FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"

Curso Superior de Tecnologia em Segurança da Informação

Hugo Leonardo Pajanoto

Planejamento de Gestão de Continuidade de Negócios

Visando aplicações em pequenas ou médias empresa

Americana, SP

2024

FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"

Curso Superior de Tecnologia em Segurança da Informação

Hugo Leonardo Pajanoto

Planejamento de Gestão de Continuidade de Negócios

Visando aplicações em pequenas ou médias empresa

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação da Professora MARIA CRISTANA ARANDA

Área de concentração: Segurança da Informação.

Americana, SP.

2024

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana Ministro Ralph Biasi-CEETEPS Dados Internacionais de Catalogação-na-fonte

PAJANOTO, Hugo Leonardo

Planejamento de gestão de continuidade de negócios visando aplicações em pequenas ou médias empresa. / Hugo Leonardo Pajanoto – Americana, 2024.

40f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientadora: Profa. Dra. Maria Cristina Aranda

1. Restauração 2. Segurança em sistemas de informação 3. Sistemas de informação. I. PAJANOTO, Hugo Leonardo II. ARANDA, Maria Cristina III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 7.06
681.518.5
681518

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

Planejamento de Gestão de Continuidade de Negócios

Visando aplicações em pequenas ou médias empresa

Trabalho de Conclusão de Curso apresentado a CEETEPS/Faculdade de Tecnologia – FATEC/ Americana como requisito parcial à obtenção do título de título de Tecnólogo em Segurança da Informação.

Americana, 20 de junho de 2024.

Banca Examinadora:

Maria Cristina Aranda
Doutorado em Engenharia Mecânica
Fatec Americana Ministro "Ralph Biasi"

Wagner Siqueira Cavalcante
Mestrado em Ciência da Computação
Fatec Americana Ministro "Ralph Biasi"

Diógenes de Oliveira
Mestrado em Engenharia de Produção
Fatec Americana Ministro "Ralph Biasi"

Americana, SP.

2024

DEDICATÓRIA

Dedico este trabalho às pequenas e médias empresas, cuja resiliência diante dos desafios inspira este estudo sobre gestão de continuidade de negócios. Que os *insights* aqui apresentados possam fortalecer suas operações e contribuir para seu sucesso. Esta dedicação se estende aos empreendedores, gestores e colaboradores dessas empresas, assim como à minha família, amigos e colegas, cujo apoio foi fundamental para a conclusão deste trabalho.

AGRADECIMENTOS

Agradeço primeiramente a Deus, fonte de toda sabedoria e inspiração, pela força e discernimento concedidos durante toda a jornada de elaboração deste trabalho. A minha orientadora, Maria Cristina Aranda, pela dedicação, orientação precisa e com valiosas dicas ao longo do desenvolvimento deste trabalho. Suas orientações foram essenciais para a condução desta pesquisa. À minha família, pelo amor incondicional, apoio constante e compreensão nos momentos de ausência durante a elaboração deste trabalho. Aos amigos e demais pessoas que, de alguma forma, contribuíram para a realização deste estudo. À FATEC de Americana, pela oportunidade de aprendizado e pelo suporte oferecido ao longo do curso. Por fim, agradeço a todos que, de alguma maneira, colaboraram para a realização deste trabalho.

RESUMO

O estudo de caso apresentado neste trabalho demonstra a importância da implementação de um Plano de Continuidade de Negócios (PCN) para pequenas e médias empresas (PMEs) do setor de serviços. O PCN é uma ferramenta fundamental para garantir a resiliência das empresas diante de disrupções causadas por eventos como ataques cibernéticos, falhas de equipamentos, desastres naturais e interrupções no fornecimento de energia. O estudo de caso da Serviços Integrados Ltda. ilustra os benefícios de sua implementação, incluindo a redução do risco de interrupções nas operações, a melhora da resiliência operacional, o aumento da confiança dos clientes e a redução de custos. A empresa também notou a importância de testar e atualizar regularmente o PCN para garantir sua efetividade. O estudo contribuiu para a literatura sobre gestão de continuidade de negócios ao apresentar um exemplo prático da implementação de um PCN em uma PME. Os resultados do estudo podem ser úteis para outras PMEs que buscam implementar um PCN para garantir a continuidade de suas operações.

Palavras-Chave: Plano de Continuidade de Negócios; Gestão de Riscos; Resiliência Operacional.

ABSTRACT

The case study presented in this paper demonstrates the importance of implementing a Business Continuity Plan (BCP) for small and medium-sized enterprises (SMEs) in the service sector. The BCP is a key tool to ensure the resilience of companies in the face of disruptions caused by events such as cyberattacks, equipment failures, natural disasters, and power supply disruptions. The case study of Serviços Integradas Ltda. illustrates the benefits of its implementation, including reducing the risk of disruptions to operations, improving operational resilience, increasing customer confidence, and reducing costs. The company also noted the importance of regularly testing and updating the BCP to ensure its effectiveness. The study contributed to the literature on business continuity management by presenting a practical example of the implementation of a BCP in an SME. The results of the study may be useful for other SMEs looking to implement a BCP to ensure the continuity of their operations.

Keywords: *Business Continuity Plan; Risk Management; Operational Resilience.*

.

SUMÁRIO

1. INTRODUÇÃO

A segurança da informação é um pilar fundamental para a proteção dos ativos digitais de uma organização. No cenário atual, em que empresas dependem cada vez mais de sistemas online, servidores externos e dados sensíveis, garantir a integridade, confidencialidade e disponibilidade dessas informações é crucial.

Por outro lado, a continuidade de negócios visa manter as operações funcionando mesmo em situações adversas, como desastres naturais, falhas de hardware ou ataques cibernéticos. É como um gerador elétrico em um hospital, que entra em ação quando a rede elétrica falha, mantendo o mínimo funcionando até que o sistema seja restabelecido.

Neste capítulo, exploraremos como a segurança da informação e a continuidade de negócios estão intrinsecamente ligadas. Veremos como estratégias de proteção de dados, políticas de acesso, monitoramento e resposta a incidentes contribuem para a resiliência das organizações diante de ameaças. Além disso, discutiremos as etapas essenciais para elaborar um Plano de Continuidade de Negócios (PCN) que garanta a operação contínua mesmo em cenários críticos.

O plano de continuidade de negócios (PCN) é um conjunto de medidas e procedimentos que visam garantir a continuidade das operações críticas de uma organização em caso de eventos adversos, como desastres naturais, ataques cibernéticos, falhas de equipamentos, entre outros. O PCN é essencial para a segurança da informação e a resiliência organizacional, pois permite a recuperação rápida e eficiente dos recursos de TI e dos processos de negócio, minimizando os impactos financeiros, operacionais e reputacionais.

No entanto, muitas pequenas e médias empresas (PMEs) não possuem um PCN adequado ou sequer o conhecem, o que as torna mais vulneráveis e suscetíveis a interrupções e perdas. Isso se deve, em parte, à falta de conscientização, de recursos e de capacitação sobre o tema, bem como à complexidade e à diversidade dos cenários de risco que as PMEs enfrentam.

Diante desse contexto, este trabalho tem como objetivo geral analisar a importância e os benefícios do PCN para as PMEs, bem como propor um modelo simplificado e adaptado de PCN para esse segmento. Os objetivos específicos são:

Identificar os principais riscos e ameaças que afetam as PMEs no âmbito da segurança da informação;

Levantar as melhores práticas e as normas internacionais sobre o PCN;

Desenvolver um modelo de PCN para as PMEs, considerando as suas características e necessidades específicas;

Aplicar e avaliar o modelo proposto em um estudo de caso de uma PME do setor de serviços.

A hipótese deste trabalho é que o PCN é um diferencial competitivo e estratégico para as PMEs, pois aumenta a sua capacidade de resposta e de recuperação diante de situações de crise, além de contribuir para a melhoria da gestão de riscos e da qualidade dos serviços prestados.

De acordo com a pesquisa da CETIC.br em 2021 (GETSCHKO at al, 2021), após um crescimento de 28,8% de empresas que venderam pela Internet no período da pandemia de COVID-19, ocorreu um aumento na demanda das empresas atuais em relação a sua disponibilidade na Internet, nesse período de 2019 a 2021 tornou-se necessário armazenar e processar uma grande quantidade de dados, e informações. Esse fato para muitos tipos de organizações passou a ser considerada o coração do negócio. Visto a importância para a continuidade de um negócio ter seus dados armazenados de forma segura, tem-se por necessidade medidas de segurança robustas. Isso inclui o uso de tecnologias de segurança da informação.

Embora os desastres na história recente tenham aumentado a conscientização sobre os riscos de Gestão de Continuidade de Negócios (GCN) e seu impacto nas finanças e operações, há empresas que não atendem aos sinais de alerta e não se preparam para desastres ou interrupções em seus negócios. Interrupções naturais ou provocadas pelo homem podem ser imprevisíveis, mas seus impactos podem ser gerenciados se um programa eficaz de GCN fizer parte de uma estrutura geral de governança corporativa (EVEREST et al., 2008).

Nesse sentido, é fundamental que as empresas estejam preparadas para lidar com essas situações e minimizar o impacto em suas operações. Para isso, é necessário que elas desenvolvam um plano de continuidade de negócios abrangente e eficaz, que possa ser acionado em caso de necessidade. Esse plano deve incluir medidas para mitigar os efeitos dos riscos e permitir que a empresa continue operando mesmo em situações adversas.

Considerando possíveis problemas como o mencionado acima, o presente estudo tem a finalidade de conhecer a importância de se ter um plano de continuidade de negócios para empresas. Identificar as principais relevâncias que devem ser consideradas no momento da composição de um plano de gestão de crise. Deste

modo criando um ambiente a fim de simular um cenário computacional empresarial de pequeno porte.

Certamente, a pandemia de COVID-19 acelerou a digitalização das empresas em todo o mundo, trazendo uma série de desafios relacionados à segurança da informação e privacidade dos dados. Com a necessidade de distanciamento social e fechamento de estabelecimentos, as empresas precisaram se adaptar rapidamente para atender às demandas dos clientes através de canais digitais. Isso exigiu uma grande mudança cultural e organizacional para muitas empresas, que precisaram reestruturar seus processos internos para permitir uma maior flexibilidade e mobilidade no ambiente de trabalho.

De acordo com a pesquisa da consultoria EY (2021), a pandemia de COVID-19 também levou a um aumento significativo nos ataques cibernéticos contra empresas em todo o mundo. Com a rápida escalada da digitalização, muitas empresas foram pegas desprevenidas e não tinham os controles de segurança necessários para lidar com a crescente ameaça.

As empresas precisaram reestruturar seus processos internos e implementar soluções de segurança adicionais para garantir a proteção dos dados de seus clientes e colaboradores. Além disso, as empresas precisaram garantir uma comunicação segura e eficaz com seus clientes, especialmente quando se trata de transações financeiras.

No entanto, essa rápida escalada na digitalização também trouxe consigo riscos significativos de segurança da informação. A transição para o ambiente digital expôs as empresas a uma série de ameaças, incluindo phishing (roubo de dados através de e-mails fraudulentos), malware (sistema malicioso projetado para prejudicar ou explorar qualquer dispositivo, serviço ou rede programável), ataques de ransomware (sequestro de dados e pedido de resgate para sua devolução) e outras formas de ataques cibernéticos. Muitas empresas não estavam preparadas para lidar com esses tipos de ameaças, o que aumentou o risco de ataques bem-sucedidos.

Além dos riscos cibernéticos, a digitalização rápida durante a pandemia também trouxe à tona questões relacionadas à privacidade dos dados dos clientes e colaboradores das empresas. Com o aumento do número de transações online e o armazenamento de dados sensíveis em nuvens, foi necessário garantir a proteção e privacidade desses dados. As organizações precisaram implementar soluções de segurança adicionais e controles rigorosos para garantir a proteção dos dados.

Um estudo realizado pela Kaspersky, uma empresa de segurança, revelou que o número de ataques cibernéticos contra empresas no Brasil aumentou 20% durante a pandemia. Os ataques mais comuns foram *phishing* e *ransomware* (KASPERSKY, 2021).

Para enfrentar esses desafios, as empresas tiveram que adotar uma abordagem mais proativa em relação à segurança cibernética. Isso inclui a implementação de soluções de segurança adicionais, como autenticação de dois fatores e criptografia de dados, e a realização de treinamentos para seus colaboradores sobre as melhores práticas de segurança cibernética.

1. SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação (SI) é um campo fundamental para as organizações no mundo digital de hoje. Ela envolve a proteção da informação contra uma variedade de ameaças, como ataques cibernéticos, perda de dados e acesso não autorizado. A informação é um ativo estratégico que precisa ser preservado para garantir a continuidade dos negócios, a proteção da reputação e a conformidade com as leis e regulamentações.

A norma internacional ABNT NBR ISO/IEC 27001:2023 (ABNT, 2023), reconhecida como o padrão líder em gestão da segurança da informação, define SI como:

- **Confidencialidade:** A informação deve ser acessível apenas para pessoas autorizadas.
- **Integridade:** A informação deve ser completa e precisa, sem alterações não autorizadas.
- **Disponibilidade:** A informação deve estar acessível quando necessário para aqueles que precisam dela.

A ISO 27001 estabelece 14 princípios fundamentais para a gestão da SI, que orientam as organizações na implementação de práticas eficazes:

- Confidencialidade
- Integridade
- Disponibilidade
- Responsabilidade
- Tomada de decisão informada
- Foco no cliente
- Adaptabilidade e flexibilidade
- Abordagem abrangente
- Equilíbrio entre segurança e outras necessidades
- Melhoria contínua
- Conformidade com as leis e regulamentações

- Promoção de uma cultura de segurança da informação
- Suporte da alta gerência
- Monitoramento e avaliação

1.1. SISTEMA DE GESTÃO DE CONTINUIDADE DE NEGOCIOS (SGCN)

A norma ABNT NBR ISO/IEC 22313:2020 (ABNT, 2020) define um Sistema de Gestão da Continuidade de Negócios (SGCN) como um conjunto de políticas, procedimentos, processos e recursos organizacionais para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a capacidade de continuidade de negócios dentro de uma organização. Segundo Sêmola (2003) o principal objetivo de um SGCN é garantir que as organizações possam responder efetivamente a incidentes, interrupções ou crises, minimizando o impacto negativo e permitindo a rápida retomada de operações críticas.

> Definir um SGCN requer uma série de etapas, como na ISO27001, incluindo o planejamento de como a organização fará a gestão dos seus processos de continuidade, o estabelecimento de uma política de gestão da continuidade, e, pelas etapas de análise de impactos no negócio, a definição de estratégias de contingência e construção dos planos de contingência propriamente ditos, que devem ser elaborados com o claro objetivo de contingenciar situações e incidentes de segurança que não puderem ser evitados. Devem ser eficazes como o paraquedas de reserva o é em momento de falha do principal, garantindo, apesar do susto, a vida do paraquedista em queda. (Sêmola, 2003, p.98)

O primeiro aspecto crítico de um SGCN é a definição de políticas e objetivos de continuidade de negócios, alinhados com os requisitos e a estratégia da organização. Essas políticas estabelecem uma direção clara e fornecem uma estrutura para orientar as ações necessárias durante uma interrupção. As metas são estabelecidas para garantir que a organização atinja o nível adequado de resiliência e recuperação.

Em seguida, o SGCN envolve a implementação de processos para identificar, analisar e avaliar os riscos que podem impactar a continuidade dos negócios. Isso inclui a análise de impacto nos negócios, que identifica as funções e processos críticos, e a avaliação de riscos, que identifica as ameaças e vulnerabilidades associadas a essas funções e processos.

Outro componente essencial é o desenvolvimento de estratégias de continuidade de negócios, que incluem medidas preventivas, mitigação de riscos e planos de resposta a incidentes. Essas estratégias visam reduzir a probabilidade e o impacto de interrupções, além de fornecer orientações claras sobre como a organização deve responder em diferentes cenários de crise.

A implementação do SGCN requer a designação de papéis e responsabilidades claras, garantindo que as pessoas certas estejam envolvidas na gestão da continuidade de negócios. Isso inclui a nomeação de um responsável pela continuidade de negócios, a criação de equipes de resposta a incidentes e a definição de comunicações eficazes durante uma interrupção.

Uma parte fundamental do SGCN é o estabelecimento de planos de continuidade de negócios (PCN) documentados. Esses planos descrevem as ações a serem tomadas em cada fase de uma interrupção, incluindo a ativação dos planos, a implementação das estratégias definidas e a coordenação das atividades de recuperação. Os planos também devem abordar a restauração dos processos de negócios e a recuperação da infraestrutura tecnológica.

Além disso, a norma ABNT NBR ISO/IEC 22313:2020 (ABNT, 2020), enfatiza a importância da realização de testes, exercícios e treinamentos regulares para garantir que o sistema esteja atualizado e funcional. Isso inclui a avaliação da eficácia dos planos, a identificação de lacunas e a implementação de melhorias contínuas para fortalecer a resiliência organizacional.

O SGCN requer o monitoramento e revisão contínua do desempenho do sistema, bem como a realização de auditorias internas e avaliações de conformidade. Isso garante que o processo esteja alinhado com as mudanças internas e externas na organização, mantendo-se atualizado e eficaz para enfrentar novos desafios e ameaças.

A implementação do SGCN nas organizações pode fortalecer sua resiliência, proteger seus ativos e garantir a continuidade dos negócios em face de incidentes e crises.

1.2. PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN)

O objetivo de um Plano de Continuidade de Negócio é garantir a continuidade de processos e informações vitais à sobrevivência da empresa,

no menor espaço de tempo possível, com o propósito de minimizar os impactos do desastre, ou seja, contingenciar situações e incidentes de segurança que não puderam ser evitados.

Segundo Sêmola (2003, p. 102):

> Esse documento tem o propósito de definir os procedimentos para contingenciamento dos ativos que suportam cada processo de negócio, objetivando reduzir o tempo de indisponibilidade e, consequentemente, os impactos potenciais ao negócio. Orientaras ações diante da queda de uma conexão à Internet exemplifica os desafios organizados pelo plano.

O PCN é uma estratégia que visa garantir que a empresa possa continuar operando de forma eficaz em caso de interrupções inesperadas ou desastres, como incêndios, inundações, interrupções no fornecimento de energia elétrica ou problemas de segurança cibernética.

De acordo com a DRI International (DRII, 2021) e o Disaster Recovery Journal (2021), um Plano de Continuidade de Negócios (PCN) é um conjunto de processos, procedimentos e ações projetados para garantir a continuidade das atividades de uma organização no caso de uma interrupção não planejada, como um desastre natural, falha de equipamento, ataque cibernético etc. O objetivo do PCN é minimizar o impacto dessas interrupções nas operações da empresa e garantir que a empresa possa continuar entregando produtos ou serviços com eficiência aos clientes, mesmo em situações de crise.

As origens dos PCNs remontam à década de 1980, quando grandes corporações começaram a se preocupar com a possibilidade de paralisação de seus sistemas de tecnologia da informação. Com o tempo, o conceito de PCN se expandiu para incluir não apenas a tecnologia da informação, mas todos os aspectos-chave dos negócios de uma organização. Hoje, o PCN é considerado uma parte essencial do gerenciamento de riscos corporativos (IBM, 2020).

A norma ABNT NBR ISO/IEC 22301:2019 (ABNT, 2019) é um padrão internacional para estabelecer requisitos para um *Business Continuity Management System* (BCMS) ou em português Sistema de Gerenciamento de Continuidade de Negócios (SGCN). O objetivo desta norma é ajudar as organizações a estabelecer, implementar, manter e melhorar um sistema de gestão de continuidade de Negócios (SGCN) eficaz. A norma fornece orientação para identificar os principais processos de uma organização, avaliar riscos, definir

estratégias de resposta e recuperação, treinar e conscientizar os funcionários e testar planos regularmente para garantir sua eficácia.

Um PCN eficaz deve considerar uma ampla gama de riscos potenciais, incluindo desastres naturais, falta de energia, ataques cibernéticos, sabotagem, greves e muito mais. Além disso, deve ser desenvolvido de forma colaborativa, envolvendo os principais *stakeholders* da organização, como gestores, colaboradores, fornecedores e clientes.

Segundo a empresa IBM Services (IBM, 2020), os PCN devem ser parte integrante da cultura organizacional, exigindo o comprometimento da alta direção e a participação de todos os colaboradores. Deve ser testado e atualizado regularmente para garantir sua eficácia. Um PCN eficaz ajuda a minimizar o impacto das interrupções nas operações de negócios, garante a continuidade dos negócios, protege a reputação de uma organização e garante a satisfação do cliente.

A ABNT NBR ISO/IEC 22301:2019 (ABNT, 2019) define os requisitos para um sistema de gerenciamento de continuidade de negócios e fornece orientação para identificar os principais processos de uma organização, avaliar riscos, definir estratégias de resposta e recuperação, treinamento e conscientização de pessoal e testar regularmente o plano para garantir sua eficácia. Um PCN é considerado uma parte essencial do gerenciamento de riscos corporativos e deve ser desenvolvido em conjunto pelas principais partes interessadas da empresa e testado e atualizado regularmente para garantir sua eficácia.

1.3. ANÁLISE DE IMPACTO NO NEGÓCIO

Segundo David Everest o *Business Impact Analyse* (BIA) ou em português Analise de Impacto nos negócios é usado para identificar processos críticos de negócios que precisem ser recuperados após um evento de desastre. O BIA pode incluir uma discussão inicial sobre as soluções de recuperação necessárias para retomar os processos críticos de negócios. Os participantes da BIA devem incluir funcionários da empresa, bem como principais fornecedores. A análise deve ser realizada com o conhecimento da avaliação de risco de continuidade de negócios que define os eventos críveis que poderiam prejudicar o negócio. Normalmente, as entrevistas de BIA são realizadas individualmente para cada equipe. Então,

ocorrem discussões com outras equipes identificadas como prestadoras críticas após cada reunião da BIA (EVEREST *et al*.,2008).

Segundo Sêmola (2003, p. 102), o BIA, sendo a primeira etapa, é fundamental por fornecer informações para o perfeito dimensionamento das demais fases de construção do plano de continuidade.

De acordo com os autores, o objetivo do BIA é identificar e avaliar o grau de relevância dos processos e atividades que compõem o escopo da contingência, levando em consideração a continuidade das operações empresariais. Nesse contexto, é necessário realizar um levantamento detalhado dos processos e atividades críticas para a organização.

Uma vez identificados os processos críticos, o próximo passo é mapear os ativos físicos, tecnológicos e humanos que são necessários para suportar cada um desses processos. Esse mapeamento é necessário para compreender quais recursos são indispensáveis para a execução adequada das atividades e para identificar potenciais vulnerabilidades e pontos de falha. Com base nessa análise, é possível apurar os impactos quantitativos que poderiam ser gerados em caso de paralisação total ou parcial dos processos críticos. Essa avaliação quantitativa permite estimar os prejuízos financeiros, operacionais e estratégicos que a empresa poderia enfrentar diante de interrupções não planejadas.

Ao aplicar a BIA, conforme proposto por Sêmola (2003), as organizações podem obter uma compreensão abrangente dos riscos envolvidos em suas operações e estabelecer medidas de contingência adequadas. Dessa forma, é possível desenvolver planos de continuidade de negócios eficientes, que considerem a proteção dos ativos críticos, a minimização de impactos e a rápida recuperação após eventos disruptivos. A BIA é, portanto, uma ferramenta valiosa para garantir a resiliência e a sustentabilidade das organizações em um ambiente de negócios cada vez mais desafiador.

1.4. PLANOS DE CONTINGÊNCIA

O objetivo de um Plano de Contingência de acordo com a norma ABNT NBR ISO/IEC 22313:2020 (ABNT, 2020), é assegurar que uma organização possa continuar operando ou restaurar rapidamente as operações após ter sido afetada por um incidente cibernético.

Segundo Marcos Sêmola os planos de contingência,

> São desenvolvidos para cada ameaça considerada em cada um dos processos do negócio pertencente ao escopo, definindo em detalhes os procedimentos a serem executados em estado de contingência. (SÊMOLA, 2003, p.103)

A implementação de novas tecnologias e ideias inovadoras pode gerar economia para as grandes corporações. Para isso, é importante quantificar corretamente os dados e levantamentos do projeto, considerando as tecnologias apropriadas para cada tipo de contingência e a possibilidade de migração de serviços críticos e instáveis para opções melhores e mais atualizadas.

Um plano de contingência deve levar em conta diversos fatores. De acordo com o Instituto de Informática (1999), alguns passos devem ser seguidos:

- **Avaliar os impactos no negócio:** Identificar os processos críticos e avaliar o impacto que a falha de cada um deles representa para a organização, considerando as interdependências entre eles.
- **Identificar riscos e definir cenários de falha:** Identificar os riscos associados a cada processo crítico e definir cenários possíveis de falha, levando em conta a probabilidade, duração dos efeitos, consequências, custos e limites aceitáveis para a falha.
- **Identificar medidas de contingência:** Listar as medidas a serem tomadas caso a falha ocorra, incluindo o contato com a imprensa, se necessário.
- **Definir ações operacionais:** Estabelecer as ações necessárias para implementar as medidas de contingência, considerando recursos físicos e humanos que possam ser adquiridos.
- **Estimar custos:** Avaliar os custos de cada medida de contingência e compará-los com os custos incorridos caso a contingência não exista.
- **Estabelecer monitoramento pós-falha:** Definir a forma de monitorar a situação após a ocorrência da falha.
- **Definir critérios de ativação do plano:** Estabelecer critérios para determinar quando o plano de contingência deve ser ativado, como o tempo máximo aceitável de duração da falha.
- **Identificar responsáveis:** Identificar quem é responsável por ativar o plano de contingência, geralmente alguém em um alto nível hierárquico da empresa. Além disso, atribuir responsabilidades específicas para a

implementação das medidas de contingência, incluindo substitutos designados para cada responsável.

- **Definir a recuperação do negócio:** Estabelecer o processo de retorno ao estado normal de operação após a contingência, incluindo responsáveis pelas ações e monitoramento do processo de recuperação.

1.5. METODOLOGIA ISO/IEC 22301PARA GESTÃO DE CONTINUIDADE DE NEGÓCIOS

A ABNT NBR ISO/IEC 22301:2019 (ABNT, 2019) é uma norma internacional que estabelece requisitos para a implementação de um sistema de gestão de continuidade de negócios em organizações de todos os tipos e tamanhos. O objetivo é garantir que a empresa esteja preparada para enfrentar interrupções em suas operações e possa se recuperar rapidamente após um incidente disruptivo.

Essa norma estabelece um conjunto de requisitos para o planejamento, implementação, monitoramento e revisão do sistema de gestão de continuidade de negócios. Entre esses requisitos está a identificação dos processos críticos da empresa, a avaliação dos riscos e ameaças potenciais, a definição de planos de contingência e a realização de testes e exercícios de simulação de desastres.

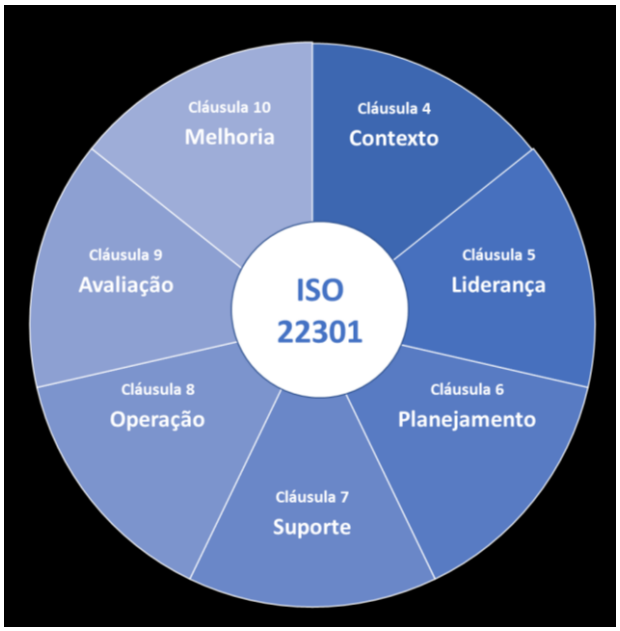
O padrão ABNT NBR ISO/IEC 22301:2019 (ABNT, 2019) pode trazer benefícios significativos para o planejamento de continuidade de negócios, independentemente de a organização buscar ou não a certificação formal dessa norma. Embora a certificação seja uma validação valiosa, não uma exigência.

Para começar, é possível criar um sólido plano de continuidade de negócios com algumas etapas simples, disponíveis no guia de início rápido da norma, que pode ser facilmente baixado.

Esta norma adota o modelo "*Plan-Do-Check-Act*" para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente a eficácia do SGCN de uma organização, suportando assim a implementação consistente e integrada e a operação com sistemas de gestão relacionados.

O padrão da ABNT NBR ISO/IEC 22301:2019 (ABNT,2019) citado acima, oferece uma estrutura para planejamento, teste e monitoramento de um SGCN. O documento contém 10 seções, que apresentam o padrão e as definições, bem como os requisitos acionáveis de acordo com a figura 1.

Figura 1: Requisitos da ISO 22301:2019



Fonte: Adaptado de ABNT NBR ISO/IEC ISO 22301:2019

Assim como outros documentos de requisitos da ISO, a norma descreve apenas o que as organizações devem fazer para alcançar a proficiência mínima - ela não prescreve como atingir esses padrões. Cada organização deve considerar suas distintas condições e obrigações para encontrar a melhor forma de atender aos requisitos. Aqui está uma visão geral das cláusulas da ABNT NBR ISO/IEC 22301:2019 (ABNT, 2019) que mais impactam uma organização:

- **Cláusula 4 - Contexto:** A organização deve entender o que é, o que faz e quais resultados e processos deve sustentar. Deve-se determinar quem tem interesse na continuidade das operações – em outras palavras, as partes interessadas. Por exemplo, os clientes têm interesse em que a organização continue funcionando.
- **Cláusula 5 - Liderança:** Poucas iniciativas organizacionais prosperam sem o suporte sustentado e o apoio da alta administração. A administração deve se comprometer com um plano de continuidade de negócios e disponibilizar todos os recursos - humanos, financeiros ou outros - para garantir seu sucesso.
- **Cláusula 6 - Planejamento:** Para planejar a sustentabilidade, deve-se entender quais interrupções podem ocorrer e como esses incidentes afetam

o negócio — em outras palavras, os riscos potenciais e impacto do negócio. Devem definir objetivos mensuráveis de continuidade de negócios para garantir os produtos ou serviços viáveis mínimos, bem como o cumprimento de quaisquer requisitos legais ou regulamentares.

- **Cláusula 7 - Suporte:** Nenhum programa pode avançar sem recursos e suporte. Decidir quais funcionários, funções e equipes precisam para responder a ameaças e como pode-se melhorar sua eficácia. Criar procedimentos de comunicação interna e externa para referência e comunicar o plano de continuidade a todas as partes necessárias antes e durante uma crise. Um sistema de gerenciamento de documentos deve ser estabelecido para os principais documentos de continuidade, como procedimentos.
- **Cláusula 8 - Operação:** Executar avaliação de risco e análise de impacto nos negócios e planejar a abordagem de recuperação de interrupções. Implementar o plano de recuperação com procedimentos detalhados e testa-lo regularmente para verificar se funciona. Certificar-se de que as pessoas possam encontrar os procedimentos (e outros documentos) de que precisam e revisar o plano conforme necessário.
- **Cláusula 9 - Avaliação:** Deve-se estabelecer um processo para medir e avaliar regularmente das políticas e procedimentos de continuidade e suas execuções através de auditorias, além de analisar e revisar o plano e documentos para garantir que sejam eficazes e relevantes.
- **Cláusula 10 - Melhoria**: Buscar melhoria contínua em todas as áreas funcionais e operacionais, inclusive por meio de revisões periódicas de gerenciamento. Melhorias nas atividades do dia a dia ajudam a fortalecer a organização em momentos de disrupção. Quando os processos se desviarem do padrão ou não estiverem em conformidade com os padrões ISO e de gerenciamento de qualidade, implementar ações corretivas.

1.6. ATIVAÇÃO DO PLANO

De acordo com a empresa de consultoria Deloitte (DELOITTE, 2015), incidentes e emergências são fatos ou ocorrências que não fazem parte do funcionamento padrão do serviço e podem resultar em interrupção ou degradação do serviço. Uma interrupção pode afetar sistemas de processamento

automatizado, serviços de suporte ou operações comerciais essenciais, resultando na incapacidade de uma organização de fornecer serviços por um período. Recomenda-se o monitoramento de incidentes e emergências inserindo um ou mais processos voltados para viabilizar a gestão da continuidade de negócio.

As crises desafiam organizações, pessoas, funções e processos de formas invulgares, exigindo uma gestão e resposta dedicada e dinâmica. O tratamento para potenciais crises devem ser tratadas através da Gestão de Crises, cujo principal objetivo é gerir eventos de grande dimensão que possam colocar em risco a viabilidade e a reputação de um negócio. Em caso de desastre físico, as ações de contingência são executadas pelas pessoas que detectar o incidente/desastre. São ações de urgência, que precedem a ativação dos diferentes planos de continuidade.

Em caso de incidente críticos, com impacto em processos vitais mapeados previamente pela organização, as ações de contingência devem ser iniciadas a fim de garantir a continuidade de negócios.

De acordo com o manual de gestão de crise da Deloitte, uma crise pode ter quatro etapas cruciais para a sua gestão, conforme observa-se na figura 2:

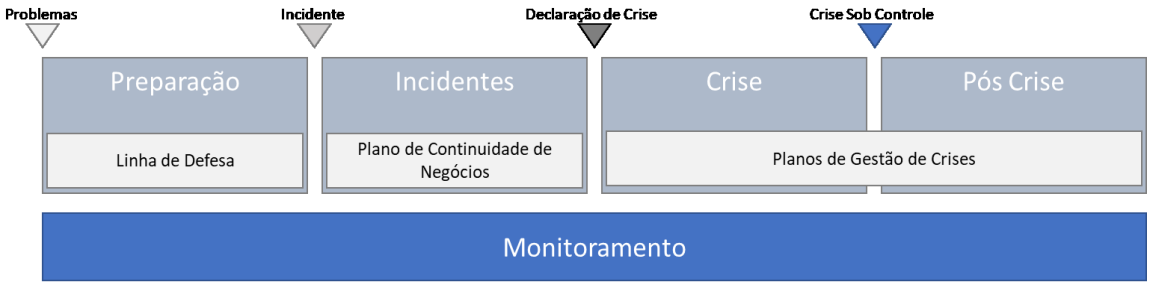
- **Preparação:** Identificar e avaliar as possíveis formas eficientes de gerenciar uma crise, permitindo que as decisões sejam tomadas de maneira estrategicamente adequadas para contornar a situação.
- **Incidentes:** Incidente e Emergência são fatos ou eventos que não fazem parte da operação padrão de um serviço e que podem causar uma interrupção ou a redução na qualidade do serviço. A interrupção pode afetar sistemas automáticos de processamento, serviços de apoio ou operações de negócios essenciais que resultem na incapacidade de uma organização para prestar o serviço por um algum período de tempo. É sugerido que os incidentes e emergências sejam monitorados por meio da inserção de um ou mais processos voltados para a Gestão de Continuidade dos Negócios. Essa por sua vez ajudará a organização a responder de forma estruturada cenários que envolvam incidentes e emergências, garantindo assim alternativas tático-operacionais para a manutenção das operações de negócio de missão crítica.
- **Crise:** Crises podem ser classificadas como qualquer evento ou percepção negativa que possa trazer danos à imagem da organização ou prejudicar seu

relacionamento com a sociedade, clientes, acionistas, investidores, parceiros, órgãos reguladores, poderes públicos entre outras. Uma organização pode ter processos estabelecidos para gerir interrupções rotineiras, porém, crises podem ser dinâmicas e imprevisíveis, dificultando sua gestão. Crises desafiam organizações, pessoas, funções e processos de forma não usual e necessitam de gestão e respostas dedicadas e dinâmicas. O tratamento para potenciais crises devem ser realizadas por meio da Gestão de Crises, cujo principal objetivo é gerenciar eventos de grande dimensão que podem comprometer a perenidade e a reputação de negócios.

Após o desastre ou crise, a organização empresarial habitual é substituída por uma organização de força-tarefa. O objetivo é responder de forma célere e assertiva frente a um incidente ou desastre.

- **Pós-Crise:** O pós-crise é o estágio subsequente à ocorrência de uma crise, onde a organização se concentra na recuperação após os danos causados pelo evento. Isso envolve as atividades como avaliação de danos, comunicação transparente, reconstrução da imagem e reputação, revisão de processos, e desenvolvimento contínua. Esse período é crucial para a organização aprender com a experiência, fortalecer sua resiliência e estar preparada para enfrentar desafios futuros.

Figura 2: Gerenciamento de Continuidade



Fonte: Adaptado de Manual de Gestão de Crise PI – Deloitte (2015)

2. ESTUDO DE CASO: APLICAÇÃO DO PLANO DE CONTINUIDADE DE NEGÓCIOS EM UMA PME DO SETOR DE SERVIÇOS DE TI

A Serviços Integrados Ltda. é uma pequena e média empresa (PME) que opera no setor de serviços, com especialização em consultoria em tecnologia da informação (TI) e gestão de processos empresariais.

2.1. INFORMAÇÕES GERAIS SOBRE A EMPRESA

A organização é composta por uma equipe de 50 profissionais e dedica-se principalmente a atender outras PMEs, oferecendo soluções sob medida para a otimização de processos, implementação de sistemas de TI e consultoria estratégica. Além disso, a continuidade das operações é fundamental para a Serviços Integrados Ltda., pois qualquer interrupção pode afetar seus clientes que dependem de seus serviços para manter a eficiência e a segurança de suas operações.

Assim, observa-se a relevância de um Plano de Continuidade de Negócios (PCN) para uma empresa, como a Serviços Integrados Ltda, e pesquisas demonstram que a ausência de preparação adequada para enfrentar desastres ou interrupções pode acarretar perdas financeiras, operacionais e de reputação conforme apresentado no referencial teórico. Além disso, a aceleração da digitalização empresarial, maximizada pela pandemia de COVID-19, aumentou a vulnerabilidade a ataques cibernéticos, destacando a urgência de adotar medidas sólidas de segurança, de acordo com Kaspersky (2021) e EY (2021).

Para a empresa entender que precisa preservar a confiança de seus clientes e assegurar a prestação ininterrupta de serviços, torna-se relevante estar preparada para enfrentar uma variedade de riscos e ameaças, o que abrange ataques cibernéticos, avarias de equipamentos, desastres naturais e falhas no fornecimento de energia. Dessa forma, a empresa reconhece que um Plano de Continuidade de Negócios (PCN) bem elaborado diminui os riscos dessas ameaças, além de fortalecer a resiliência da empresa, facilitando uma recuperação rápida e eficaz (SÊMOLA, 2003).

É interessante destacar que em um contexto onde a perpetuação das atividades empresariais se torna de suma importância, a Serviços Integrados Ltda. empenha-se em instaurar um Plano de Continuidade de Negócios (PCN) que abranja todas as melhores práticas e normas internacionais pertinentes, assim

como a ABNT NBR ISO/IEC 22313:2020, a qual delineia um Sistema de Gestão da Continuidade de Negócios (SGCN) abrangente (ABNT, 2019). A empresa pretender instituir políticas explícitas, definir processos cruciais, identificar e avaliar ameaças, desenvolver estratégias de mitigação e resposta, e garantir que todos os funcionários estejam devidamente capacitados e prontos para agir diante de possíveis incidentes.

Ao adotar um Plano de Continuidade de Negócios (PCN), a Serviços Integrados Ltda. pretende assegurar a continuidade de suas operações, além de melhorar sua gestão de riscos e elevar a qualidade dos serviços oferecidos. A implementação de um sistema de gestão da continuidade de negócios permitirá uma vantagem competitiva, destacando aos clientes e *stakeholders* o comprometimento da empresa com a segurança e a resiliência, aspectos de suma importância para o sucesso a longo prazo (IBM, 2020).

2.2. RISCOS E AMEAÇAS INDENTIFICADOS

A empresa, Serviços Integrados Ltda, se depara com uma diversidade de riscos e ameaças que podem afetar suas operações e dentre os mais críticos identificados estão ataques cibernéticos, falhas de equipamentos, desastres naturais e interrupções no fornecimento de energia. Dessa forma, uma análise abrangente desses riscos é fundamental para elaborar um Plano de Continuidade de Negócios (PCN) eficaz, assegurando a resiliência da empresa.

Os ataques digitais estão entre as ameaças mais frequentes para a Serviços Integrados Ltda. e a crescente digitalização e dependência dos sistemas de TI tornam a empresa um alvo fácil para cibercriminosos que pretendem explorar suas fraquezas. Observa-se que *phishing*, *malware* e *ransomware* são métodos comuns de ataques cibernéticos que podem comprometer informações sensíveis, interromper operações e provocar grandes prejuízos financeiros (KASPERSKY, 2021). A pesquisa conduzida pela EY (2021) destaca que a pandemia de COVID-19 escalou ainda mais a frequência de ataques cibernéticos, enfatizando a importância de medidas sólidas de segurança da informação.

Por sua vez, problemas com equipamentos também constituem um perigo para a Serviços Integrados Ltda. e a dependência de infraestrutura tecnológica, como servidores, redes e dispositivos de armazenamento, pressupõe que qualquer falha nesses componentes pode causar interrupções nas operações. Nesse aspecto, o

estudo de Everest et al. (2008) demonstram que muitas empresas subestimam a importância de um programa eficaz de gestão de continuidade de negócios (GCN), resultando em recuperações lentas e dispendiosas em caso de falhas tecnológicas.

Além disso, catástrofes naturais, assim como dilúvios, abalos sísmicos e ciclones, representam também ameaças que não podem ser negligenciadas. Apesar de sua ocorrência ser menos comum, as consequências podem ser muito destrutivas, provocando estragos severos nas infraestruturas, perda de informações críticas e paralisações operacionais prolongadas. A habilidade de reagir de maneira eficiente a esses incidentes é fundamental para reduzir os prejuízos e assegurar a continuidade das atividades empresariais (SÊMOLA, 2003).

Já as falhas no fornecimento de eletricidade representam outra ameaça e a dependência de energia para o funcionamento de sistemas dá a entender que qualquer interrupção pode travar as operações da empresa. Assim, planos de contingência, como geradores de reserva e fontes de energia alternativas, é fundamental para assegurar que os sistemas continuem operando mesmo durante quedas de energia, com finalidade de garantir a disponibilidade.

As possíveis repercussões desses riscos nas operações da Serviços Integrados Ltda. são abrangentes, considerando que ataques cibernéticos podem comprometer dados confidenciais, prejudicar a reputação da empresa e acarretar custos elevados para a recuperação. Por sua vez, falhas de equipamentos podem interromper serviços, resultando em perda de produtividade e receita. Da mesma forma, os desastres naturais podem causar grandes danos físicos, demandando longos períodos de recuperação, e, por fim, interrupções de energia podem paralisar as operações, afetando a capacidade de atendimento aos clientes e o cumprimento de prazos.

Para reduzir esses riscos, a Serviços Integrados Ltda. deve adotar uma abordagem ativa na gestão de continuidade de negócios, o que abrange a implementação de fortes medidas de segurança da informação, como autenticação de dois fatores e criptografia de dados, além de treinar os funcionários sobre as melhores práticas de segurança cibernética. Além disso, torna-se fundamental realizar manutenção regular e testes da infraestrutura

tecnológica, desenvolver estratégias de resposta a desastres naturais e garantir fontes alternativas de energia (SÊMOLA, 2003; ABNT, 2019).

2.3. DESENVOLVIMENTO DO PLANO DE CONTINUIDADE DE NEGÓCIOS

O desenvolvimento do Plano de Continuidade de Negócios (PCN) da Serviços Integrados Ltda. foi realizada através de um método organizado e abrangente, com a finalidade de assegurar a persistência das operações essenciais e reduzir os efeitos de possíveis disrupções. Este método compreendeu diversas etapas, começando pela determinação das políticas de continuidade de negócios, que constroem a direção e os objetivos macro do plano. Essas políticas foram alinhadas com a estratégia corporativa e as necessidades dos *stakeholders*, garantindo uma participação total da alta direção com a resiliência da empresa.

A etapa subsequente envolveu a identificação dos processos críticos da Serviços Integrados Ltda., sendo conduzida uma análise das operações da empresa, delineando as funções e atividades essenciais para a continuidade dos negócios. Este levantamento abrangeu processos relacionados à consultoria em TI, gestão de projetos e suporte ao cliente. A identificação dos processos críticos é fundamental, pois direciona os esforços de continuidade para as áreas que mais podem impactar a operação e o atendimento aos clientes (SÊMOLA, 2003).

Após a identificação dos processos críticos, foi realizada uma Análise de Impacto nos Negócios (BIA). O objetivo da BIA era avaliar as consequências de uma interrupção nos processos críticos, quantificando os impactos financeiros, operacionais e reputacionais. Por meio de entrevistas e questionários com os gestores de cada área, foram mapeados os recursos tecnológicos, humanos e físicos necessários para a continuidade de cada processo. A análise permitiu estimar o tempo máximo tolerável de interrupção (MTTI) para cada função crítica e identificar os principais pontos de falha (EVEREST et al., 2008).

A partir das conclusões derivadas da Análise de Impacto nos Negócios (BIA), foi conduzida uma avaliação de riscos, destacando as ameaças mais prováveis e suas respectivas vulnerabilidades. Esta análise contemplou uma variedade de riscos, o que abrange ataques cibernéticos, falhas críticas de equipamentos, desastres naturais catastróficos e interrupções no fornecimento de energia elétrica.

Os riscos identificados foram avaliados em termos de sua probabilidade de ocorrência e o possível impacto que poderia gerar, possibilitando a hierarquização das ameaças mais significativas. Esta avaliação de riscos detalhada estabeleceu uma base sólida para a formulação de estratégias eficazes de redução e resposta a incidentes, conforme estipulado pela norma ABNT NBR ISO/IEC 22301:2019 (ABNT, 2019).

O próximo passo no desenvolvimento do Plano de Continuidade de Negócios (PCN) foi a formulação de estratégias para mitigação e resposta a incidentes. Para cada risco identificado, foram projetadas ações preventivas e corretivas. Entre as estratégias de mitigação, destacam-se a implementação de política/sistemas de backup e recuperação de dados, a adoção de soluções robustas de segurança cibernética, como a autenticação de dois fatores e a criptografia de dados, além da manutenção regular dos equipamentos de TI. Além disso, foram elaborados planos de resposta para situações de crise, especificando as ações a serem executadas em caso de incidentes, como a ativação de equipes de resposta a emergências, comunicação com stakeholders e recuperação de operações críticas (SÊMOLA, 2003; IBM, 2020).

A última etapa do desenvolvimento do Plano de Continuidade de Negócios (PCN) compreendeu a documentação e a disseminação do plano. Neste estágio, o PCN foi formalizado, abrangendo todos os processos, políticas, procedimentos e planos de ação estipulados. Para garantir uma implementação eficaz e a manutenção contínua, foi estabelecida uma estrutura de governança específica, responsável por supervisionar, revisar e atualizar o PCN periodicamente, refletindo quaisquer mudanças no ambiente de negócios e nas ameaças emergentes. Além disso, foram planejados treinamentos e simulações para preparar os funcionários para a ativação do plano, caso seja necessário, garantindo que todos estejam cientes de suas responsabilidades e possam responder de maneira eficaz a possíveis crises (ABNT, 2019).

2.4. IMPLEMENTAÇÃO E TREINAMENTO

A execução do Plano de Continuidade de Negócios (PCN) na Serviços Integrados Ltda. envolveu um processo de planejamento destinado a assegurar que todas as ações fossem tomadas para garantir a resiliência da empresa. Inicialmente, a distribuição de papeis e responsabilidades foi estabelecida. Uma

estrutura de governança específica para a continuidade dos negócios foi implementada, composta por um comitê de continuidade liderado por um gerente especializado em continuidade de negócios. Este comitê tinha a responsabilidade de supervisionar todas as atividades relacionadas ao PCN, garantindo que os objetivos traçados no plano fossem devidamente atingidos.

A formação das equipes de resposta a incidentes teve um papel de suma importância na execução do Plano de Continuidade de Negócios (PCN). Essas equipes eram compostas por funcionários provenientes de diversos departamentos, possuindo habilidades que se complementavam mutuamente, e foram incumbidas de tarefas específicas para gerenciar diferentes tipos de incidentes. A equipe era liderada por um coordenador encarregado de planejar atividades durante uma crise, além de assegurar uma comunicação eficaz com o comitê de continuidade. A definição precisa de funções e responsabilidades foi fundamental para evitar mal-entendidos e garantir uma resposta organizada e eficiente diante de situações emergenciais (SÊMOLA, 2003).

A condução de treinamentos e simulações teve uma grande relevância na implementação do PCN e todos os colaboradores participaram de sessões de capacitação que abordaram os aspectos fundamentais do plano, o que abrange políticas de continuidade, procedimentos a serem seguidos durante incidentes e medidas de segurança da informação. Esses treinamentos foram concebidos para aumentar a conscientização sobre a relevância da continuidade dos negócios e garantir que todos soubessem exatamente como agir em caso de uma interrupção (ABNT, 2019).

Além dos treinamentos, foram conduzidas simulações de incidentes para testar a eficácia do Plano de Continuidade de Negócios (PCN) e preparar os funcionários para situações reais. Essas simulações englobaram cenários como ataques cibernéticos, falhas de equipamentos e desastres naturais. Durante as simulações, as equipes de resposta a incidentes praticaram a ativação do plano, a comunicação com *stakeholders*, a recuperação de dados e a restauração de operações críticas. As simulações oferecem contribuições de grande relevância sobre possíveis lacunas no plano e áreas que precisavam de melhorias (EVEREST et al., 2008).

A Serviços Integrados Ltda. reconhece a importância do treinamento contínuo e para garantir que o Plano de Continuidade de Negócios (PCN) permaneça

atualizado e eficaz, foi implementado um programa abrangente de treinamento contínuo. Este programa abrange revisões periódicas do plano, atualizações em resposta a novas ameaças ou mudanças na estrutura organizacional, além de treinamentos regulares para todos os funcionários. Além disso, auditorias internas e avaliações de conformidade são componentes fundamentais desse programa, garantindo que o PCN esteja sempre em consonância com as melhores práticas e normas internacionais, como a ISO/IEC 22313:2020 e ABNT NBR ISO/IEC 22301: 2019.

2.5. CRISE E ATIVAÇÃO DO PLANO

No estudo de caso, a empresa Serviços Integrados Ltda. passou por um ataque cibernético devastador, causando a interrupção total de seus sistemas. O incidente ocorre em um dia comum de trabalho, quando os funcionários descobrem que não conseguem acessar os sistemas de TI e recebem mensagens de erro indicando um ataque de *ransomware*. Dessa forma, rapidamente, o comitê de continuidade de negócios é alertado, e o Plano de Continuidade de Negócios (PCN) é imediatamente acionado.

A ação inicial empreendida pela equipe de resposta a incidentes consiste na convocação imediata de uma reunião de emergência, cujo objetivo é avaliar a situação atual e determinar a extensão do ataque sofrido. O líder da equipe de TI confirma que um *ransomware* criptografou dados cruciais e está exigindo um resgate para liberar esses dados. Decidida a não ceder às exigências dos criminosos, a equipe implementa os protocolos de resposta definidos no Plano de Continuidade de Negócios (PCN), iniciando pelo isolamento dos sistemas comprometidos para evitar a propagação do *malware* (KASPERSKY, 2021).

A comunicação interna é iniciada, com o comitê de continuidade alertando todos os funcionários sobre o incidente e ordenando a desconexão imediata de todos os dispositivos da rede. Os colaboradores são instruídos a prosseguir com tarefas que não dependem dos sistemas comprometidos e a seguir as diretrizes de segurança cibernética previamente estabelecidas. Nesse sentido, essa comunicação clara e eficiente ajuda a manter a calma e a organização dentro da empresa (EY, 2021).

Além disso, de forma simultânea, a equipe de resposta a incidentes começa a recuperação dos dados utilizando *backups* seguros, conforme os procedimentos

definidos no Plano de Continuidade de Negócios (PCN). A empresa havia estabelecido uma política rigorosa de backups regulares, agora essencial para restaurar os dados sem a necessidade de pagamento de resgate. Enquanto isso, a equipe de segurança realiza uma análise forense para identificar a origem do ataque e corrigir as vulnerabilidades exploradas pelos invasores.

Durante períodos de crise, a comunicação externa tem uma contribuição de grande relevância e o comitê de continuidade elabora um comunicado oficial direcionado a clientes, parceiros e fornecedores, detalhando o incidente ocorrido e as ações implementadas para mitigar seus efeitos. A manutenção da transparência é essencial para sustentar a confiança e a reputação da empresa, enfatizando que medidas concretas estão sendo executadas para resolver a situação. O plano de comunicação abrange atualizações regulares à medida que a recuperação progride.

Na medida em que a restauração dos sistemas críticos avança gradualmente, a equipe de resposta mantém uma vigilância constante sobre a integridade dos dados e a segurança dos sistemas. Já com a finalização da recuperação, a empresa conduz uma revisão pós-incidente para avaliar a eficácia da resposta e identificar possíveis melhorias no Plano de Continuidade de Negócios (PCN). As lições aprendidas durante a crise são registradas e incorporadas nas revisões futuras do plano, assegurando que a Serviços Integrados Ltda. esteja ainda mais preparada para enfrentar possíveis incidentes semelhantes no futuro (SÊMOLA, 2003).

2.6. AVALIAÇÃO E MELHORIA

Depois da simulação de crise e da ativação do Plano de Continuidade de Negócios (PCN) na Serviços Integrados Ltda., uma análise exaustiva foi conduzida para avaliar o desempenho do plano, o que demandou um exame minucioso de cada ação realizada durante a crise, com o objetivo de identificar as lições aprendidas, lacunas e oportunidades de melhoria.

A análise realizada evidenciou múltiplos aprendizados, começando pela eficiência na comunicação tanto interna quanto externa que demonstrou ser fundamental para assegurar a tranquilidade e a coordenação ao longo do incidente. Contudo, identificou-se que a comunicação inicial poderia ter sido mais ágil e detalhada, apontando para a necessidade de otimização dos protocolos de

notificação e das mensagens predefinidas para distintos cenários de crise usando o que foi definido pela ABNT NBR ISO/IEC 22301: 2019.

Um aspecto importante foi a prontidão das equipes de resposta a incidentes, considerando que, embora a equipe tenha apresentado um desempenho satisfatório de modo geral, a simulação destacou a necessidade de treinamentos mais frequentes e especializados para aumentar a familiaridade com os procedimentos de recuperação de dados e segurança cibernética. Nesse sentido, isso abrange a prática regular de cenários variados para garantir que todos os membros da equipe saibam exatamente como reagir a diferentes tipos de crises (SÊMOLA, 2003).

A investigação também destacou a relevância crítica de possuir *backups* que estejam constantemente atualizados e facilmente acessíveis. A política rígida de *backups,* adotada pela Serviços Integrados Ltda. foi posta à prova durante a crise, revelando-se eficaz. No entanto, foram detectadas deficiências na regularidade das verificações e testes desses backups. Portanto, sugere-se a implementação de um cronograma mais severo para testes de recuperação de dados, assegurando que os *backups* estejam sempre prontos para uso imediato (EVEREST *et al*., 2008).

A análise subsequente ao incidente destacou a urgência de melhorar a infraestrutura de TI para aumentar a resiliência contra invasões cibernéticas. Assim, propôs-se alocar recursos em tecnologias de ponta para detecção e resposta a ameaças, além de fortalecer as práticas de segurança cibernética, o que abrange autenticação multifatorial e criptografia de ponta a ponta. Essas medidas têm como objetivo diminuir a suscetibilidade a futuros ataques e aprimorar a capacidade de resposta da organização (KASPERSKY, 2021; EY, 2021).

Por fim, a relevância da revisão contínua do Plano de Continuidade de Negócios (PCN) foi ressaltada como um elemento de suma importância para a resiliência duradoura da Serviços Integrados Ltda. A manutenção periódica do plano, que requer a avaliação de novos riscos e a atualização das estratégias de mitigação, é fundamental para garantir a eficácia contínua do PCN. Ademais, a execução de testes e auditorias regulares foi enfatizada como uma prática indispensável para detectar e corrigir potenciais falhas, prevenindo crises reais (ABNT, 2019).

3. CONSIDERAÇÕES FINAIS

A partir do desenvolvimento do trabalho, foi possível perceber que a criação e a implementação de um Plano de Continuidade de Negócios (PCN) são fundamentais para assegurar a resiliência e a capacidade de recuperação de uma empresa perante incidentes e crises. Dessa forma, utilizando o estudo de caso da Serviços Integrados Ltda., pôde-se evidenciar a relevância de cada fase do desenvolvimento de um PCN, desde a identificação dos riscos e ameaças até a avaliação contínua e a melhoria do plano.

A Serviços Integrados Ltda., uma pequena e média empresa (PME), operando no setor de serviços, confrontou uma variedade de cenários de risco, abrangendo desde ataques cibernéticos e falhas de equipamentos até desastres naturais e interrupções no fornecimento de energia. Assim, através de uma identificação e análise desses riscos, a empresa conseguiu desenvolver estratégias de mitigação e resposta altamente eficazes. Essas estratégias foram alinhadas com as melhores práticas e normas internacionais, especificamente a ABNT NBR ISO/IEC 22313:2020, garantindo uma abordagem ampla e resiliente para a continuidade dos negócios.

A implantação do PCN demandou a definição de funções e responsabilidades, a constituição de equipes dedicadas à resposta a incidentes, além de um cronograma contínuo de treinamentos e simulações práticas. Essas medidas asseguraram que todo o quadro de funcionários estivesse apto a agir prontamente diante de quaisquer interrupções, reduzindo ao máximo os impactos sobre as operações essenciais da empresa (ABNT, 2020).

Por sua vez, o ataque cibernético expôs a eficácia do Plano de Continuidade de Negócios (PCN), que identificou áreas que necessitam de aprimoramento e a comunicação ágil e eficiente, a restauração de dados a partir de *backups* seguros, e a análise forense para corrigir vulnerabilidades foram fundamentais para uma recuperação bem-sucedida. A importância da avaliação pós-incidente e da melhoria contínua foi enfatizada, assegurando que o plano permaneça atualizado e eficaz frente a novos desafios.

Por fim, a empresa Serviços Integrados Ltda. mantém-se em constante prontidão para lidar com possíveis incidentes futuros por meio de revisões periódicas do Plano de Continuidade de Negócios (PCN), testes regulares e auditorias internas. O compromisso inabalável com a segurança da informação e a resiliência organizacional

resguarda os ativos da empresa, além de consolidar a confiança de clientes, parceiros e demais *stakeholders*.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO 22301:2019 - Sistemas de gestão de continuidade de negócios - Requisitos.** Rio de Janeiro: ABNT, 2019. 27 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 22313:2020 - Segurança e resiliência - Sistemas de gestão de continuidade de negócios - Orientações sobre o uso da ABNT NBR ISO 22301**. Rio de Janeiro: ABNT, 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27001:2023 - Segurança - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos**. Rio de Janeiro: ABNT, 2023.

DAS, Swapan Kumar; GARG, Dinesh. Business continuity planning: importance, need and challenges**. International Journal of Computer Applications**, v. 48, n. 10, p. 1-5, 2012.

DELOITTE. **Manual de gestão de crises para relações com investidores comunicação e estratégia para a preservação de valor.** [S.l.]: Deloitte Touch, 2015.

DRI International. Business Continuity Overview. Dearborn, MI: DRI International, 2024. 26 p. Disponível em: https://drii.org/education/BCP-OVR Acesso em: Acesso em: 23 abr. 2024.

EVEREST, David, *et al*. **IPPF**: Guia prático gestão de continuidade de negócios. 2ª ed. São Paulo: The Institute of Internal Auditors, 2008. Disponível em: https://iiabrasil.org.br/korbilload/upl/ippf/downloads/livro-1-gesto-d-ippf-00000001-12122018093750.pdf Acesso em: 06 jun. 2024.

EY. **Ataques cibernéticos a empresas aumentam 300% na pandemia.** EY Brasil. Disponível em: https://www.ey.com/pt_br/agencia-ey/noticias/ataques-ciberneticos-a-empresas-aumentam-300-por-cento-na-pandem. Acesso em: 06 jun. 2024.

GETSCHKO, Demi. *et al.* **Núcleo de informação e coordenação do ponto br - NIC.br**, 2021. Disponível em: https://cetic.br/media/docs/publicacoes/2/20221121123006/resumo_executivo_tic_empresas_2021.pdf Acesso em: 06 jun. 2024.

HARRISON, Nigel**. Disaster recovery and business continuity**. London: Butterworth-Heinemann, 2013.

IBM Services. **IBM Maximo Worker Insights (Public edition).** IBM, V. 37, p. 10, 2012. Disponível em: https://www.ibm.com/docs/en/mwi?topic=overview-business-continuity-plan Acesso em: 06 maio 2024.

IBM Services. **PCNs: Business Continuity Plans: An Essential Guide**. 2020.

INSTITUTO DE INFORMÁTICA. **Planos de contingência de mercado**. 1999. Disponível em: http://www.inst-informatica.pt/o-instituto/factos-historicos/publicacoes/guias-tecnicos/ano2000.pdf. Acesso em: 23 abr. 2024.

KASPERSKY. **Panorama de Ameaças: Phishing.** 2021. Disponível em: https://www.kaspersky.com.br/about/press-releases/2021_panorama-de-amenazas-phishing. Acesso em: 27 jun. 2024.

OLIVEIRA, D. P. R. **Planejamento estratégico**: conceitos, metodologia e práticas. São Paulo: Atlas, 2017.

RICHARDSON, Maggie. **The essentials of business continuity**. Chichester: John Wiley & Sons, 2010.

SANTOS, M. C. A. da S. **Continuidade de negócios**: conceitos, princípios e práticas. São Paulo: Érica, 2014.

SÊMOLA, Marcos**. Gestão da segurança da informação**: uma visão executiva. Rio de Janeiro: Campus, 2003.

TOMIC, Ivana; RAKIC, Biljana; CVETKOVIC, Dragan. **Business continuity planning:** a comprehensive approach. Procedia Engineering, v. 178, p. 592-600, 2017.

VARAJÃO, J. **Arquitectura da gestão de sistemas de informação**. 3ª ed. [S.l.]: Editora FCA, 2006.

VARAJÃO, M. A. F. et al. **Modelo para a avaliação do desempenho potencial de gestores de sistemas de informação**. Interciência, v. 43, n. 1, p. 724-733, 2018.