oportunidades para a melhoria contínua de todos os planos de PCN. Portanto, é indiscutível o árduo preparo do time responsável pela GCN em analisar situações, que possam vir a impactar o negócio e, com isso, balizar estratégias de investimentos em planos de recuperação de desastres, por exemplo, baseados na análise de risco, identificado na análise de impacto do negócio e no preenchimento do BIA – *Business Impact Analysis* (Análise de Impacto nos Negócios).

Dentro da análise de gestão de crise e dentro de gestão de continuidade de negócios, apesar do risco inerente na adoção de um *site* compartilhado de posições de negócio para utilização em um plano de contingência, é possível afirmar que há muita resiliência na operação das organizações entrevistadas. Inclusive, pelo menos uma vez ao ano, são executados exercícios para testar a recuperação dos principais processos de negócio no *site* alternativo, com a prerrogativa de queda do *site* principal, validando junto às áreas usuárias a recuperação de acessos e verificando o atendimento às expectativas dos RTO's estipulados.

Há apenas mais um ponto a ser explanado, a estrutura de *site* alternativo utilizado evidencia a diferença na gestão de crise *versus* o investimento em um *site* dedicado. Apesar de apresentar um custo financeiro menor, há igualmente um risco assumido, e um investimento significativo para manter a governança e a segurança da

informação, com envolvimento efetivo dos colaboradores para manter a revisão, documentação e análises constantes sobre o modelo utilizado. A organizações tem disponível uma árvore de acionamento bem definida e claramente inserida como parte dos planos de PCN da organização.

As organizações, por meio dos seus entrevistados, informaram a existência de um documento BIA, no qual os processos são classificados por impacto financeiro. Entretanto, declarou-se também a impossibilidade de apresentar ou disponibilizar esse documento por conter questões de confidencialidade de informações e por endereçar processos de negócios e o envolvimento de valores de negócios.

As organizações possuem também, em seus planos de recuperação de desastres, as informações necessárias sobre seus principais fornecedores mais críticos, que precisam estar disponíveis em caso de uma declaração de contingência. Porém, não se informou em que área essa informação estaria disponibilizada dentro do GCN.

As organizações apresentaram um bom nível de maturidade em governança corporativa, de gestão de continuidade de negócios e gestão de crises, utilizando a ABNT NBR ISO/IEC 22301. Além disto, possuem um estruturado processo de revisão de incidentes e de mudanças, que são apurados após os exercícios de contingência, fechando o ciclo de revisão de problemas encontrados ao longo dos testes de acionamento do PCN.

Dentro de uma análise dos construtos liderança em momentos de crise; planejamento de crise; coordenação de parcerias, longevidade, compreensão; pessoas, TI e negócios, entende-se que as organizações executam, no mínimo uma vez ao ano, um exercício que simula a queda do *site* principal e testam a recuperação dos principais processos considerados críticos no *site* alternativo. Perfazem-se, junto às áreas usuárias, as validações dos RTO’s e RPO’s, de forma ainda mais aprimorada.

Notoriamente, dentro de uma análise dos construtos mencionados no parágrafo anterior, entende-se que as organizações também possuem um elevado grau de governança de TI. A aplicação de uma política estruturada de continuidade de negócios, que atua em diferentes níveis, é indiscutível e permite o desenvolvimento

de exercícios de simulação, pelo time de continuidade de negócios, para testar, simular e validar a manobra de contingência.

4.3.3. Visão geral de Governança Corporativa

Sob o enfoque de gestão, a visão de Governança Corporativa na organização inclui uma efetiva supervisão sobre a GCN para proteção dos interesses dos *stakeholders*, partes internas e externas da organização. Tal visão encontra-se alinhada com as melhores práticas, considerando que conta com conselhos independentes, comitês com funções específicas e estrutura diretiva dedicada, estabelecendo políticas e normas, e provendo recursos humanos, materiais e tecnológicos voltados a essa atividade.

O Gerenciamento Corporativo de GCN está fundamentado na elaboração de planos para as atividades essenciais, utilizando metodologias e ferramentas que uniformizam o formato de coleta e tratamento dos dados, bem como a documentação dos processos de PCN. O desenvolvimento do GCN nas áreas de negócios obedece aos critérios, tais como: necessidades estratégicas para os negócios; exigências contratuais com clientes; demandas de órgãos reguladores; certificações que agregam valor aos negócios; solicitações das áreas de negócios; foco na cadeia de valor da organização (processos que agregam valor); atendimento ao cliente; prestação de serviços; entrega de produtos; cronograma de trabalho da área de PCN. A atuação da GCN tem como foco as áreas de negócio e seus processos de negócios considerados críticos, e como se relacionam com os demais processos.

4.4. Perfil amostra - Entrevistas

4.4.1. Entrevista ATOR_1

Ao se iniciar a entrevista, foi perguntado:

Entrevistador: A organização possui uma área específica de Gestão de Continuidade de Negócios? Se afirmativo, com qual diretoria estava a responsabilidade de GCN? Por quê? Explique o ponto.

ATOR_1: Sim. A GCN, em nossa organização, está na unidade responsável pela Gestão de Segurança da Informação, vinculada à Diretoria de Risco Corporativo. A GCN está subordinada à área de Risco desde sua criação e acredito que a posição se deve à resolução 3380[28] do BACEN.

Entrevistador: A organização considera GCN como um ponto importante para alcançar seus objetivos de negócio? Como GCN se encaixa na estratégia de negócios da empresa?
ATOR_1: A GCN é considerada importante para o atendimento das demandas legais e de auditoria. Normalmente, não é considerada na estratégia de negócios.

Entrevistador: A organização possui políticas(s) específica(s) para o cumprimento de ações relacionadas à gestão de continuidade de negócios? Sim ou Não. Todas as áreas de negócios foram contempladas nesta política?
ATOR_1: Sim, possui. Toda a corporação é contemplada.

Entrevistador: A organização possui um centro de processamento de dados de produção ou principal e um centro de processamento secundário ou alternativo para acionamento em caso de um impacto operacional em suas operações? Sim ou não? Explique como se dá o acionamento de contingência para o site alternativo.
ATOR_1: Sim, possui. A organização possui dois centros de processamento. O acionamento é realizado com base nos planos de recuperação de desastres da TI.

Entrevistador: Em caso afirmativo, a organização possui uma equipe ou comitê de mudança (*change management*), que garanta que todas as atualizações feitas no ambiente de produção também sejam realizadas no centro de processamento secundário ou alternativo? Sim ou não? Explique como se dá.
ATOR_1: Sim, a empresa tem um processo implantado de Gestão de Mudanças. Existe equipe dedicada e políticas sobre este tema dentro da área de TI.

[28] Em junho de 2006 pelo Conselho Monetário Nacional – CMN, publicou a resolução 3380:2006 que reflete especificações apresentadas na Basileia II, tratando do risco operacional e foi substituída pela resolução nº 4557 de 23 de fevereiro de 2017.

Entrevistador: A organização possui duplicação de abordagem de *link* de telecomunicação de dados entre seus principais sites de negócio? Em caso afirmativo, essa duplicidade de conectividade de *links* de dados ocorre com operadoras de telecomunicações diferentes ou não?
ATOR_1: Sim, a duplicação de *links* é implementada com empresas diferentes, o que não garante que estas empresas utilizem o mesmo meio físico. Alguns *links* têm contingenciamento via satélite.

Entrevistador: A organização possui um processo de monitoração e manutenção dos planos de continuidade de negócios (*Plan – Do – Check - Act*)? Sim ou não?
ATOR_1: Sim, a empresa implementou um programa de Continuidade dos Negócios.

Entrevistador: GCN é valorizado ou mesmo exigido pelo mercado/acionistas/Bolsa? O que a organização tem feito nesse sentido? As iniciativas de GCN são comunicadas ao mercado e aos investidores? Qual o retorno disso?
ATOR_1: Não se aplica. A empresa não tem capital aberto.

Entrevistador: A organização considera GCN como um ponto importante para alcançar seus objetivos de negócio? Como GCN se encaixa na estratégia de negócios da empresa?
ATOR_1: A GCN é considerada importante para o atendimento das demandas legais e de auditoria. Normalmente, não é considerada na estratégia de negócios.

Entrevistador: A organização possui um mapeamento da sua cadeia de principais fornecedores? Esses fornecedores possuem classificação de criticidade? Os fornecedores críticos participam de testes de continuidade de negócios? Sim ou não? Descreva como isso ocorre.
ATOR_1: Sim, os fornecedores críticos são mapeados. Não existe classificação. Eles não participam nos testes. Deles é exigido a apresentação de um plano de continuidade.

Entrevistador: A organização possui a revisão e a coleta dos resultados dos testes e a criação de planos de ação para corrigir os problemas ocorridos durante as manobras de recuperação (Lições Aprendidas)? Sim ou não? Como ocorrem essas análises?

ATOR_1: Após o teste, é obrigatório o preenchimento de relatório, o qual será avaliado pela área gestora do programa da continuidade. Caso necessário, um plano de ação é elaborado em conjunto, gestor do processo de negócio e área gestora do programa da continuidade. Sim.

Entrevistador: GCN faz parte do treinamento de todos os colaboradores da empresa? Por quê? De que forma? Foi possível medir algum resultado? Quais?
ATOR_1: Sim. Existe curso específico na Universidade Corporativa. Também são realizados eventos ao longo do ano. O acompanhamento é realizado por meio da prova realizada após treinamento.

Entrevistador: A organização possui um mapeamento de conexão de entidades externa (B2B), (B2C)? Essas entidades externas (B2B), (B2C) possuem classificação de criticidade? As entidades externas participam de testes de continuidade de negócios? Sim ou não? Como isso ocorre?
ATOR_1: Não.

Entrevistador: É feito algum tipo de mensuração sobre a adoção de GCN? Quais? Que nova iniciativa surgiu após análise dos dados?
ATOR_1: Existem indicadores relativos à GCN definidos em política específica. Estes indicadores são acompanhados pelo conselho diretor. Correções, caso necessárias, são feitas após análise destes indicadores.

Entrevistador: GCN é valorizado ou mesmo exigido pelo mercado/acionistas/Bolsa? O que a organização tem feito neste sentido?
As iniciativas de GCN são comunicadas ao mercado e aos investidores? Qual o retorno disto?
ATOR_1: Não se aplica. A empresa não tem capital aberto.

4.4.1.1. Síntese da entrevista ATOR_1

De acordo com o entrevistado, a organização na qual ele trabalha possui, na área GCN, equipe dedicada e está na unidade responsável pela Gestão de Segurança da Informação, vinculada à Diretoria de Risco Corporativo. AGCN é considerada uma

área importante para o atendimento das demandas legais e de auditoria, porém não é considerada como estratégica. A organização possui dois centros de processamento e seu acionamento é realizado com base nos planos de recuperação de desastres da TI. Tem um processo de gestão de mudanças implantado e a organização contempla todas as áreas de negócio com políticas sobre o tema.

A organização conta com a duplicação de *link* de telecomunicação entre seus principais sites de negócio e é implementada com empresas diferentes, o que não garante que estas empresas utilizem o mesmo meio físico. Alguns *links* têm contingenciamento via satélite e também conta com: a) um processo de monitoração e manutenção dos planos de continuidade de negócios; b) mapeamento da sua cadeia de fornecedores considerados críticos, sendo que esses não participam dos testes, e deles são cobrados seus próprios planos de continuidade de negócios; c) revisão e coleta dos resultados dos testes que, após sua realização, é obrigatório o preenchimento de um relatório, o qual é avaliado pela área gestora do programa da continuidade. Se necessário, um plano de ação é elaborado em conjunto com o gestor do processo de negócio e área gestora do programa da continuidade.

A GCN promove treinamentos com cursos específicos, por meio da Universidade Corporativa, que podem ser realizados durante todo o ano e seu acompanhamento é realizado por meio de prova, após término do treinamento. Existem indicadores relativos à GCN definidos em política específica e estes indicadores são acompanhados pelo conselho diretor. Correções, caso necessárias, são feitas após análise destes indicadores

4.4.2. Entrevista ATOR_2

Ao se iniciar a entrevista, foi perguntado:
Entrevistador: A organização considera a GCN como um ponto importante para alcançar seus objetivos de negócio? Como GCN e GC se encaixam na estratégia de negócios?
ATOR_2: Sim. A organização considera GCN como uma disciplina principal para a gestão de riscos operacionais, assim como segurança da informação, cibersegurança e gestão de riscos. A GCN é parte da estratégia de negócios como forma de

mapeamento dos processos críticos e de negócio e como forma de determinação de impacto financeiros em seus negócios.

Entrevistador: Qual é a importância estratégica do GCN para sua organização?
ATOR_2: A GCN possui um papel importante na estratégia de gestão de risco operacional da empresa para garantir que exista resposta adequada às interrupções, que podem ser causados por eventos de pequeno e grande severidade, mantendo a disponibilidade dos ambientes produtivos das áreas de negócio.

Entrevistador: Quais foram e tem sido os principais "marcos" da GCN na sua organização? Quais as principais conquistas e desafios?
ATOR_2: O desenvolvimento do mapeamento dos processos críticos das áreas de negócio e uma atribuição financeira aos processos críticos da empresa. Já as principais conquistas foram o desenvolvimento de uma cultura de gestão de riscos operacionais nas primeiras linhas de defesa[29] da empresa.

Entrevistador: A organização possui uma equipe ou comitê de mudança que garanta que todas as atualizações feitas no ambiente de produção também sejam realizadas no site alternativo? Explique como se dá.
ATOR_2: Sim, a organização possui um comitê de mudanças que garante que qualquer alteração no ambiente de produção, que seja considerado um processo como *"major change"*. Só aprova o *deployment* para produção a partir de um plano de replicação para os ambientes de contingência e com a obrigatoriedade de um teste em até 120 dias após o ambiente ser atualizado.

Entrevistador: A organização possui a revisão e a coleta dos resultados dos testes e prática de lições aprendidas? Como ocorrem essas análises?
ATOR_2: Sim! Todos os testes de continuidade de negócios são validados pelas áreas usuárias e as falhas dos testes da área possuem a abertura de um *issue* (RCSA) nos sistemas de gestão de risco com um plano de ação devidamente documentado. Essas análises são realizadas com os times de tecnologia e times de negócios, que são liderados pelo time de continuidade de negócios, em que o resultado dos testes dentro

[29] Linhas de Defesa: termo utilizado em Governança Corporativa. Consulte Anexo E.

das janelas esperadas é realizado e, a partir dos resultados, uma planilha de validação do *script* de testes é realizada e revisada ao final dos testes. Em caso de falha, as evidências são reunidas e discutidas em reunião gerencial e um reteste é agendado em até 120 de acordo com a política da área.

Entrevistador: A organização possui um processo de monitoração e manutenção da GCN?
ATOR_2: Sim. Há a utilização de uma ferramenta global de gestão de continuidade de negócios que requer uma atualização cíclica para testes e *sign-off* de atualização de processos e informações como *call tree*, time crítico, aplicações, fornecedores, conexões externas, B2B, processos críticos e grade de horários críticos.

Entrevistador: A organização possui um mapeamento da sua cadeia de principais fornecedores?
ATOR_2: Sim. No sistema global de gerenciamento de informações de GCN, todos os fornecedores considerados críticos, tanto para a estratégia de contingência quanto para a recuperação das atividades de negócios, são listados com seus respectivos *risk assessment* no sistema.

Entrevistador: Esses Fornecedores possuem classificação de "criticidade"?
ATOR_2: Sim. Todos os fornecedores possuem uma classificação e um *tier* de risco operacional para o negócio. Os riscos do fornecedor podem ser de *tier* 1 a 3 - alto risco ou de 4 a 5 *tier,* considerados riscos baixos, dependendo de uma série de análises dos fornecedores

Entrevistador: Os fornecedores críticos participam dos seus testes de continuidade de negócios? Descreva como isso ocorre.
ATOR_2: Sim. Os fornecedores considerados como críticos para a estratégia de recuperação ou para a operação do negócio possuem uma cláusula contratual que garante a participação do fornecedor nas agendas de testes e validação de contingência. Isso se dá no planejamento da atividade de recuperação onde os fornecedores são convidados a participar dos planos e as cláusulas de recuperação são acionadas normalmente como se fosse um evento real.

Entrevistador: A sua organização monitora *stakeholders* que podem influenciar a GCN? Como ocorre esse monitoramento?
ATOR_2: Sim, na verdade a organização possui comitês de gestão de risco onde se discutem os principais aspectos da disciplina de GCN, entre outras: pontos como testes, resultados dos testes, agenda de testes e atualizações dos planos, e os principais *stakeholders* de gestão de riscos, negócios e alta gestão participam e formalizam em atas auditadas a participação de *stakeholders* nos processos de *InfoSec* e GCN. Através dos comitês registrados nos manuais de governança corporativa da Organização em que são discutidos aspectos de risco operacional que incluem o envolvimento dos principais *stakeholders* nos assuntos de risco operacional.
Entrevistador: E quais são os principais stakeholders?
ATOR_1: *Heads* das principais áreas de negócios, CEO, *Head* de Auditoria Interna, 2ª. e 3ª. linha de defesa, *Compliance*, Riscos, Tecnologia, Segurança da Informação e CFO.

4.4.2.1. Síntese da entrevista ATOR_2

Segundo o entrevistado, a organização_2 considera a área de GCN como uma disciplina principal para: gestão de riscos operacionais; segurança da informação; cibersegurança e gestão de terceiros. Assim, a estratégia de negócio se encaixa: a) como forma de mapeamento dos processos de negócios considerados críticos; b) como forma de determinação de impacto financeiros.

A GCN possui um papel importante na estratégia da organização e seus principais "marcos" são: a) desenvolvimento do mapeamento dos processos considerados críticos das áreas de negócios; b) uma distribuição financeira aos processos de negócios considerados críticos. Por outro lado, suas conquistas foram o desenvolvimento de uma cultura de gestão de riscos operacionais nas primeiras linhas de defesa da organização.

A organização possui um comitê de mudanças que garante que, em qualquer alteração no ambiente de produção, haja o reflexo no ambiente de contingência, com prioridade de um teste em até 120 dias após o ambiente ser atualizado. O entrevistado

lembra que todos os testes são validados pelas áreas de negócios e as falhas dos testes são registradas em sistema com um plano de ação devidamente documentado.

A organização possui um mapeamento da sua cadeia de principais fornecedores para gerenciamento de informações de GCN, tanto para a estratégia de contingência quanto para a recuperação das atividades de negócios. Estes fornecedores possuem uma classificação de “criticidade” e participam dos testes de continuidade de negócio.

A organização conta com um comitê de gestão de risco, no qual se discutem os principais aspectos da GCN. Seus principais *heads* são: CEO, *Head* de Auditoria Interna; 2ª e 3ª linha de defesa.

4.4.3. Entrevista ATOR_3

Ao se iniciar a entrevista, foi perguntado:
Entrevistador: A organização considera GCN como um ponto importante para alcançar seus objetivos de negócio?
Como GCN e GC se encaixa na estratégia de negócios?
ATOR_3: Sim, os negócios são priorizados para atendimento aos níveis de resiliência requeridos. Algumas vezes o nível de resiliência define objetivos de nossas metas corporativas na organização.

Entrevistador: Qual é a importância estratégica do GCN para sua organização?
ATOR_3: Não tem importância estratégica, utilizamos a disciplina de GCN para assegurar a resiliência requerida pela companhia junto a seus *stakeholders*.

Entrevistador: Quais foram e tem sido os principais “marcos” da GCN na sua organização? Quais as principais conquistas e desafios?
ATOR_3: Priorização, simplificação de processos e documentos e, principalmente, adequação as necessidades atuais e reais da organização. Processos simples e objetivos para manutenção das estratégias de GCN e atendimento às necessidades de coordenação de eventos reais.

Entrevistador: A organização possui uma equipe ou comitê de mudança que garanta que todas as atualizações feitas no ambiente de produção também sejam realizadas no site alternativo? Explique como se dá.
ATOR_3: Sim. A documentação de mudanças só tem aprovação para implementação em produção se os requisitos do ambiente alternativo estiverem também contemplados. Além desse processo documental, todas as mudanças são avaliadas quanto aos seus impactos e validações necessárias após reunião de aprovação documentada com os times técnicos envolvidos.

Entrevistador: A organização possui a revisão e a coleta dos resultados dos testes e prática de lições aprendidas? Como ocorrem essas análises?
ATOR_3: Sim. Os resultados dos testes realizados movimentam indicadores estabelecidos para GCN e são analisados previamente e durante a reunião de lições aprendidas. Esses resultados podem gerar planos de ação para acompanhamento do time de GCN.

Entrevistador: A organização possui um processo de monitoração e manutenção da GCN?
ATOR_3: Sim.

Entrevistador: A organização possui um mapeamento da sua cadeia de principais Fornecedores?
ATOR_3: Sim.

Entrevistador: Esses fornecedores possuem classificação de “criticidade”?
ATOR_3: Sim.

Entrevistador: Os fornecedores críticos participam dos seus testes de continuidade de negócios? Descreva como isso ocorre
ATOR_3: Sempre que necessário, possível/viável. Mais comumente em testes de tecnologia, chaveamento de infraestrutura tecnológica entre sites onde necessitamos da participação de nossos fornecedores.

Entrevistador: A sua organização monitora *stakeholders* que podem influenciar GCN? Como ocorre esse monitoramento?
ATOR_3: Sim. No âmbito de riscos corporativos e operacionais, que são *inputs* para o tratamento da disciplina de GCN, os riscos internos e externos são avaliados e monitorados ciclicamente. Adicionalmente, avaliamos ciclicamente o atendimento aos requisitos de GCN de nossos fornecedores críticos e mantemos uma relação muito próxima a nossos reguladores e as demandas de resiliência aportadas por nossos clientes.

4.4.3.1. Síntese da entrevista ATOR_3

De acordo com o entrevistado, para a organização_3, a área de GCN, apesar de não ser considerada como estratégica, mantém disciplinas que asseguram a resiliência requerida pela organização juntos a seus *stakeholders*. Vale ressaltar que, algumas vezes, o nível de resiliência define objetivos das metas corporativas. Os principais "marcos" da área de GCN são: priorização; simplificação de processos e documentos e principalmente adequação às necessidades atuais e reais da organização. Processos simples e objetivos para manutenção das estratégias de GCN e atendimento às necessidades de coordenação de eventos "reais" são tidos como principais desafios e conquistas.

No âmbito de riscos corporativos e operacionais, que são *inputs* para o tratamento de disciplinas de GCN, os riscos internos e externos são avaliados e monitorados ciclicamente. Adicionalmente, é avaliado ciclicamente o atendimento aos requisitos de GCN dos fornecedores críticos. É mantida uma relação próxima como os reguladores e as demandas de resiliência são aportadas pelos clientes. Um ponto importante para todo o processo de GCN foi reportado com relação às mudanças na documentação, que só tem aprovação para implantação no site principal se os requisitos também forem atendidos para o site alternativo.

Os resultados dos testes movimentam indicadores que são avaliados em reuniões técnicas de lições aprendidas, que podem geram planos de ação.

4.4.4. Entrevista ATOR_4

Nota Importante: o ATOR_4 é o gestor GCN do banco que é o braço digital, criado em 2016, da organização_4.
Ao se iniciar a entrevista, foi perguntado:
Entrevistador: A organização considera GCN como um ponto importante para alcançar seus objetivos de negócio?
Como GCN e GC se encaixa na estratégia de negócios?
ATOR_4: Sim. Sendo uma empresa digital, a premissa é disponibilidade total.

Entrevistador: Qual é a importância estratégica do GCN para sua organização?
ATOR_4: Primordial para a satisfação dos clientes.

Entrevistador: Quais foram e tem sido os principais “marcos” da GCN na sua organização? Quais as principais conquistas e desafios?
ATOR_4: Estratégia de DR para negócio e tecnologia, aumento da complexidade dos testes, e como desafio foi a área dedicada na governança de negócio e Ti, equipe aumentando em 2022. Desafios: manter a cultura de risco devido à grande rotatividade dos colaboradores.

Entrevistador: A organização possui uma equipe ou comitê de mudança que garanta que todas as atualizações feitas no ambiente de produção também sejam realizadas no site alternativo? Explique como se dá.
ATOR_4: Sim. Na ferramenta de planejamento da mudança, este item está contemplado.

Entrevistador: A organização possui a revisão e a coleta dos resultados dos testes e prática de lições aprendidas? Como ocorrem essas análises?
ATOR_4: Sim. A cada teste, a cada revisão do plano.

Entrevistador: A organização possui um processo de monitoração e manutenção da GCN?
ATOR_4: Está em construção.

Entrevistador: A organização possui um mapeamento da sua cadeia de principais Fornecedores?
ATOR_4: Sim.

Entrevistador: Esses fornecedores possuem classificação de “criticidade”?
ATOR_4: Sim.

Entrevistador: Os fornecedores críticos participam dos seus testes de continuidade de negócios? Descreva como isso ocorre.
ATOR_4: Não.

Entrevistador: A sua organização monitora *stakeholders* que podem influenciar a GCN? Como ocorre esse monitoramento?
ATOR_4: Não.

4.4.4.1. Síntese da entrevista ATOR_4

De acordo com o entrevistado, para a organização_4, a área de GCN é considerada como muito importante, mas não como estratégica, apesar de se tratar de uma organização digital, cuja premissa é de disponibilidade total. Entende-se também que a área é primordial para a satisfação do cliente e isto é um “marco” valioso para a área, assim como para a organização.

O aumento da complexidade dos testes e a estratégia dos planos de recuperação de desastres são considerados desafios e conquista para o negócio e a tecnologia. Outro desafio encontrado pela organização é o aumento do time de colaboradores e a manutenção da cultura, visto que o *turnover* é considerado alto. As mudanças no ambiente de produção são realizadas por área dedicada de governança e TI.

Adicionalmente, a área de GCN efetua revisão dos planos e coletas dos resultados dos testes que são aplicados as técnicas de lições aprendidas. Existe a monitoração e manutenção dos planos, assim como é realizado mapeamento da sua cadeira de principais fornecedores.

Por ser uma organização relativamente nova no mercado nacional, a área digital ainda não monitora os *stakeholders* que possam vir a influenciar o GCN.

4.4.5. Entrevista ATOR_5

Ao se iniciar a entrevista, foi perguntado:
Entrevistador: A organização considera GCN como um ponto importante para alcançar seus objetivos de negócio?
Como GCN e GC se encaixam na estratégia de negócios?
ATOR_5: Toda empresa, nos dias de hoje, se deseja ao menos sobreviver, deve considerar o tema gestão de crises importante, e, muito mais do isso, deve dar uma atenção especial a esse ponto, pois a única coisa que se pode ter certeza diante das incertezas do mercado é que, cedo ou tarde, é provável que, em algum momento, a empresa terá que lidar com algum tipo de crise, seja ela ocasionada por danos à sua imagem ou oriundas de falhas internas ou de TI. E saber gerenciá-las é importante para sua sobrevivência. No entanto, na prática, ainda é vigente nas organizações a falsa ideia de que o gerenciamento de um processo desses é simples e bastam alguns mediadas simples para tornar a empresa mais resiliente. Daí, quando uma crise ocorre de verdade, percebe-se que estavam enganados. Só que, nesse momento, dependendo do tamanho e do tipo da crise, as consequências podem ser tamanhas que muitas empresas não conseguem mais se recuperar. Por isso, foi elaborado o PAS 200:2011 - *Crisis management – Guidance and good practice*. Ele orienta como as empresas podem se preparar adequadamente para lidar com esse tipo de situação. Em relação à organização, nós nos preparamos conforme orientam os normativos sobre o tema. Para poder contribuir com qualquer negócio, o GCN precisa conhecer o que é ou não crítico para ele, e isso se consegue com o BIA e com uma boa análise de riscos, que procura identificar aqueles a que estão expostas as principais operações da empresa, e que não pode parar. Daí, procura-se elaborar estratégias para evitar a interrupção dessas operações com a confecção de planos de contingência para os processos mais críticos já identificados, planos de recuperação de desastre para os ativos de TI (PRD-TI) que os suportam e planos de contingência para os principais sistemas de informação que sustentam o negócio chamados de ISCP (*Information System Contingency Plan*).

Entrevistador: Qual é a importância estratégica da GCN para sua organização?
ATOR_5: O fornecimento de informações estratégicas para a tomada de decisão de forma mais racional, lógica e tempestiva possível, muitas vezes de forma antecipada, possibilitando a construção de estratégias mais eficientes diante de situações novas e inesperadas.

Entrevistador: Quais foram e tem sido os principais "marcos" da GCN na sua organização? Quais as principais conquistas e desafios?
ATOR_5: A criação de uma nova mentalidade em toda a organização, fazendo com que muitos dos princípios das normas isso/ABNT adotados internamente sejam levados pelos empregados e aplicados em suas vidas pessoais. A conscientização sobre a importância de se agir de forma preventiva, ao invés de reativa, também é algo que precisa ser ainda solidificado nas mentes das pessoas. Mas, de forma geral, já existe uma adesão a esse pensamento, e isso fortalece a organização, na medida que os processos são executados com isso em mente, o que minimiza a possibilidade de ocorrência de interrupções. A conquista principal foi ter conseguido implantar e passar por todos os ciclos (PDCA[30]) do GCN numa organização que nunca havia ouvido falar de GCN há alguns anos. Não é um processo simples, rápido e nem tão pouco fácil, mas olhando para trás foi algo necessário e não consigo imaginar hoje uma empresa sem GCN e que não esteja correndo mais riscos do que uma que o possui. Os desafios são vários, mas solidificar o processo de aculturação das pessoas faz parte deles, assim como, levantar os *gaps* para os corrigir enquanto ainda é possível. Aperfeiçoar o processo de gestão de crise também é importante.

Entrevistador: A organização possui uma equipe ou comitê de mudança que garanta que todas as atualizações feitas no ambiente de produção também sejam realizadas no site alternativo? Explique como se dá.
ATOR_5: Essa pergunta deveria ser respondida pelo pessoal de TI, já que no banco são eles que tratam desse assunto. Mas sim, o banco possui esse comitê e toda nova implantação de sistemas ou aplicativos passa necessariamente por um ambiente de homologação, onde são testadas e verificadas as suas falhas, e somente depois de

[30] PDCA – Modelo **P**lan (planejar); **D**o (fazer); **C**heck (checar); **A**ct (agir) – Detalhes veja Anexo C.

muitos testes é que se “sobe” para produção. Simplifiquei o processo, mas, de forma geral, é assim que ocorre por aqui.

Entrevistador: A organização possui a revisão e a coleta dos resultados dos testes e prática de lições aprendidas? Como ocorrem essas análises?
ATOR_5: Hoje temos uma segregação de atividades relacionadas aos testes de contingência. Uma área específica da TI realiza o teste anual do PRD (Plano de Recuperação de Desastre para os ativos de TI críticos) do qual eu também participo, mas apenas como observador, juntamente com várias outras áreas do banco, como auditoria, riscos e conformidade e algumas áreas negociais. São colhidas evidências e todos os participantes elaboram relatórios sobre suas observações, inclusive oportunidades de melhorias, e envia à área gestora do teste. Com isso, busca-se, cada vez mais, errar menos e solidificar as lições aprendidas. O outro teste é dos PCO’s (Planos de Contingência Operacionais) das áreas que suportam o negócio. Este sou eu quem conduz e já temos um calendário para o exercício de 2022. Com relação do PRD, eu já expliquei agora, em relação ao PCO, todas as áreas que participam do teste recebem um modelo de relatório onde devem anexar as evidências do que foi testado, de acordo como plano de contingência da área, e responder uma série de perguntas sobre o teste, como a sua duração, o que foi testado. Ou seja, quais processos foram executados, quais sistemas foram acessados, o que deu errado durante o teste, as sugestões de melhoria identificadas, se houve impacto em outras áreas e se o plano está realmente funcional ou não. Após o teste cada área tem cinco dias úteis para me enviar esse relatório assinado por quem testou e seu gestor. Faço a análise e, se detecto algo a ser melhorado, já tomo as providências que o caso exigir. Findo o recebimento de todos os relatórios, eu elaboro um final a ser encaminho ao diretor da minha área que o submete a diretoria colegiada e ao conselho de administração.

Entrevistador: A organização possui um processo de monitoração e manutenção da GCN?
ATOR_5: Sim, esse ano todo revisamos todos os processos já mapeados e os respectivos planos de contingência, bem como fizemos o BIA de 26 novas áreas, que foram criadas na última reestruturação. Nesse próximo ano, serão realizados os testes do PCO’s e já iniciado as revisões das áreas que completaram um ano desde a última

revisão. Conforme manual de gestão de continuidade de negócios interno, os gestores também são responsáveis por nos enviar qualquer alteração que ocorra nos processos ou nos planos de contingência de sua área, para podermos atualizar no nosso sistema de gestão.

Entrevistador: A organização possui um mapeamento da sua cadeia de principais fornecedores?
ATOR_5: Não respondeu.

Entrevistador: Esses fornecedores possuem classificação de "criticidade"?
ATOR_5: Não respondeu.

Entrevistador: Os fornecedores críticos participam dos seus testes de continuidade de negócios? Descreva como isso ocorre.
ATOR_5: Não respondeu.

Entrevistador: A sua organização monitora *stakeholders* que podem influenciar a GCN? Como ocorre esse monitoramento?
ATOR_5: Por sermos um banco cujo maior acionista é o Governo, tudo é feito de modo a balancear os anseios do governo com os dos demais acionistas. Não existe um monitoramento específico, no entanto, como existe um entendimento direto do presidente do banco com o governador, qualquer novo posicionamento que precisemos adotar nos é repassado pelo presidente.

4.4.5.1. Síntese da entrevista ATOR_5

Para a organização_5, segundo seu gestor, a GCN é mais uma ferramenta utilizada para garantir a sobrevivência da organização e que orienta a gestão da GCN, de acordo com os normativos, regulatórios e melhores práticas de mercado. A GCN não é considerada estratégica, mas é muito importante, pois, para ser executada, há a necessidade de se contribuir com qualquer área de negócio e ter discernimento para reconhecer o que é ou não crítico. Assim, configura-se sua importância estratégica, por meio do fornecimento de informações.

A organização tem como “marco” a contribuição na criação de uma nova mentalidade na organização e a conscientização sobre a importância de agir de forma preventiva. A área da GCN tem como principal conquista a implantação do PDCA, passando por todos os *steps* da referida metodologia. Já como desafio, pode-se elencar: a) solidificar o processo de “aculturamento”; b) levantar os “gaps” e corrigi-los; e c) aperfeiçoar o processo de gestão de crise.

A organização possui um comitê de mudança e toda nova implantação de sistemas ou aplicativos passa, necessariamente, por um ambiente de homologação para posterior passagem ao ambiente de produção. A organização realiza coleta de avaliação de resultados, inclusive com as oportunidades de melhorias, e possui um calendário de testes para 2022 formalizado.

5. ANÁLISE DOS RESULTADOS E CONSIDERAÇÕES FINAIS

A condução de uma análise de resultados qualitativos, como parte de uma avaliação das entrevistas, comporta bem a apresentação de achados empíricos. Segundo Yin (2014), a pesquisa pode dar passos adiante para interpretar os dados identificados, observando-se o fenômeno em seu mundo real e, após a análise e interpretação, é possível extrair conclusões gerais sobre a investigação ou mesmo na reformulação de resultados, o que reforça a capacidade que há na pesquisa qualitativa trabalhos voltados para as áreas corporativas, como é o caso desta dissertação.

Visando obter uma visão de análise mais simplificada, um arranjo bidimensional de linhas e colunas foi utilizado nesta pesquisa, para recompor os principais pontos de análise, para uma abordagem visual direta, em que se dispõem as informações coletadas e sumarizadas nas respectivas células que apoiam o processo de varredura de informações com dados dispostos e organizados para uma análise de resultados. Os resultados da análise se encontram em alinhamento e consonância com a fundamentação teórica tendo como guia a ABNT NBR ISO/IEC 22301 e que, comumente, são chamados de processos intrínsecos à operacionalização de uma Gestão de Continuidade de Negócios.

Abaixo, em resumo, encontra-se os principais resultados obtidos na fase de entrevista e coleta de dados desta pesquisa.

Quadro 9 – Resumo dos resultados obtidos durante a entrevista

Organização	1	2	3	4	5
A Organização considera GCN como um ponto importante para alcançar seus objetivos de negócio?	Sim	Sim	Sim	Sim	Sim
Como GCN se encaixa na estratégia de negócios?	Todos as áreas de negócio com processos considerados críticos têm planos de continuidade.	Como forma de: mapeamento dos processos; e determinação de impacto financeiro	Atendimento aos níveis de resiliência requeridos	Disponibilidade total	elaborar estratégias para evitar a interrupção dessas operações com a confecção de planos.
Qual é a importância estratégica do GCN para sua organização?	A Alta administração considera a GCN estratégica.	Alto	Baixo	Alto	Alto
Quais foram e tem sido os principais marcos da GCN na sua organização?	A GCN, de forma corporativa, iniciou no ano de 2005. Desde então a empresa desenvolveu modelos de atuação, políticas e treinou equipes para a atuação em situações adversas, tendo hoje um modelo consolidado e permanente.	Mapeamento	Adequação as necessidades atuais e reais	Estratégia de DR e, Aumento da complexidade dos testes	Criação de uma nova mentalidade

Quais as principais conquistas e desafios?	As principais conquistas foram a criação de unidade específica para a gestão da GCN corporativa, implementação de política e orçamento específico. O desafio é manter estas estruturas funcionais e capacitar as equipes envolvidas.	Cultura de GRO	Processos simples e objetivos para manutenção das estratégias de GCN	Área dedicada na governança de negócio de TI	Implantar e passar por todos os ciclos PDCA
A organização possui uma equipe ou comitê de mudança que garanta que todas as atualizações feitas no ambiente de produção também sejam realizadas no site alternativo?	Sim	Sim	Sim	Sim	Sim
Explique como se dá?	Existem equipes designadas nas áreas de negócio e na TI para assegurar que as mudanças ocorridas sejam implementadas nos ambientes alternativos.	Obrigatoriedade de um teste em até 120 dias após o ambiente ser atualizado	Reunião de aprovação documentada com os times técnicos envolvidos	Planejamento da mudança este item está contemplado	Sistemas ou aplicativos passa necessariamente por um ambiente de homologação onde são testadas e verificadas as suas falhas
A organização possui a revisão e a coleta dos resultados dos	Sim	Sim	Sim	Sim	Sim

testes e prática de lições aprendidas?					
Como ocorrem essas análises?	As análises são feitas pelas equipes das áreas de negócio e TI responsáveis pelos testes.	Testes de continuidade de negócios são validados pelas áreas usuárias	Gerar planos de ação para acompanhamento do time de GCN	A cada revisão do plano	São colhidas evidências e todos os participantes elaboram relatórios sobre suas observações.
A organização possui um processo de monitoração e manutenção da GCN?	Sim	Sim	Sim	Em construção	Sim
A organização possui um mapeamento da sua cadeia de principais fornecedores?	Não se aplica	Sim	Sim	Sim	Não se aplica
Esses fornecedores possuem classificação de "criticidade"?	Não tem capital aberto	Sim	Sim	Sim	Não se aplica
Os fornecedores críticos participam dos seus testes de continuidade de negócios?	Não se aplica	Sim	Sempre que necessário	Não	Não se aplica
Descreva como isso ocorre.	Não se aplica	Possui uma cláusula contratual que garante a participação	Comumente em testes de tecnologia	Não respondeu	Não se aplica

A sua Organização monitora *stakeholders* que podem influenciar GCN?	Sim	Sim	Sim	Não	Sim
Como ocorre esse monitoramento?	Existe o monitoramento das expectativas das partes interessadas no que tange a GCN, SI e GC.	Ciclicamente	Ciclicamente	Não se aplica	Não existe monitoramento específico
Quais são os principais *stakeholders*?	Não se aplica	Gestores	Não respondeu	Não se aplica	Não se aplica

Fonte: Elaborado pelo autor

5.1. Limitações da pesquisa e sugestões para estudos futuros

Toda pesquisa possui limitações para se focar nos objetivos de estudo, contudo como já foram mencionados no item de contextualização por Michael Porter (2004), em artigo publicado pela revista Exame (13/01/2004): "...*Brasil é um país onde há muitos talentos incríveis atropelados pelo sistema, talentos que têm de lidar com um monte de desvantagens e impossibilidades por causa do ambiente*...", "...*Eu nunca sei o que vai acontecer amanhã...".* Outro item, pode ser atribuído a pandemia do coronavírus, COVID-19, que continua impactando todos os setores produtivos no país, adicionalmente ainda temos o imediatismo conjugado com a visão de curto prazo.

Para efeito desta pesquisa acrescentou-se a indústria financeira – bancos com aplicação de ISO's com todos os regulatórios, circulares, normativos e resoluções expedidas pelos órgãos competentes. Para Lara, Perdómo e Jimenez, 1999, o setor bancário aparece como um dos setores que mais investe em TI, tendo grande parte de seus produtos e serviços, dependências dessas tecnologias, e Drucker, 1999, comenta que o computador tem exercido um forte impacto sobre as operações bancárias, sendo hoje, talvez, a indústria bancária a mais informatizada de todas. Mesmo sendo a indústria mais regulamentada do país, nota-se claramente que este investimento ainda é feito com uma visão de curto prazo, para "apagar incêndios". A necessidade de aderir às novas tecnologias é uma constante, mas ela se torna mais efetiva quando há horizonte estrategicamente definido a ser alcançado.

Outro item a se destacar e que até então não tinha sido considerado foi o fator *"tempo de entrevista".* Em tempo, ao realizar a entrevista com o ATOR_1, ele nos posicionou sobre este elemento o que nos possibilitou a revisão deste item. O que ocasionou revisão das perguntas que envolviam a entrevista, passando de 15 para 5 o que trouxe uma nova dinâmica com redução significativa do tempo de entrevista.

5.2. Principais resultados encontrados na pesquisa de campo

5.2.1 Dados específicos e complementares da pesquisa

Entre as 5 (cinco) organizações avaliadas, os profissionais que participaram da entrevista mencionaram que vários outros fatores são relevantes na produção diária de seus trabalhos, tal como a criação de diretrizes para a GCN e que seja aplicada para todas as áreas de negócio e que seu o cumprimento seja ***dever de todos,*** diretores, colaboradores, estagiários, aprendizes, terceiros e prestadores de serviços, da organização, que devem proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada, de tal forma a: assegurar que os recursos colocados à sua disposição sejam utilizados apenas para as finalidades aprovadas pela organização; garantir que as informações sob sua responsabilidade estejam adequadamente protegidas; cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual; atender as leis que regulamentam as atividades da organização e seu mercado de atuação; selecionar os mecanismos de segurança da informação, balanceando fatores de risco, tecnologia e custo.

Uma vez estabelecido as diretrizes implementar de forma corporativa: política de continuidade de negócios, de deve conter, mas não se limitando a: finalidade, escopo e usuários; objetivo da GCN; abrangência; principais produtos e serviços; responsabilidades da GCN; métricas e plano de comunicação. O engajamento de todos os colaboradores se dá com a disseminação da disciplina incluindo a GCN na cultura da organização, podendo ser através da mobilização, conscientização, treinamentos, aplicação cíclica de testes.

Continuando, os profissionais que responderam as entrevistas mencionaram que as organizações detêm um *site* alternativo, com posições de trabalho capacitadas com a infraestrutura tecnológica, variável de constructo, necessária para operacionalização dos negócios pelos colaboradores.
O grau de maturidade das organizações, dado a aplicação de políticas para continuidade de negócios e segurança da informação, disseminados em todos os níveis hierárquicos da organização, foi considerado alto. Tal ação possibilita o desenvolvimento de testes que validam toda a cadeia de processos de negócios considerados críticos da organização pelo time de gestão de risco, propiciando o tempo de resposta requerido no RTO – *Recovery Time Objetive* (Objetivo de Tempo de Recuperação), e a realização de *backups* de forma tempestiva e atendendo aos requisitos de RPO - *Recovery Point Objective* (Ponto Objetivado de Recuperação),

atendendo às expectativas dos acionistas no contorno de um evento de crise que pode variar desde pequenos eventos até os de grandes proporções.

A identificação dos processos de negócios considerados críticos e o mapeamento dos possíveis impactos financeiros, através do preenchimento do BIA, são encorajados pela GCN, que conta com a aplicação cíclica de testes de contingência para analisar e documentar os resultados obtidos, lições aprendidas, identificando oportunidades para a melhoria contínua. Portanto, é indiscutível o árduo preparo do time responsável pela GCN para promover análises e desenvolver estratégias para a manutenção do negócio, possíveis perdas financeira, pagamentos indevidos de multas, entre outros, evidenciando que a GCN é um centro de investimento e não de custos. (Guindani - 2011).

As organizações mantêm todos os seus treinamentos de forma integrada e corporativa onde todas as áreas de negócios são convocadas anualmente através de um programa de conscientização e mobilização. Toda e qualquer mudança significativa ocorrida nas áreas de negócios ou processos de negócios considerados críticos é levado em consideração e um novo teste deverá ser incluído no programa e ser realizado oportunamente.

5.2.2. Análise dos resultados

Ao se compilar os resultados das entrevistas juntos aos profissionais das 5 (cinco) organizações, e após o enquadramento e tabulação das respostas obtidas contatou-se:

O objetivo primário, a manutenção da organização ativa-operacional mesmo que em momentos de crise tornou-se evidente ao observar as respostas dos profissionais que de forma unanime, afirmaram que a Gestão de Crise desempenha um papel muito importante para alcançar os objetivos de negócios, ao passo que a GCN tem importância estratégica para todas as organizações respondentes exceto a organização_3. Na estratégia de negócio, a GCN se encaixa: para organização_1 como uma estrutura permanente que atua na gestão das crises, no intuito de proteger os colaboradores e o patrimônio da organização, evitando prejuízos financeiros e os

impactos negativos à imagem e reputação organizacional; para a organização_2 como uma disciplina principal para a gestão de riscos operacionais assim como segurança da informação, cibersegurança e gestão de terceiros; para a organização_3 como atendimento aos níveis de resiliência requeridos; para organização_4 na premissa de disponibilidade total; para organização_5 como a elaboração de estratégias para evitar a interrupção dessas operações com a confecção de planos.

Os profissionais afirmam que os principais “marcos”, para a GCN, foram e tem sido de forma corporativa, com iniciou no ano de 2005 e desde então a organização_1 desenvolveu modelos de atuação, políticas e treinou equipes para atuar em situações adversas, tendo hoje um modelo consolidado e permanente; já o mapeamento foi mencionado para organização_2; assim como adequação estratégica de PRD e aumento da complexidade dos testes; e criação de uma nova mentalidade foram citadas pelas organizações _3, _4 e _5, respectivamente.

Outro ponto importante a se analisar foi quando se questionou sobre as principais conquistas e desafios da GCN nas organizações. A resposta da organização_1 foi a criação de unidade específica para a gestão da GCN corporativa, implementação de política e orçamento específico e seu desafio foi manter as estruturas funcionais com capacitação das equipes; para organização_2 a cultura de Gestão de Risco Operacional; para a organização_3 processos simples e manutenção das estratégias de GCN; para a organização_4: uma área dedicada na governança de negócios de TI; e para a organização_5 foi implantar na totalidade todos os ciclos do PDCA.

Dentro da análise do constructo “longevidade, coordenação de parcerias, compreensão” entende-se que a proposição *“P2 - planejamento de crise pode ser executado por meio de: coordenação de parcerias, longevidade, compreensão”*, com destaque a variável cooperação e a participação de todas as equipes técnicas e de negócio que atuam desde o instante “t2”, momento em que pode ocorrer um evento, independentemente de seu grau de severidade. Este instante uma vez configurado dá início a todas as etapas apresentadas na figura 1 - *Framework* Síntese – GCN, desta dissertação onde a variável: de redução de recursos, e os constructos “tecnologia, negócio e pessoas”, presentes na proposição *“P3 – planejamento da crise depende da qualidade de recursos: pessoas, TI, negócios”* caminham em paralelo, cooperam

em verdadeiro sincronismo para que não haja sobreposição de atividades entre as equipes. Para que um planejamento seja realizado e documentado de forma realmente eficiente e eficaz, as atividades referentes à sua recuperação devem ser específicas, pois o planejamento da crise depende efetivamente da qualidade destes recursos, configurado nas equipes de negócios e técnicas.

Já o objetivo secundário: compreender se quanto mais a alta administração, estiver engajada melhor será a qualidade dos resultados/planejamento da crise; verificar se o planejamento de crise pode ser executado; identificar se o planejamento de crise depende da qualidade. Quando questionado sobre: a) sua organização possui uma equipe ou comitê de mudança que garanta que todas as atualizações feitas no ambiente de produção também sejam realizadas no *site* alternativo; b) a organização possui a revisão e a coleta dos resultados dos testes e prática de lições aprendidas; a resposta dos profissionais das 5 organizações foi única – "sim". Adicionalmente foi questionado se a organização possui processo de monitoração e manutenção da GCN e a resposta foi "sim" para todas as organizações exceto a organização_4 que respondeu que este processo está em desenvolvimento, vale a pena ressaltar que se trata do braço digital da organização_4. Outra pergunta realizada foi se a organização monitora seus *stakeholders* que podem influenciar GCN, e mais uma vez a resposta foi "sim" para todas as organizações exceto a organização_4 "não".

Dentro da análise dos constructos "liderança e propriedade, planejamento de crises" e das variáveis: proatividade; aprendizado; boa gestão humana; qualidade dos testes; qualidade da equipe de testes; simulação realizadas, entende-se que a proposição "P1 – quanto mais a alta administração estiver engajada melhor será a qualidade dos resultados, planejamento de crise" que neste caso ocorrem entre os momentos "t3" até "t5" é de fundamental importância que neste **"Δt"** (diferença entre "t5" e "t3") seja realizado tudo aquilo que foi "aprendido" durante o período de simulação e testes.

Durante o processo de entrevista ficou evidenciado nas entrelinhas das respostas dos entrevistados dois grandes fatores de integração, a primeira trata-se dos cenários de simulações e testes, da infraestrutura tecnológica, e o gerenciamento utilizado para gerar links e apoiar o trabalho comunicação entre as equipes de trabalho (técnica e negócios) com a equipe de GCN. A segunda, maior engajamento entre a equipe GCN

com a alta administração especialmente quando se fala dos “tempos de resposta” para a tomada de decisão que é fundamental para o negócio, lembrando que este tempo é regido pelo RTO definido junto aos gestores de negócios e com a aprovação pela alta administração.

5.3. Conclusão

Ter e manter uma equipe de GCN altamente treinada e qualificada traz para alta administração uma “tranquilidade” e é notório que muitas vezes a Alta Administração acredita que a manutenção da equipe é custo não enxergando o valor agregado que a equipe traz para o negócio.

Se coloca na posição de querer apenas ter a tomada de decisão “estratégica”, fazendo pequenos questionamentos e solicitando algumas explicações e, a partir daí decide sobre o tema apresentado. A contraindicação deste método é que isto traz de certa forma “algumas” autonomias para o Gestor GCN pois ele acaba assumindo e acelerando alguns temas que ele enxerga como relevantes e apenas apresentam seus resultados.

As organizações onde há profissionais com “alto conhecimento” e especialização em GCN conseguem interagir com maior nível de maturidade e atuar em harmonia com a Alta Administração demonstrando a necessidade de efetuar o que é solicitado pelos reguladores e ISO’s conquistando assim maior grau de maturidade.

Os reguladores, através da emissão de circulares, normativos e resolução, atingem com maior rapidez a Alta Administração pois caso não faça o que foi regulamentado sofrerá sanções severas o que pode culminar em altas multas ou até mesmo a perda da licença de funcionamento, ao passo que as ISO’s não têm sanções.

Os profissionais entrevistados evidenciaram alto conhecimento acadêmico e técnico, onde foi evidenciado pelos seus *curriculum* disponibilizados no aplicativo *linkedin*.
A Alta Administração tem conhecimento da capacidade destes profissionais/gestores na disciplina em si, também ficou evidenciado que há a necessidade de muita habilidade técnica para que haja a inclusão da GCN na estratégia das organizações!

Quando a organização_5 coloca que sua principal conquista e desafio na condução GCN foi implantar na totalidade todos os ciclos do PDCA, veja anexo C, reforça-se a importância de entender as necessidades da organização e a imprescindibilidade de estabelecimento de política e objetivos para a gestão de continuidade de negócios; implementar e operar controles e medidas para a gestão da capacidade geral da organização para gerenciar incidentes de interrupção; monitorar e analisar criticamente o desempenho e a eficácia do SGCN; e melhorar continuamente com base na medição objetiva; assim, podemos demonstrar a complexidade que está por traz desta resposta.

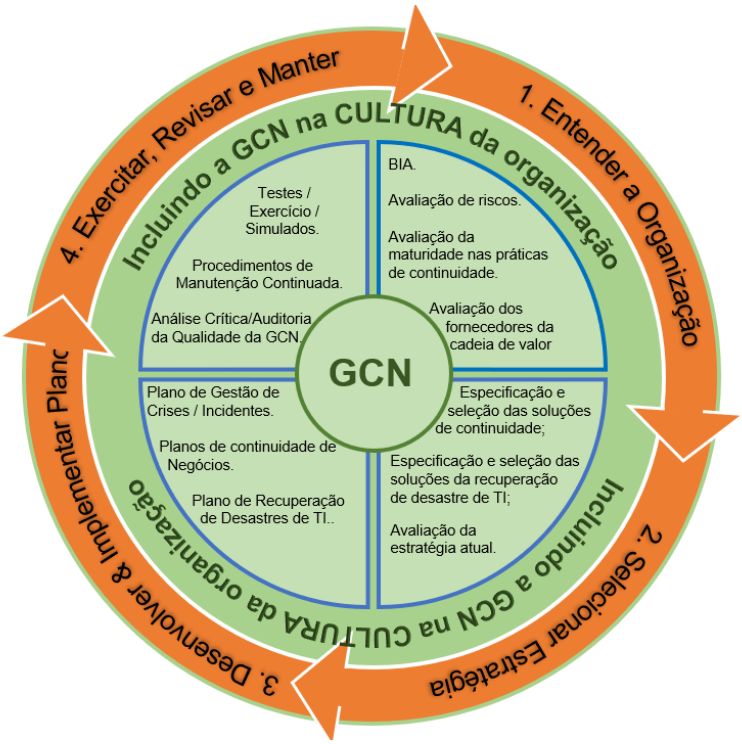


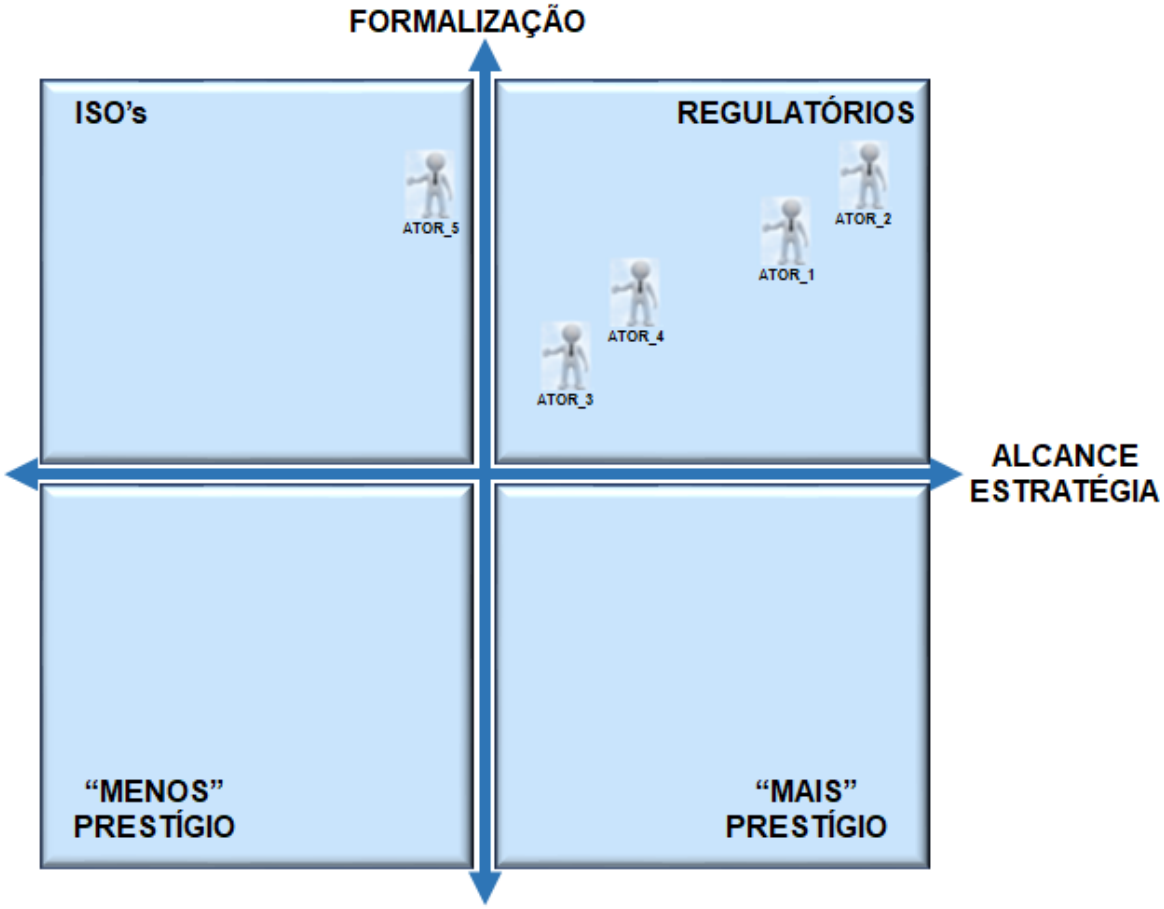
Figura 12 – GCN – Melhores práticas
Fonte: Brasiliano, adaptado pelo autor.

Note a importância e o grau de destaque que se dá para **"incluindo a GCN na cultura da organização"** com sendo o elo, a liga, o link, entre todas as micros atividades inerentes ao GCN, e as macros atividades intrínsecas do PDCA, onde podemos agregar entre outros, os anexos: anexo A – Tipos de ambiente Operacional; anexo B – Procedimentos e conceitos de Simulação e Testes; anexo C – Lei n° 13.709, de 14 de agosto de 2018; anexo E – Modelo de três linhas de Defesa; este último

promovendo a integração das áreas de negócios, com as áreas de governança corporativa e tornando a GCN plenamente auditável.

Após um estudo aprofundado das respostas dos 5 (cinco) respondentes, podemos responder a problematização, a contribuição social e a contribuição acadêmica. O framework a seguir é fruto deste trabalho onde no eixo “y” procuramos definir todo processo de formalização que o desenvolvimento de um GCN exige e no eixo “x” definimos quão importante deve ser o alcance de uma estratégia definida dentro da GCN. Vejamos:

Figura 13 – Framework – Engajamento Alta Administração



Fonte: Criado pelo autor. – Posicionamento dos Atores, visão do Autor.

Diante deste cenário e, conforme apresentado no quadro 4 - Matriz de Amarração, a contribuição social se dá pela execução da análise de como a indústria financeira no Brasil atua na gestão da continuidade de seus negócios e na sua capacidade de resposta em tempo adequado a eventos de alto impacto operacional. Assim,

consegue-se mitigar perdas potenciais em suas operações, sem que isso traga risco de liquidação financeira, ou de reputação ou de imagem para estas organizações, ou até mesmo um problema sistêmico, algo muito comum na década de 60, 70, 80 do século passado, mantendo um sistema financeiro resiliente e saudável para atender a sociedade brasileira, assegurando a estabilidade das transações bancárias no Brasil.

Por se tratar de uma pesquisa que envolve segurança da sociedade e descrição da abrangência da fundamentação teórica de Gestão de Continuidade de Negócios, que é composta por disciplinas como Segurança da Informação, Tecnologia da Informação, Governança Corporativa e Risco Operacional Corporativo, a proposta da pesquisa pode ser uma referência para outros trabalhos relacionados ao tema.

Assim, como descrito em nossa matriz de amarração e para concluir, nosso objeto de pesquisa, refere-se à gestão de continuidade de negócios das organizações da indústria financeira brasileira, conectando a utilização de controles e governança. Desta forma, prioriza-se a identificação de processos considerados críticos ao negócio, identificando-se ameaças significativas e planejando uma estratégia coordenada de resposta a um alto impacto operacional, assegurando uma efetiva e eficiente resposta diante um evento de crise, garantindo a sobrevivência (longevidade) da organização e o atendimento aos seus compromissos junto a clientes, reguladores e investidores mantendo a organização ativa-operacional.

A questão de pesquisa: *“GCN – sua organização “aceita” falar sobre este assunto? Proposta para uma ferramenta para autodiagnóstico organizacional.”* Se aplicado o framework - Engajamento Alta Administração proposta pode responder de forma afirmativa a este questionamento.

6. REFERÊNCIAS

Alevate, W Gestão de Risco e Gestão de continuidade de Negócio. 1ª ed. Rio de Janeiro, Elsevier, 2014

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO GUIA 73. 1: Gestão de riscos - Vocabulário. São Paulo, 11/2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO 15219. 1: Plano de emergência – Requisitos e procedimentos. São Paulo, 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR 15999. 1: Gestão de continuidade de negócios parte 1: Código de prática. São Paulo, 2007.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO 22301. 1: Segurança da Sociedade – Sistema de Gestão de continuidade de negócios – Requisitos. São Paulo, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO 31000:2018 Gestão de riscos – Diretrizes;

BANCO CENTRAL DO BRASIL. Circular nº 3380 de 23/03/2008. Dispõe sobre a implementação de estrutura de gerenciamento do risco operacional. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Circular&numero=3380 - Data da consulta: 25/04/2021.

BRITISH STANDARDS BS 25999-2. 1: Gestão de continuidade de negócios – Especificação. São Paulo, 2007.

COBIT 5 - Modelo Corporativo para Governança e Gestão de TI da Organização - ISBN 978-1-60420-284-7 Impresso nos Estados Unidos da América,

Coombs, W. T. (2001). Teaching the crisis management/communication course. Public Relations Review, 27(1), 89–101. https://doi.org/10.1016/S0363-8111(01)00072-8

Coombs, W. T. (2007). Protecting Organization Reputations During a Crisis: The Development and Application of Situational Crisis Communication Theory. Corporate Reputation Review, 10(3), 163–176. https://doi.org/10.1057/palgrave.crr.1550049

Coombs, W. T. (2010). Ongoing Crisis Communication: Planning, Managing, and Responding. Crisis, 53(2), 174–178.

Coombs, W. T. (2015a). Ongoing Crisis Communication (4th ed.) Retrieved from https://books.google.pt/books?hl=ptPT&lr=&id=CkkXBAAAQBAJ&oi=fnd&pg=PR1&dq=Coombs,+W.T.,+2015.+Ongoin+Crisis+Communication,+4th+ed.+Sage,+Thousand+Oaks,+CA&ots=NHB84gmk9b&ig=iOipi2NbBzOqsldcF7wXfgmy9KA&redir_esc=y#v=onepage&q&f=false

Coombs, W. T. (2015b). The value of communication during a crisis: Insights from strategic communication research. Business Horizons, 58(2), 141–148. https://doi.org/10.1016/j.bushor.2014.10.003

Coombs, W. T., & Holladay, J. S. (2012). The para crisis: The challenges created by publicly managing crisis prevention. Public Relations Review, 38(3), 408–415. https://doi.org/10.1016/j.pubrev.2012.04.004 Coombs, W. T., & Holladay, S. J. (2002). Helping crisis managers protect reputational assets: Initial Tests of the Situational Crisis Communication Theory. Management Communication Quarterly, 16(2), 165–186. https://doi.org/10.1177/089331802237233

Coombs, W. T., & Laufer, D. f(2018). Global Crisis Management – Current Research and Future Directions. Journal of International Management, 24(3), 199–203. https://doi.org/10.1016/j.intman.2017.12.003

CUMMINGS, M; HAAG, S.; MCCUBREY, D. J. Management Information Systems for the Information Age. McGraw-Hill Companies, Inc., 2005, 592 p.
cumming

Computerworld from IDG https://www.computerworld.com/about/about.html - Data de acesso 19/02/2021

DRII - Disaster Recovery Institute International, Falls Church, Virginia, Phone: (703) 538-1792, URL http://www.dri.org/ - Data de acesso 09/06/2004.

DRJ - Disaster Recovery Journal, PO Box 510110, St. Louis, MO 63151, (314) 894-0276, (314) 894-7474-Fax, Street Address, 11131 E. South Towne Sq. St. Louis, MO 63123

DRUCKER, P. *Desafios gerenciais para o século XXI*. São Paulo: Pioneira, 1999.

FEBRABAN. *X Congresso e Exposição de Tecnologia da Informação das Instituições Financeiras*, Brasil, 2000.

FEBRABAN. *XII Congresso e Exposição de Tecnologia da Informação das Instituições Financeiras*, Brasil, 2002.]

GARTNER GROUP. Acessado em maio de 2021. http://www.gartner.com/technology/about.jsp.

GUINDANI, Alexandre. Deus é brasileiro – O Guia da Gestão da Continuidade dos Negócios. Rio de Janeiro: Ed. Ciência Moderna ltda., 2011.

GUINDANI, Alexandre. Gestão da Continuidade dos Negócios. Revista de Pós-graduação da União Pioneira da Integração Social–Faculdades Integradas (UPIS), v. 1, 2008.

GOODE, W.; HATT, P. Metodologias em pesquisa social. 7.ed. São Paulo: Nacional, 1979.

HAGUETTE, T.M.F. Metodologias qualitativas na sociologia. 4ª ed. Petrópolis: Vozes 1995.

ISO/IEC – CD 25002. Systems and software engineering, 2019.

ISO 22300:2018 Security and resilience — Vocabulary.

LARA, F.; PERDÓMO, J.; JIMÉNEZ, J. I*nforme sobre el desarrollo y tendencias de la tecnologia en la industria de servicios financieros en America Latina*. Bogotá: FELABAN, 1999.

LEWIS, G. Organizacional Crisis Management: The Humam Factor. Boca Raton: Auerbach Publications, 2006.

LÜDKE, M.; ANDRÉ, M. Pesquisa em educação: abordagens qualitativas. São Paulo: EPU, 1986.

LUNA, Jairo Nogueira. O PARADIGMA HOLOGRÁFICO NUM SONETO DE GREGÓRIO DE MATOS.

LUECKE, R. Gerenciando a Crise: dominando a arte de prevenir desastres. Rio de Janeiro: Record, 2007.

Matos, Gregório de Poemas / Gregório de Matos; biografia, vocabulário, comentários, bibliografia por Leticia Malard; Belo Horizonte; 96p – (Literatura literária, 1) ISBN 85-86583-11-1; Autêntica editora: Rua Tabelião Ferreira de Carvalho, 584, CEP 31170-180 – Belo Horizonte – MG - 1998

Matos, Gregório de,
www.uoc.edu/in3/hermeneia/sala_de_lectura/ackmar_luiz_gregorio_matos.htm

MINAYO, M.C. de S. O desafio do conhecimento: pesquisa qualitativa em saúde 3.ed. São Paulo: Hucitec/Abrasco, 1994.

Mitroff, I.I. Shrivastava, P. e Udwadia, F.E. Effective Crisis Management. Academy of Management. 1987.

SILVA, Aldo. **Gestão de Continuidade de Negócios.** 2010. Disponível em: http://securityofficer.wordpress.com/2010/07/28/gestao-de-continuidade-de-negocios. Acesso em julho 2015.

SILVA, Elizabeth B. Política empresarial de controle da força de trabalho: rotatividade como dominação. São Paulo, 1981. Dissertação (Mestrado) – Faculdade de Filosofia, Letras e Ciências Humanas, Universidade de São Paulo (na época, a autora assinava como Elizabeth Silva Sztuman).

SIQUEIRA, Marcelo Costa. Gestão Estratégica da Informação. Rio de Janeiro: Brasport, 2005.

Shrivastava, A; Somasundaram, G. “Armazenamento e Gerenciamento de Informações”, Bookman, 2009.

TRIVIÑOS, A.N.S. Introdução à pesquisa em ciências sociais: a pesquisa qualitativa em educação. São Paulo: Atlas, 1987.

Global Technology Audit Guide - 2008

Jornal do Comércio do Ceará – Artigo publicado em 29/09/2020.

The Good Practice Guidelines (Manual de Boas Práticas) do BCI – Business Continuity Institute disponível em (https://www.thebci.org/product/good-practice-guidelines-2018-edition—download.html)

WHEATMAN, Vic. Aftermath: disaster recovery. **Gartner Research, AV-14-5238,** setembro de, 2001.

APENDICE

ANEXO A - Tipos de Ambiente Operacional

Dados Importantes – Ambientes

Ambiente de desenvolvimento: ambiente disponível para os times de tecnologia, que deve ser uma réplica fiel de todo o ambiente tecnológico de produção, constando assim que todas as especificações exatas existentes, como no ambiente de produção, sirvam para que os times e equipes de desenvolvimento possam aplicar as mudanças, sem que isso crie impactos para os clientes e para os usuários de negócio. Trata-se de um ambiente seguro, em que os times de desenvolvimento possam executar alterações, sem passar por nenhum processo, fluxo ou revisão de grupos terceiros, para simular o comportamento das mudanças antes de aplicá-las nos ambientes produtivos, evitando possíveis comportamentos que impactem a produção.

Ambiente de Teste e Aceite de Usuário: é toda a infraestrutura onde o **teste** será executado, compreendendo configurações de hardware, software, ferramentas de automação, equipe envolvida, aspectos organizacionais, suprimentos, rede e documentação.

Ambiente de Homologação: É o ambiente de testes, onde pode ser emitido Nota Fiscal Eletrônica (NFe), Conhecimento de Transporte Eletrônico (CTe), Manifesto Eletrônico de Documentos Fiscais (MDFE), entre outros documentos fiscais eletrônicos, sem nenhuma validade fiscal ou jurídica, podendo também usar dados reais ou fictícios no preenchimento do documento. Esse ambiente também é utilizado para testar ajustes de sistemas, como em casos em que há alteração do tipo de regime ou tributação da empresa, onde então o documento é emitido sem valor fiscal para verificar se, quando for gerado de verdade, sairá com as informações corretas. O ambiente de homologação pode ser usado pelas empresas a qualquer momento, sempre que preciso, entretanto, a empresa deve estar credenciada juntamente à SEFAZ do estado para realizar este tipo de emissão. Vale lembrar que documentos fiscais emitidos em ambiente de homologação não podem ser consultados no portal da NFe ou CTe da SEFAZ. A consulta ao CTe ou NFe completa está disponível apenas para os documentos emitidos em ambiente de Produção, que vamos detalhar a seguir.

Ambiente de Produção: é o ambiente designado para documentos com valor fiscal, ou seja, são documentos válidos e reconhecidos fiscal e juridicamente. A forma de emissão dos documentos fiscais eletrônicos é idêntica, tanto em produção quanto em homologação, possuindo as mesmas regras, diferenciando apenas a validade fiscal de cada um destes documentos. Em alguns estados, é exigido uma quantidade mínima de emissão de documentos em ambiente de homologação, para que então seja liberada a emissão em Produção.
Existe um boato de que não é possível usar o mesmo certificado digital para emitir documentos fiscais eletrônicos nos dois ambientes. É importante frisar que essa informação não procede. Não há nenhum trecho em manuais ou na legislação que embase este rumor. Portanto, o emissor pode estar em ambiente de produção e realizar testes em homologação sem nenhum problema. É importante ressaltar

também que em hipótese alguma a mercadoria pode ser transportada com NFe, CTe, MDFe, ou demais documentos fiscais eletrônicos emitidos em ambiente de homologação.
O único ambiente aceito pela fiscalização é o de Produção, por isso, é necessário estar sempre atento na hora de emitir o documento.

Ambiente de Contingência: este ambiente considera uma réplica de todos os ambientes críticos da empresa. A gestão de mudança possui um papel crucial no aumento do nível de governança de gestão de risco operacional e na gestão de continuidade de negócios, pois, durante o processo de manobra de “virada” do ambiente de tecnologia de produção, para que seja realizada a ativação do ambiente de contingência, é preciso que todas as versões existentes no ambiente de produção sejam exatamente as mesmas que o ambiente de contingência. Sem que esse comitê garanta que as mudanças submetidas estejam refletindo as mesmas mudanças no ambiente de UAT, que será descrito abaixo, o ambiente de contingência da submissão da solicitação de mudança passa a reprovar a aprovação de seguir em frente com a submissão do processo de atualização.
Fonte: Desenvolvido pelo autor.

ANEXO B - Procedimentos e Conceitos de Simulação e Testes.

Introdução

A efetividade do GCN será alcançada quando estiver claro para todos os colaboradores o que é esperado deles na ocorrência de um evento. Isso só poderá ser alcançado com um ciclo consistente de treinamentos, simulações e testes.

Deve começar de modo simples e progressivamente aumentar em sua complexidade, baseando-se na experiência obtida anteriormente. Esta abordagem é a chamada de bloco de construção. Há três propósitos que devemos buscar:

- **Validar** – avaliar a eficácia dos procedimentos e do acesso aos recursos e identificar oportunidades de melhorias com a depuração do plano;
- **Treinar** – desenvolver competências e habilidades dos membros das equipes, mostrando qual é o papel e responsabilidade de cada um. No momento do acionamento do GCN poderá não haver tempo suficiente para ler todo o plano. Todos já deverão estar preparados para a ação. Um real comprometimento de todos dará credibilidade ao PCN.
- **Testar** – executar os procedimentos previstos e torná-los de conhecimento do maior número de colaboradores, para que em possível ativação do GCN, as ações necessárias e programadas sejam executadas naturalmente, sem transtornos.

Objetivo Geral

Estabelecer uma metodologia para o planejamento e execução de Simulação e Testes dos planos envolvidos na GCN, atividades a serem realizadas e um fluxo a ser seguido.

Objetivo Específico

Definir um conjunto de ações que permitam avaliar a capacidade que o Plano de GCN tem de responder cabalmente aos requisitos de desempenho pré-definidos.

É admissível que o plano não possa ser simulado e/ou testado em todos os seus componentes.

Contudo as simulações e os testes a serem realizados devem dar um grau de segurança suficiente de que os procedimentos para ativar os planos de GCN irão resolver com sucesso os eventuais problemas causados pelo evento.

Os Planos de Simulação e Testes devem:

- Prever a expectativa mínima na área de teste e simulação;
- Coordenar, planejar, avaliar e validar a simulação e o teste de um plano documentado;
- Definir objetivos, políticas, diretrizes, responsabilidades e as especificações de simulação e teste.
- Estabelecer e coordenar a simulação e teste de forma apropriada.

Abrangência

Aplicável a todas as equipes da Organização.

Responsabilidades

Cabe a Organização, em conjunto, a responsabilidade pelo aprimoramento contínuo deste documento, revisando-o com periodicidade anual.

Regras e Conceitos

Conscientização

Programas de treinamento e conscientização da recuperação de desastres têm o potencial de agregar valor para toda a Organização. Um programa efetivo de treinamento e conscientização está correlacionado com a habilidade da Organização em se recuperar de forma efetiva depois de uma crise ou desastre, assegurando a recuperação dentro dos tempos pré-definidos.

Treinamento

É um processo educacional nos quais as equipes e os colaboradores são preparados e qualificados sobre os seus papéis e responsabilidades na implementação / execução do GCN.

Simulação

Está associado a um processo de melhoria do plano aperfeiçoando as ações pré-estabelecidas e corrigindo as possíveis distorções encontradas.

Teste

São atividades realizadas para avaliar a eficiência e a eficácia ou a capacidade de um plano em relação aos objetivos especificados ou critérios de medição. Teste geralmente envolve exercícios destinados a manter as equipes de colaboradores eficazes em suas funções e para revelar fraquezas no GCN que deverão ser corrigidas. O Teste está associado a uma avaliação, a uma nota qualitativa ou quantitativa.

Programado

Dizemos que a Simulação ou Teste é programado quando ele está previsto num calendário anual de planejamento de Exercícios e Testes e é de conhecimento de todos.

Não Programado

É quando a Simulação ou Teste é programado junto com o Principal Gestor da Dependência o qual autoriza a sua execução e indica o melhor período, sem que os demais colaboradores fiquem sabendo. O efeito surpresa é o grande fator para avaliação do conhecimento do plano por parte das pessoas envolvidas e a sua organização na execução.

Teste de Mesa (tabletop)

Um método de ensaio que apresenta uma simulação limitada de um cenário de crise em um formato de narrativa na qual os participantes discutem, mas não executam a política, métodos, procedimentos, a coordenação e as atribuições de recursos associados com a ativação do plano. Os participantes discutem as ações que tomariam baseados nos seus planos, mas as ações não são efetivamente realizadas. O teste pode ser realizado com uma única equipe, ou múltiplas equipes, geralmente sob a orientação de facilitadores.

Nota: Por exemplo, os membros da equipe de recuperação/restauração se encontram em uma sala de reunião, pré-definida, para discutir a definição de suas responsabilidades e como eles reagiriam a emergências, seguindo o plano. Às vezes é referido como um teste passo a passo estruturado.

Teste Passo-a-Passo (Walkthrough)

Os membros das equipes seguem passo a passo o plano para identificar e corrigir pontos fracos, fazendo uma revisão dos procedimentos. As equipes desempenham suas funções percorrendo o conteúdo do plano, sem realmente dar início aos procedimentos de recuperação/restauração. Exemplo.: Árvore de Acionamento.

Nota: Deve envolver representantes de cada uma das áreas funcionais para rever o plano a fim de determinar se os planos relativos à sua área são precisos e completos, podem ser utilizados, quando necessário.

Teste de Notificação – (Árvore de Acionamento)

É um processo estruturado em cascata, que permite que uma lista de pessoas, funções e / ou organizações a serem contatadas, como parte de um plano de informação ou procedimento de chamada. É utilizado para notificar os colaboradores designados como membros da equipe de recuperação/restauração, utilizando a lista de contatos conforme documentado no plano. Constitui num dos meios mais eficientes e eficazes de comunicar alguma notícia ou instruções a todos os colaboradores, incluindo toda a organização.

Teste Integrado

É um teste realizado em vários componentes de um plano, em conjunto com os outros, geralmente em condições de operação simulada.

Envolve a integração de um número de componentes, seguindo a ordem em que elas ocorrem durante as operações efetivas de recuperação/restauração.

Teste integrado baseia-se em sucessos de testes e crescente conscientização dos colaboradores gerados durante os testes de componentes.

Simulação

É o processo pelo quais os membros da equipe de recuperação/restauração realizarão todas as ações que tomariam no caso da ativação do plano. Pode envolver uma ou mais das equipes de recuperação e são realizados em condições que, pelo menos, simulem os desastres.

Teste de Simulação Parcial

É semelhante ao teste de simulação total exceto que apenas a algumas unidades de negócios estarão envolvidas. Contudo, para estas unidades, o teste terá maior detalhe e abrangência.

Teste de Simulação total

É o derradeiro teste de GCN que ativa o plano de PCN total.

Nota: O objetivo é simultaneamente um ensaio de tantos componentes quanto possível na estrutura de recuperação/restauração da Organização. O teste é susceptível de ser caro e

pode “atrapalhar” as operações normais e, portanto, deve ser abordado com cautela. Deve ser agendada o momento adequado para o teste. A diferença significativa entre um teste “vivo” é que ele não exige que o *Site* e os sistemas sejam interrompidos. Um teste no qual os participantes executam algumas ou todas as ações que tomariam no caso de ativação do plano. Exercícios de simulação são realizados em condições o mais próximo possível as condições do "mundo real".

Teste de Interrupção Total

É um exercício em que todos os procedimentos e as estratégias de Recuperação - Restauração são testados. Ele realmente é uma réplica de uma catástrofe, interrompendo toda a produção.

Nota: Esta é o mais extenso de Teste Plano do PCN.

Teste de Componentes

É uma série de testes que incidem sobre os diversos componentes de um plano de PCN. Exemplos de testes de componentes inclui:

- Confirmar a Disponibilidade / Versão do Plano;
- Obter cópia dos registros vitais armazenados fora do Site;
- Contatar Colaboradores, Fornecedores e Outros;
- Verificar o prazo de entrega dos equipamentos críticos;
- Verificar se as Listas importantes estão atualizadas;
- Confirmar o preparo do *Site* Alternativo;
- Testar o Conhecimento das Equipes;
- Trazer de volta os dados armazenados no *Site* Alternativo;

Teste - Checklist

É uma revisão pela equipe sobre o plano para assegurar que os componentes-chaves do plano estão atualizados, disponíveis ou completo.

Nota: O Teste de Checklist (Lista de verificação) é um método utilizado para testar um PCN – Plano de Continuidade de Negócios por completo.

Exemplo: o plano é distribuído e comentado pelas unidades de negócio, inclusive TI, para garantir a precisão do seu conteúdo, rigor e eficácia.

Teste e Exercício de Participação

Várias equipes da própria organização, bem como do setor público, parceiros e provedores, podem participar dos testes.

Nota: Antes de viabilizar a participação consulte normas e regulamentos internos e externos.

Planejamento

Exercícios e testes podem variar muito em custo, tamanho, escopo, complexidade, propósito e abordagem. Vários tipos podem ser realizados. A escolha de qual tipo de simulação ou teste a ser

usado, dependerá muito do nível de maturidade da área de negócio. O plano de simulação e teste do PCN deve ser (**S.M.A.R.T.**):

- E**S**pecífico - delimitado/foco/restrito;
- **M**ensurável - deve ser possível de medição;
- **A**lcançável – ter os recursos e condições para atingir o objetivo;
- **R**ealista – mais próximo possível da realidade da Organização;
- **T**empestivos - data, tempo e situação de testes onde as simulações e os testes serão efetuados.

Específico

O estabelecimento de metas e expectativas serve para avaliar objetivamente se o plano estabelecido responderá satisfatoriamente a certos eventos de crise e como ela pode ser melhorada.

Objetivos

- Definir quais áreas e equipes serão envolvidas;
- Qual fase será testada - (Prevenção, Resposta, Recuperação, Reinício, Restauração);
- Certificar se a área poderá continuar operando, independente dos eventos de interrupção que possam ocorrer;
- Garantir que a comunicação durante um evento de contingência, seja realizada de forma eficiente e eficaz;
- Validar as medidas tomadas de contenção local para situações não emergenciais e definir/validar a infraestrutura necessária para a recuperação/restauração no Site alternativo;
- Validar a contingência planejada para cada um dos processos críticos;
- Treinar e educar os membros da equipe, bem como a todos os colaboradores, validando e aperfeiçoando os planos.

Escopo

- Todos os processos críticos, devem ser simulados, testados e constar no Plano;
- Não deverão contemplar as áreas de suporte que não tenham impacto direto ao negócio. Mas não deixar de forma alguma de incluir áreas suportadas e/ou afetadas pelos processos críticos contemplados nesta mesma simulação e teste;
- O teste e simulação devem estar baseados única e exclusivamente nas informações contidas na última versão do PCN;
- Todo o suporte necessário deve ser previamente identificado e listado em procedimentos;
- O objetivo é garantir que cada simulação e teste se torne mais complexo ao longo do tempo.
- No princípio, as simulações e os testes devem começar relativamente simples, tornando-se cada vez mais complexos conforme evolução do processo;
- No início os testes podem incluir listas de verificação, exercícios simples e pequenos componentes dos Planos. Com o tempo e o amadurecimento, os testes devem tornar-se cada vez mais complexos, até uma escala de ativação integral do PCN, incluindo a participação externa, órgãos públicos de segurança e emergência.

- Os processos manuais podem ser testados e simulados no dia a dia, mas devem ser devidamente documentados a fim de evidenciá-los e validá-los.
- Os funcionários e/ou colaboradores participantes dos grupos de simulações e testes devem ser previamente identificados.

Métodos de Simulação e Teste

Esses métodos incluem exercícios tanto para a recuperação de negócios e a recuperação de desastres.

- Exercícios de recuperação de negócios concentram-se sobretudo sobre as operações de teste dos processos de negócios;
- Exercícios de recuperação de desastres estão focados em testar a continuidade dos componentes da tecnologia, incluindo sistemas, redes, aplicações e dados;

Podem variar do simples ao complexo, dependendo da preparação e recursos necessários. Cada um tem suas próprias características, objetivos e benefícios. O tipo ou combinação de métodos de ensaio empregado para a Organização deve ser determinado, entre outras coisas, pela experiência de planejamento de recuperação de desastres, o tamanho, a complexidade e a natureza do seu negócio.

Mensurável

- As simulações e os testes devem ser elaborados de forma que seu êxito possa ser medido após a conclusão, quantitativamente ou qualitativamente;
- O volume a ser testado e/ou simulado deve considerar a capacidade de processamento de um dia normal de trabalho; envolvendo diferentes produtos, fornecedores, sistemas e processos.

Alcançável

Ter os recursos e condições para atingir o objetivo:

- quem é o responsável para chamar, planejar e coordenar as simulações e os testes;
- observadores “independentes” do teste - os nomes de quaisquer observadores “independente” que observarão a conduta das simulações e dos testes;
- observadores “internos” do teste – nomes de quaisquer observadores de outras áreas/equipes de negócio onde há uma interface a eles;
- participantes - os nomes dos participantes necessários para executar as simulações e os testes;
- Recursos necessários: transporte, alimentação.

Realista

Simulações e testes devem ser baseados nos cenários previamente identificados e documentados nos planos que reflitam situações reais e factíveis.

Cenário

É uma descrição de circunstâncias dentro de que os testes são colocados em prática, cobrindo o desastre ou falha que ocorreu e a extensão de estrago, indisponibilidade de serviço, ausência do pessoal etc. O que é possível de ser simulado ou testado?

- Aplicações e Sistemas;

- Componentes de Infraestrutura
- Rede, comunicações e telecomunicações;
- Internet
- E-mail;
- Processos de Negócios;
- Papéis e responsabilidades das Equipes, Líderes e Membros

Tempestivos

- data, tempo e a situação de onde as simulações e os testes serão executadas;
- duração planejada das simulações e dos testes de modo que participantes possam programar sua participação com seus outros deveres;

Ciclo de Exercícios e Testes

O planejamento de Simulação e Testes devem contemplar diferentes níveis de teste para ser realizado nos seus componentes. É importante notar que as simulações e os testes de recuperação/restauração de desastres são diferentes de testes de continuidade de negócios. O Planejamento de simulação e/ou testes devem ser avaliados e modificados conforme necessário. Devem ser dinâmicos, tendo em conta as mudanças para o PCN, a rotatividade de pessoal, os incidentes reais, e os resultados de exercícios anteriores.

Executar

Uma explicação inicial feita pelo Coordenador PCN deve preceder simulação e/ou teste, definindo as razões e objetivos, os cenários e seus alcances, as regras de conduta, e os papéis dos participantes que estarão presentes.

O responsável pela simulação e/ou teste deve administrar o ambiente de teste, permitindo que a área/equipe de negócios execute os testes reais enquanto ele assegura que a simulação e/ou testes são empreendidos de acordo com os scripts, contando apenas com os recursos previamente definidos e disponíveis no local.

Caso necessário, o Coordenador PCN da simulação e/ou teste pode e deve agir como o papel de instrutor, com o intuito de treinar a equipe. Da mesma forma, se o gerente de teste está ciente de uma deficiência no GCN sob simulação e/ou teste ele pode guiar a equipe a descobrir esta deficiência. (p.ex. perguntar como uma ação particular pode ser alcançada se não existe nenhum passo correspondente no plano).

Durante a simulação e/ou teste, se necessário, o gerente de teste pode introduzir “acontecimentos” imprevistos visando testar a capacidade de reação da equipe para lidar com mudanças de acontecimentos.

Monitoramento da Simulação e Teste

Observadores deverão ser designados com a atribuição de documentar uma lista cronológica dos acontecimentos durante a simulação e o teste. Deve tomar notas durante o ensaio de todas as dificuldades, problemas, deficiências que aparecerem durante todo o procedimento.

Avaliar

O Responsável deve conduzir uma reunião formal de revisão do teste com os observadores e o pessoal envolvido nas simulações e nos testes, com a data, hora e local como indicado no Planejamento original da Simulação e Teste. Deve considerar se os objetivos determinados foram alcançados: quaisquer problemas, omissões, deficiências etc. encontrado pelo pessoal de Simulação, Teste e observadores.

Após a conclusão, o resultado do Planejamento deve ser criticamente avaliado.

A avaliação deve incluir, entre outras coisas, uma avaliação:

- Qual o nível que as metas e objetivos da simulação e do teste foram alcançados;
- A eficácia da participação das equipes / colaboradores;
- Funcionalidade da execução dos Planos como planejado no caso de um evento real;
- As simulações e testes somente poderão ser considerados “concluídos com êxito”, se todos os procedimentos definidos vierem a ser concluídos sem falhas;
- Todas as falhas identificadas devem ser acompanhadas pelo “Responsável”, que por sua vez, deverá comunicar todo o acompanhamento da Equipe de Gerencial;
- Avaliar, atualizar e informar a gerência executiva sobre os resultados do exercício;
- Identificar quais as partes do PCN não puderam ser simuladas/testadas e as eventuais consequências daí resultantes.

Agir

Deve ser criado após a finalização de cada simulação e teste realizado, um Plano de Ação contendo:

- **Documento de Lições aprendidas**

  Descrever as conclusões na conduta e eficácia das simulações e dos testes, os problemas e deficiências mais importantes. Tal documento deve fazer parte da documentação de evidência das simulações e testes. Este documento deve ser utilizado como entrada para as simulações e testes seguintes.
- **Plano de Ação**

  Todas as falhas identificadas durante as simulações e testes, devem ser avaliadas e um plano de ação deve ser elaborado com o propósito de corrigir estas irregularidades e os Planos atualizados.

Caso alguma falha identificada ou mudança no ambiente ou outros fatores que afetem a viabilidade do plano, seja considerada grave, um novo teste e/ou simulação deve ser realizado em tempo oportuno a ser definido pela Equipe Gerencial.

Simulações e Testes futuros, bem como os Planos, devem então ser modificados conforme a necessidade, com base nos resultados da simulação e/ou teste.

Procedimentos

- **Calendário**

  Um cronograma anual definindo as datas nas quais o plano e seus componentes serão simulados e/ou testados devem ser estabelecidos.

  Esse cronograma deverá ser enviado para a Equipe Gerencial para que esta possa acompanhar.
- **Frequência**

Durante o desenvolvimento inicial do DRP Mainframe, simulações e testes devem ser um processo interativo até que o plano seja julgado e considerado plenamente pronto para uso.

Uma vez que o plano está adequado, mais simulações e testes devem ocorrer assim que ocorram mudanças significativas nas operações de negócio ou na infraestrutura de ativos e serviços de suporte (IT, voz etc.) e/ou no próprio plano.

Os recursos necessários para tais simulações e/ou testes dependerão da extensão de mudança.

De todo modo, simulações e/ou testes periódicos devem acontecer para assegurar que o plano permanece em linha com os requisitos de negócios e da Organização.

Sistemas Envolvidos

Os planos atualizados devem estar disponíveis em um diretório único defino em conjunto entre as equipes de gerenciamento.

Evidências para Auditoria

Treinamentos, Simulações e/ou Testes deverão ter uma lista com os dados e assinatura dos participantes, a qual deverá permanecer devidamente documentada junto aos resultados de Simulações e testes da Organização.

Durante a realização das simulações/testes devem ser coletadas evidências que possam comprovar a sua realização, local data, hora e atividade realizada.

Todo este material deverá permanecer sob guarda do Equipe Gerencial.

Relacionamentos

Papéis e Responsabilidades

Existem várias funções, papéis e responsabilidades que os participantes das simulações e testes podem desempenhar. Todos os participantes devem compreender seus papéis no exercício, e o exercício deve envolver todos os participantes.

Como parte das simulações e/ou testes, os participantes devem ter a possibilidade de interagir e discutir as questões e lições aprendidas.

Facilitador

Supervisiona a simulação e teste. Possui um conhecimento global na direção do cenário.

Monitora a sequência dos eventos, ajusta o ritmo, e controla a linha do tempo.

Controlador

Introduz estímulos artificiais com a orientação do facilitador. Atua como uma extensão do facilitador.

Toma decisões em caso de ações não previstas ou recursos necessários.

Ajuda a eliminar problemas de segurança e danos à propriedade para manter a ordem, bem como monitorar e auxiliar as ações dos participantes.

Simulador

Adiciona realismo à encenação do cenário.

Retrata os particulares das empresas, organismos e organizações que, normalmente, interagem com os colaboradores.
Atua como vítima, o adversário, membro da mídia, e qualquer outra função adicional que precisa ser preenchido.

Observador
Colaborador estrategicamente posicionado para monitorar, observar e documentar, cronologicamente os acontecimentos e o desempenho da simulação e do teste. Deve ser informado sobre o assunto ou função que está sendo avaliada. Valida as ações dos participantes e da eficácia do PCN.

Participantes
Assumir papéis de crise e realizar atividades reais ou simuladas compatível com o tipo de exercício e o cenário a ser utilizado.

Responsável
Manter o GCN da Organização atualizado, simulado, testado e documentado de acordo com as políticas e normas da Organização em tempo oportuno e aceitável.

- Promover;
- Coordenar a simulação e testes de recuperação/restauração para seus respectivos grupos de testes;
- Manter documentadas evidências de simulações e testes, bem como qualquer documento que possa evidenciar atividades desenvolvidas com relação ao DRP.
- Informar a gerência executiva sobre os resultados do exercício;

Auditoria
A Auditoria deverá ser convidada, e seu envolvimento será facultativo, a participar dos testes e simulações a fim de verificar a aderência das atividades de GCN da Organização.

Área de TI
Certificação Anual, a fim de garantir a efetividade do GCN, sob responsabilidade da Organização, fica definido o processo de simulação e testes conforme abaixo:

- Anualmente efetuará simulação e teste integrado a fim de validar a efetividade do GCN;
- Caso seja identificado algum problema que inviabilize a validação do Plano, o mesmo deverá ser corrigido num período não superior a 30 dias, a partir da data de detecção.

ANEXO C – O modelo “Plan-Do-Check-Act” – (PDCA)

C. Introdução

C1. Visão Geral

Esta Norma especifica requisitos para estabelecer e gerenciar um eficaz Sistema Gestão de Continuidade de Negócios (SGCN).

Um SGCN reforça a importância de:

a) entender as necessidades da organização e a imprescindibilidade de estabelecimento de política e objetivos para a gestão de continuidade de negócios;
b) implementar e operar controles e medidas para a gestão da capacidade geral da organização para gerenciar incidentes de interrupção;
c) monitorar e analisar criticamente o desempenho e a eficácia do SGCN; e
d) melhorar continuamente com base na medição objetiva.

O SGCN, assim como outros sistemas de gestão, possui os seguintes componentes-chave:

a) uma política;
b) pessoa com responsabilidade definidas;
c) pessoas de gestão relativos a: política; planejamento; implementação e operação; avaliação de desempenho; análise crítica pela Direção; e, melhorias.
d) Documentação fornecendo evidências auditáveis; e
e) Quaisquer processos de gestão de continuidade de negócios pertinentes à organização.

A continuidade de negócios contribui para uma sociedade mais resiliente. É possível que seja necessário envolver no processo de recuperação a comunidade em geral, assim como outras organizações em função do impacto no ambiente organizacional.

C2. O modelo “Plan-Do-Check-Act” (PDCA)

Esta Norma adota o modelo “Plan-Do-Check-Act” para planejar, estabelecer, implantar, operar, monitorar, analisar criticamente, manter e melhorar continuamente a eficácia do SGCN de uma organização.

Isto garante um grau de consciência com outras normas de sistemas de gestão, tais como a ABNT NBR ISO 9001:2000 (Sistema de gestão da qualidade) e ABNT NBR ISO 14001:2004 (Sistema de gestão ambiental), ABNT NBR ISO/IEC 27001:2005 (Gestão de serviços de TI), e ABNT NBR ISO 28000 (Especificação para sistemas de gestão de segurança para cadeia logística), suportando assim, a implementação consistente e integrada e a operação com sistemas de gestão relacionados.

A Figura 14 ilustra como o SGCN considera com entradas as partes interessadas e os requisitos de continuidade de negócios e, por meio de ações necessárias e processos, produz resultados de continuidade (por exemplo, continuidade de negócios gerenciada) que atendem aqueles requisitos.

Figura 14 – Modelo PDCA aplicado aos processos do SGCN
Fonte: ABNT NBR ISO 22301:2013 – Adaptado pelo autor.

A continuidade de negócios contribui para uma sociedade mais resiliente. É possível que seja necessário envolver no processo de recuperação a continuidade em geral, assim como outras organizações em função do impacto no ambiente organizacional.

Tabela 2 – Explicação do modelo PDCA

Plan (Estabelecer)	Estabelecer uma política de continuidade de negócios, objetivos, metas, controles, processos e procedimentos pertinentes para a melhoria da continuidade de negócios de forma a ter resultados alinhados com os objetivos e políticas geral da organização;
Do (Implementar e operar)	Implementar e operar a política de continuidade de negócios, controles, processos e procedimentos;
Check (monitorar e analisar criticamente0	Monitorar e analisar criticamente o desempenho em relação aos objetivos e política de continuidade de negócios, reportar os resultados para a direção para análise crítica, e definir e autorizar ações de melhorias e correções;
Act (Manter e melhorar)	Manter e melhorar o SGCN tomando ações corretivas e preventivas, baseadas nos resultados da análise crítica pela Direção e reavaliando escopo do SGCN e as políticas e objetivos de continuidade de negócios.

C3. Componentes do PDCA nesta norma

No modelo “Plan (Planejar) -Do (Fazer) – Check (Checar) – Act (Agir)” exibido na Tabela 2, as Seções 4 a 10 desta norma envolvem os seguintes componentes:

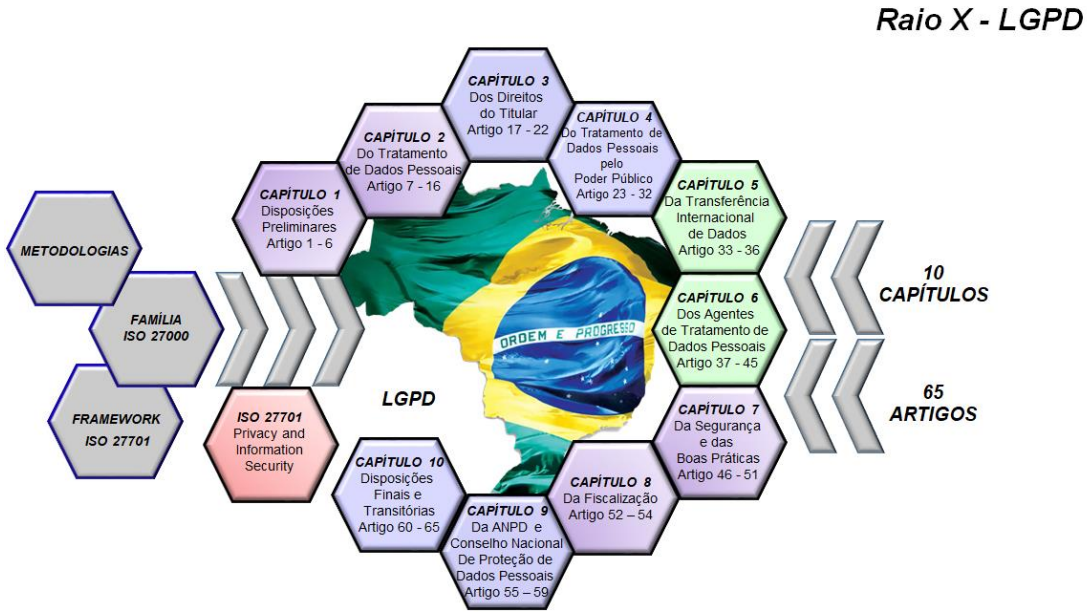
- A Seção 4 é um componente do "Planejar". Introduz os requisitos necessários para estabelecer o contexto do SGCN, como se aplica na organização, bem como suas necessidades, requisitos e escopo;
- A Seção 5 é um componente do “Planejar”. Resume os requisitos específicos para o papel da Alta Direção no SGCN e como a liderança deve articular suas expectativas para a organização por meio de uma declaração ele política;
- A Seção 6 é um componente do “Planejar”. Descreve os requisitos para a aplicação de objetivos estratégicos e princípios direcionadores para o SGCN como um todo. O conteúdo da Seção 6 difere do estabelecimento de oportunidades para o tratamento de riscos decorrentes do processo de avaliação de risco, bem como dos objetivos de recuperação derivado da análise de impacto nos negócios (BIA);

  NOTA: Os requisitos dos processos de análise de impacto nos negócios e de avaliação de riscos estão detalhados na Seção 8.

- A Seção 7 é um componente do “Planejar”. Suporta a operação do SGCN, atribuindo competências e comunicação de forma recorrente/conforme necessária com as partes interessadas, bem como documentando, controlando., mantendo e retendo as documentações necessárias;
- A Seção 8 é um componente do "Fazer". Define requisitos para a continuidade de negócios, determinando como abordá-los e como desenvolver procedimentos para gerenciar um incidente de interrupção;
- A Seção 9 é um componente do "Checar”. Resume os requisitos necessário para medir o desempenho da gestão de continuidade de negócios, a conformidade do SCGN com esta Norma e com as expectativas da Direção e busca o feedback dos gestores com relação às expectativas;
- A Seção 10 é um componente do "Agir". Identifica e atua em aspectos do SGCN que não estão em conformidade através de ações corretivas;

ANEXO D - LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.

Figura 15 – Raio X - LGPD



Fonte: Elaborado pelo autor

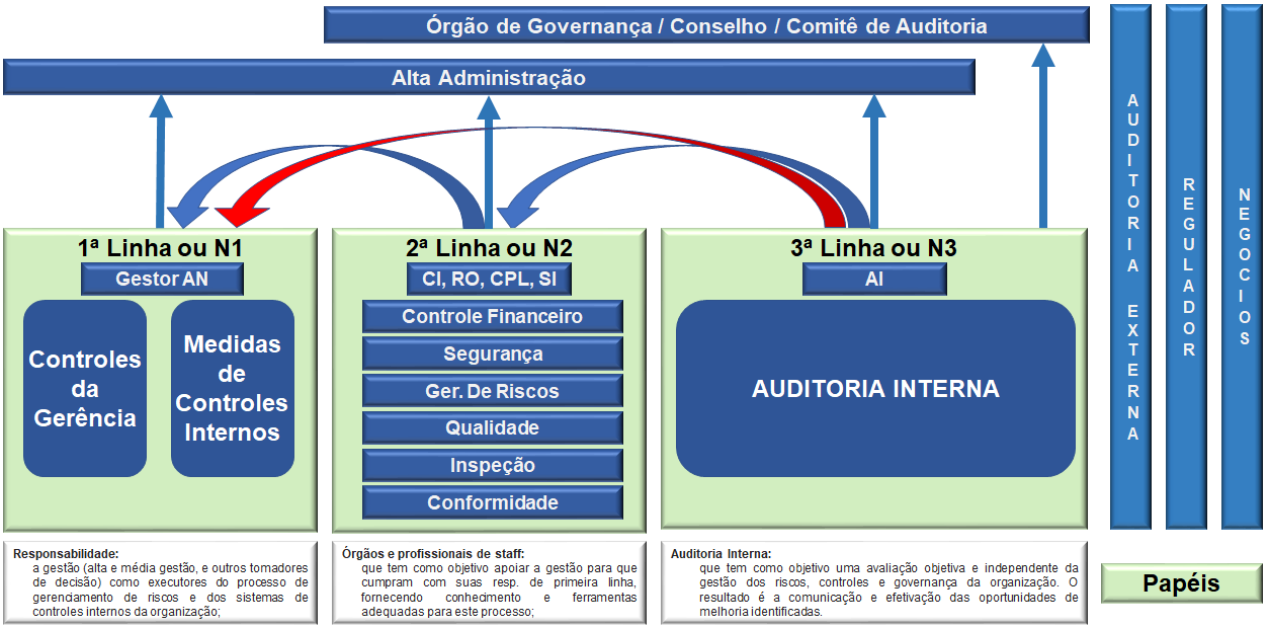
Figura 16 – Visão Geral - LGPD

Fonte: Elaborado pelo autor

Nota importante: Consulte a LEI Nº 13.709, DE 14 DE AGOSTO DE 2018, para tomar ciência de seu teor.

ANEXO E – Modelo de três linhas de Defesa.

Figura 17 – Modelo de três linhas de Defesa



Fonte: Adaptado pelo autor.