

UTILIZAÇÃO DO PLANO DE CONTINUIDADE DE NEGÓCIOS COMO FERRAMENTA PARA ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS

USE OF THE BUSINESS CONTINUITY PLAN AS A TOOL FOR COMPLIANCE WITH GENERAL DATA PROTECTION LAW

Ana Rita Akayama Kanagusku
Fatec Americana
rita.kanagusku@gmail.com

Maria Cristina Aranda
Fatec Americana
mcris.aranda@fatec.sp.gov.br

Resumo

A Lei Geral de Proteção de Dados (LGPD) estabelece requisitos específicos para a proteção e o tratamento adequado de dados pessoais, enfatizando aspectos dos três principais pilares da Segurança da Informação: Confidencialidade, Integridade e Disponibilidade (CID) desses dados. No entanto, a referida lei é associada quase que instintivamente à privacidade de dados, o foco nesse caso, recai sobre a Confidencialidade, enquanto os aspectos de Integridade e Disponibilidade não são contemplados com o mesmo destaque. Nesse contexto, o Plano de Continuidade de Negócios (PCN) pode ser uma ferramenta fundamental para atendimento dessa demanda, com estratégias e planos de ações que consigam garantir em situações adversas, o pleno funcionamento dos serviços essenciais, entre os quais está a proteção de dados. A integração adequada de um PCN com os requisitos da LGPD, permite às organizações não apenas cumprirem com as exigências legais, mas também fortalecerem sua resiliência e garantir a proteção abrangente dos dados. O presente estudo emprega o método dedutivo, embasado em pesquisa bibliográfica e documental, além de uma sucinta análise do PCN de uma empresa privada, focalizando sua conformidade com os requisitos estabelecidos pela LGPD.

Palavras-chave: Plano de continuidade de negócios, Proteção de dados, LGPD.

Abstract

The General Data Protection Law (LGPD) establishes specific requirements for the protection and adequate processing of personal data, emphasizing aspects of the three main pillars of Information Security: Confidentiality, Integrity and Availability (CIA) of these data. However, the aforementioned law is almost instinctively associated with data privacy, the focus in this case is on Confidentiality, while the aspects of Integrity and Availability are not covered with the same emphasis. In this context, the Business Continuity Plan (BCP) can be a fundamental tool for meeting this demand, with strategies and action plans that can guarantee, in adverse situations, the full functioning of essential services, including data protection. Proper integration of a BCP with LGPD requirements allows organizations to not only comply with legal requirements, but also strengthen their resilience and ensure comprehensive data protection. The present study uses

the deductive method, based on bibliographic and documentary research, in addition to a succinct analysis of the BCP of a private company, focusing on its compliance with the requirements established by the LGPD.

Keywords: Business continuity plan, Data protection, LGPD.

1. Introdução

A segunda década do século XXI já está sendo referenciada como a era dos dados, era da informação ou era digital em que a quantidade de informações e dados gerados e armazenados está aumentando exponencialmente. Esse fenômeno ocorre devido ao avanço da tecnologia, ao grande uso da Internet, da necessidade de maior interconexão através das redes de comunicação e a intensificação da globalização (Gonçalves, 2023). Outro fator que levou à evolução digital foi a pandemia da Covid-19, momento este que foi necessário maior investimento em TI.

Há uma crescente necessidade de as empresas se adaptarem a esses avanços, garantindo que estejam preparadas para enfrentar qualquer interrupção nas operações, e ao mesmo tempo, apresentarem conformidade com as leis de proteção de dados, como a LGPD no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia.

Esse aspecto indica a compreensão de quão volátil e complexo é o ambiente de negócios, a consciência da inevitabilidade de desenvolver estratégias de continuidade de negócios para lidar com possíveis incidentes levando a interrupções, seja por questões regulatórias, tecnológicas ou outros desafios (Bruno, Costa & Rodrigues, 2020).

Uma gestão adequada de dados e informações pessoais desempenha um papel fundamental na resiliência do negócio, não apenas garantindo o cumprimento da legislação, mas também prevenindo sérias repercussões financeiras e de reputação decorrentes da perda ou comprometimento de dados.

A Norma ISO/IEC 22301 (2019) destaca que o PCN é um documento que descreve as medidas específicas a serem tomadas para garantir a continuidade das operações e minimizar os impactos em caso de incidentes que possam afetar a organização. Esse plano deve incluir as atividades necessárias para garantir que as funções críticas possam ser retomadas e mantidas dentro de tempos previamente determinados após um incidente perturbador.

Essas atividades incluem a identificação de riscos e ameaças potenciais, a avaliação do impacto nos negócios, a definição de estratégias de resposta, a elaboração de planos de recuperação e a coordenação de esforços durante a implementação do plano.

Nesse sentido, as estratégias e planos de ação abrangidos pelo PCN, destinados à proteção e recuperação de dados em situações adversas, como ataques cibernéticos, desastres naturais e outros eventos que possam comprometer a disponibilidade e integridade dos dados, apresentam significativa importância na conquista da conformidade com a LGPD. Esses elementos estão intrinsecamente ligados à proteção de dados e à continuidade das operações comerciais.

O objetivo do presente estudo consiste em enfatizar a relevância do PCN como uma poderosa ferramenta no contexto da conformidade com a LGPD. Esta abordagem se justifica

pelo fato de que o PCN desempenha um papel fundamental na prevenção de incidentes de segurança de dados, no gerenciamento de riscos e na definição de procedimentos apropriados para a resposta a incidentes, tornando-se, assim, um componente essencial para a garantia do cumprimento das normas estabelecidas pela referida lei.

Embora a LGPD (Brasil, 2018), não faça menção direta aos pilares da Segurança da Informação (CID), ela está alinhada com esses princípios ao estabelecer requisitos específicos para salvaguardar a confidencialidade, integridade e disponibilidade dos dados pessoais e sensíveis. O objetivo é proteger a privacidade e os direitos dos titulares desses dados, para atingir esse propósito, a referida lei estabelece uma série de requisitos e práticas obrigatórias para empresas e organizações, entre os quais se destacam:

- Base legal para o tratamento de dados: é preciso haver uma justificativa legal, que deve ser registrada e ser coerente com o objetivo de cada tratamento de dados pessoais e sensíveis, como consentimento do titular, execução de contrato, ou cumprimento de obrigação legal. Além disso, a coleta deve ser limitada ao mínimo necessário para cumprir com essa finalidade.
- Transparência e informação: Os titulares devem ser informados sobre como seus dados serão tratados, quais dados estão sendo coletados, para quais finalidades, e com quem serão compartilhados.
- Segurança da informação: A LGPD exige que as empresas implementem medidas de segurança técnicas e organizacionais para proteger os dados pessoais contra acessos não autorizados, vazamentos, e outras ameaças.
- Direitos dos titulares: Os titulares de dados têm diversos direitos assegurados pela LGPD, e as empresas devem estar prontas para atendimento das solicitações, como o direito de acesso, correção, exclusão, anonimização, portabilidade, e oposição ao tratamento de seus dados.
- Encarregado pelo tratamento de dados: As organizações devem nomear um responsável (em inglês, DPO - *Data Protection Officer*) para supervisionar a conformidade com a LGPD e atuar como ponto de contato para titulares e a Autoridade Nacional de Proteção de Dados (ANPD).
- Relatórios de impacto e auditorias: Em certos casos, é necessário realizar um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) para avaliar os riscos e os impactos do tratamento de dados pessoais, especialmente em tratamentos considerados de alto risco.
- Notificação de incidentes de segurança: Caso ocorra um incidente de segurança que possa comprometer os dados pessoais, as empresas devem notificar a ANPD e, dependendo do caso, os titulares afetados.

Assim, diante do exposto, quando o PCN é implementado de maneira eficaz, ele pode abranger esses três pilares essenciais da segurança da informação, tornando-se um elemento essencial para garantir o cumprimento das regulamentações estabelecidas pela LGPD.

Especialmente no que tange ao pilar da confidencialidade, isso se manifesta pela possibilidade de um PCN envolver a implementação de controles de acesso restrito, criptografia de dados, políticas de gerenciamento de senhas, treinamento de funcionários sobre segurança da informação e medidas de segurança física para proteger os recursos de TI da empresa. Além

disso, o PCN pode estabelecer procedimentos para lidar com incidentes de segurança de dados de maneira rápida, minimizando o impacto na confidencialidade das informações.

Devido à constante evolução da LGPD, a utilização dessa valiosa ferramenta exige uma abordagem contínua de atualização, com o intuito de manter sua conformidade com as mudanças regulatórias em curso.

2. Referencial Teórico

A origem do PCN data dos anos de 1970, como uma decorrência dos planos de recuperação de desastres. Naquela época as instituições financeiras foram as pioneiras ao investir em locais alternativos, onde armazenavam fitas de *backup* em ambientes resguardados e distantes dos sistemas computacionais. Em grande parte, a ativação dos esforços de recuperação estava condicionada à ocorrência de eventos físicos, como incêndios, inundações, tempestades e outros desastres similares. Na década seguinte pouca coisa mudou com o crescimento da adoção de locais de recuperação comercial, os quais proporcionavam serviços de computação compartilhados (Kyndryl, 2022).

A partir da década de 1990 com o fenômeno da aceleração da globalização e crescente expansão do acesso aos dados, o *modus operandi* das organizações precisou ser repensado para não haver o risco de perdas de clientes e competitividade, resultando em um reconhecimento da necessidade de um plano de continuidade de negócios capaz de contemplar todos esses avanços.

Em decorrência dessa demanda, surge a necessidade de uma padronização dos PCNs e em 1995, é publicada a Norma sobre Gestão de Desastres/Emergências e Programas de Continuidade de Negócios (NFPA 1600), que já foi revisada diversas vezes e é adotada como boa prática até a atualidade, especialmente por empresas estadunidenses. Por outro lado, a International Standard Organization publicou em 2012 a ISO 22301, com reconhecimento mundial e atualmente em sua versão 2019, é tida como referência na estrutura de continuidade de negócios. (Advisera, 2023).

O Banco do Brasil (2022) apresenta uma definição bastante adequada aos dias atuais:

O Plano de Continuidade de Negócios (PCN) é uma ferramenta de gestão que reconhece ameaças potenciais a uma organização e analisa o impacto que elas podem ter nas operações do dia a dia. Também fornece uma maneira de mitigar essas ameaças, colocando em prática uma estrutura a qual permite que as funções-chave do negócio continuem, mesmo que o pior aconteça.

A complexidade e abrangência dos PCNs aumenta na medida em que a interconectividade de informações avança, ocasionando uma demanda de adaptação contínua das organizações diante de um cenário tão dinâmico, no qual a rápida propagação e intercâmbio de dados intensifica os desafios relacionados à identificação, avaliação e gestão de riscos, bem como à eficácia das estratégias de resposta e recuperação implementadas.

2.1 A Importância da Implementação de um PCN

O avanço da tecnologia possibilita aos indivíduos e às organizações facilidades anteriormente inimagináveis, em contrapartida, existe a preocupação em como garantir a proteção dos dados. A cada dia surgem treinamentos e *softwares* mais sofisticados, impulsionando um crescente investimento das empresas em relação à segurança da informação.

Segundo Santos (2019), “ O plano de continuidade de negócio é uma ferramenta essencial que visa garantir que a empresa está preparada para uma recuperação imediata das suas atividades críticas e dos seus interesses de apoio e aplicações em caso de um desastre. ”

A manutenção da continuidade dos serviços é essencial para atender às expectativas dos *stakeholders* (partes interessadas) e preservar a confiança do mercado. Os PCNs garantem que os serviços essenciais sejam mantidos, mesmo em situações de crise, através de uma mobilização de planos detalhados sobre alocação de recursos como pessoal, tecnologia e infraestrutura, de maneira eficiente. Isso evita a desorganização e garante que os recursos críticos sejam direcionados para onde são mais necessários.

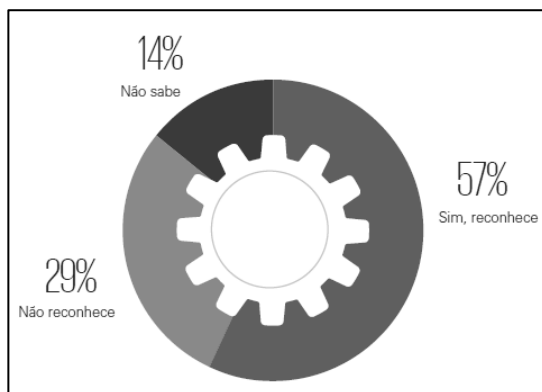
De acordo com Bruno, Costa e Rodrigues (2020), a implementação de Planos de Continuidade de Negócios (PCN) e Planos de Recuperação de Negócios (PRN) desempenha um papel primordial na sustentação operacional das organizações frente a eventos disruptivos que possam impactar adversamente suas operações fundamentais. Estes planos não apenas preveem ações estratégicas para mitigar os efeitos de tais eventos, mas também estabelecem diretrizes claras para a rápida restauração das funções críticas da organização.

Entretanto, apesar da relevância dos PCNs, a pesquisa de maturidade dos Planos de Continuidade de Negócios no Brasil, realizada pela KPMG (2021) concluiu que o quadro atual das organizações no Brasil apresenta índices baixos de preparo para enfrentamento de crises, apenas 27% das empresas possuem um PCN estruturado, e 40% não responderiam ou seriam ineficientes a uma situação crítica. A pesquisa ainda revela que os 33% restantes dessas empresas pesquisadas, até possuem mecanismos de estratégias de continuidade de negócios, mas não identificam e direcionam todos os eventos que possam afetar as operações de maneira adequada. No início da pandemia apenas 12% das empresas nacionais tinham um PCN de acordo com TI Inside (2022).

Um dos principais fatores para esse nível de maturidade tão abaixo do aceitável é a carência de uma cultura de gestão de riscos e crises, é necessário alavancar o processo de conscientização desde a alta administração até o nível operacional sobre a relevância desse tema. Outro ponto a se considerar é a falta de testes e atualizações periódicas nos PCNs existentes.

Em contrapartida, a mesma pesquisa revela que 57% dos entrevistados reconhece a importância de implementação de um PCN, conforme ilustra a Figura 1.

Figura 1 – Reconhecimento da administração sobre a importância de um PCN



Fonte: KMPG, 2021

O que se observa é que mesmo reconhecendo a importância dos PCN, ainda não está sedimentado os seus potenciais benefícios nas organizações brasileiras, fazendo com que outras prioridades sejam contempladas. Ainda não há um entendimento suficiente para que a implementação de um PCN seja considerada prioritária, especialmente em pequenas e médias empresas, que carecem de recursos e uma estrutura organizacional capacitada para conduzir esse processo.

De acordo com Oliveira, Fernandes, Luzia e Severiano Júnior (2024), para pequenas e médias empresas, implementar um PCN pode ser desafiador, especialmente devido a:

- Limitações de recursos financeiros e humanos, o que dificulta a alocação de recursos especializados para a criação, manutenção e atualização de um PCN;
- Falta de *expertise* em segurança da informação, essas empresas dificilmente podem contar com profissionais qualificados em segurança da informação, tornando a estruturação de um PCN para a proteção de dados pessoais uma tarefa complexa e custosa;
- Dificuldade em criar um mapeamento de dados eficiente, mapear todos os processos que envolvem dados pessoais e entender as interdependências operacionais pode ser desafiador para pequenas empresas, que muitas vezes não têm processos documentados ou tecnologia para rastrear essas operações;
- Custos de tecnologia, a implementação de sistemas de backup, recuperação de dados e soluções de segurança robustas pode ser inviável financeiramente para empresas menores, e a contratação de consultorias externas para elaborar e manter o PCN pode representar um custo elevado;
- Complexidade para conseguir garantir a atualização contínua do PCN, como o ambiente de segurança cibernética e a legislação estão em constante evolução, manter o PCN atualizado exige um compromisso constante, o que é desafiador para empresas com equipes enxutas e outras prioridades operacionais.

Essas dificuldades que as pequenas e médias empresas enfrentam para implementar um PCN, podem ser mitigadas com algumas estratégias: uso de soluções de segurança e continuidade em nuvem, contratação de consultorias com custo-benefício adequado e

implementação de planos de contingência simplificados.

2.2 O PCN como ferramenta de adequação à LGPD

Uma vez apresentada a importância de implementação de um PCN, é possível enumerar aspectos relacionados a ele que farão a diferença e poderão contribuir significativamente para a conformidade com a LGPD.

O artigo 5º da LGPD (Brasil, 2018), define:

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Esta definição corrobora a necessidade de tratativas que possam dar garantia de atendimento aos três principais pilares da segurança da informação, conhecidos pela sigla CID, confidencialidade, integridade e disponibilidade dos dados e informações. Nesse sentido um PCN pode contribuir implementando as seguintes práticas: *backup* regular de dados críticos, recuperação de desastres, testes de restauração de *backup*, simulações de recuperação de desastres, classificação e priorização de dados, políticas de segurança da informação, treinamento e conscientização dos envolvidos, monitoramento constante de sistemas de dados e atualização contínua do plano, para que permaneça relevante e eficaz ao longo do tempo.

2.2.1 Disponibilidade de Dados

De acordo com a LGPD (Brasil, 2018), a diferenciação entre dados pessoais e dados sensíveis é de suma importância no contexto da LGPD, que estabelece critérios rigorosos para a gestão e proteção dessas informações. Enquanto os dados pessoais referem-se a informações que identificam ou podem identificar um indivíduo, como nome, CPF e endereço, os dados sensíveis podem revelar aspectos mais profundos e íntimos da vida do titular. Por sua natureza, a proteção desses dados é ainda mais rigorosa do que a dos dados pessoais. A exposição ou manipulação indevida dos dados sensíveis pode comprometer a dignidade, a privacidade e até a reputação do indivíduo. Esses dados, por lidarem com características íntimas e vulneráveis, podem gerar discriminação, preconceito e constrangimento, além de danos emocionais e psicológicos, visto que seu uso indevido pode resultar em danos morais significativos. Entre os tipos de dados sensíveis estão informações sobre a origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, orientação sexual, detalhes sobre a saúde, dados biométricos.

A LGPD estabelece com rigor às organizações a responsabilidade de garantir a disponibilidade e segurança desses dados, exigindo a implementação de medidas técnicas e organizacionais robustas para protegê-los contra acesso não autorizado, perda ou destruição. Nesse contexto, um PCN bem elaborado, que contemple estratégias visando assegurar a acessibilidade dos dados pessoais e sensíveis mesmo em situações adversas, como falhas de hardware, desastres naturais ou ataques cibernéticos, pode atender de maneira eficaz essa exigência regulatória.

Ao optar pela adoção de um PCN abrangente, uma organização pode aumentar significativamente sua capacidade de manter a continuidade operacional e elevar suas chances de garantir a disponibilidade contínua de dados, independentemente das circunstâncias

adversas.

Basicamente, pode-se dizer que a implementação eficaz de um PCN não apenas contribui para o atendimento dos requisitos da LGPD, mas também é uma salvaguarda proativa, concedendo à organização antecipar, responder e se recuperar rapidamente de eventos que possam comprometer a disponibilidade dos dados.

2.2.2 Recuperação de Dados

O PCN geralmente contém procedimentos detalhados de *backup* e recuperação de dados. Isso é essencial para garantir que os dados pessoais possam ser recuperados em caso de perda ou dano, atendendo ao requisito de integridade dos dados da LGPD.

De acordo com Pereira (2018):

A implementação de rotinas de *backup*, é crucial para as organizações bem como para o usuário comum, pois são através dessas técnicas que é possível garantir a recuperação das informações caso elas não estejam mais disponíveis. O *backup* não é apenas utilizado para a recuperação de um ou outro arquivo, muitas vezes um *backup* pode realizar a restauração de um ambiente todo, garantindo assim a sobrevivência de uma empresa no mercado.

Dentre as orientações para proteção contra *malware* que constam na ISO/IEC 27002 (2022) encontra-se: preparar planos de continuidade de negócios apropriados para recuperação de ataques de *malware*, incluindo todos os dados necessários, *backup* de *software* (incluindo *backup online* e *offline*) e medidas de recuperação.

2.2.3 Proteção contra Interrupções

Segundo Santos (2019), o PCN desempenha um papel crucial na proteção contra interrupções, pois incorpora medidas destinadas a prevenir ou minimizar a ocorrência de eventos disruptivos nos processos de negócios, não apenas visando manter a continuidade operacional, mas também contribuir significativamente para a preservação da disponibilidade e integridade dos dados pessoais, elementos críticos em um cenário cada vez mais digital e interconectado.

Nesse sentido, uma abordagem proativa é fundamental no desdobramento de um PCN, isso inclui a identificação e mitigação de potenciais fontes de interrupções, sejam elas de origem natural, como desastres ambientais, ou causadas por fatores tecnológicos, como falhas de sistemas críticos. A implementação de estratégias preventivas, como a redundância de sistemas e a diversificação de fornecedores, busca reduzir a probabilidade de ocorrência de interrupções, porém, mesmo adotando medidas preventivas rigorosas, é impossível eliminar totalmente o risco.

Portanto, o PCN deve também incorporar estratégias para minimizar os impactos quando uma interrupção ocorre, como por exemplo a rápida transição para operações alternativas e a mobilização de recursos de recuperação em tempo hábil.

A velocidade de recuperação é um elemento-chave na proteção contra interrupções, no contexto da proteção de dados pessoais, um PCN é projetado para garantir que as informações estejam disponíveis quando necessário e permaneçam íntegras mesmo diante de interrupções. Isso envolve a implementação de práticas de segurança robustas, garantindo que os dados

peçoais dos clientes, funcionários e demais partes interessadas estejam resguardados contra perdas ou acessos não autorizados.

2.2.4 Gestão de Incidentes

A LGPD exige que as organizações relatem violações de dados, um PCN pode ser um excelente instrumento nesse processo, por poder incorporar planos de resposta a incidentes que definem como identificar, relatar e lidar com violações de dados, permitindo o cumprimento desse requisito legal.

A norma ISO/IEC 27001 (2022) recomenda que as organizações classifiquem os incidentes com base em critérios predefinidos, para permitir uma resposta adequada a diferentes tipos e níveis de incidentes, bem como, incentiva a avaliação do impacto de incidentes de segurança da informação através da BIA (Business Impact Analysis) para determinar as medidas de resposta adequadas.

É preciso que haja monitoramento do desempenho, revisões regulares do processo de gestão de incidentes e implementação de melhorias conforme necessário, levando sempre em consideração o tamanho, a complexidade e a natureza das operações.

2.2.5 Controle de Acesso

O controle de acesso é um componente primordial para garantir a conformidade com a LGPD no contexto da segurança da informação, envolve a proteção adequada dos dados pessoais, garantindo que apenas pessoas autorizadas tenham acesso a essas informações.

A implementação de políticas claras de acesso, autenticação e autorização é uma prática padrão em um PCN, isso impede o acesso não autorizado a sistemas e dados críticos.

Um PCN pode incluir estratégias de controle de acesso que ajudam a proteger a confidencialidade dos dados pessoais, garantindo que apenas pessoas autorizadas tenham acesso às instalações, sistemas e dados necessários para manter as operações críticas durante uma interrupção. Portanto, o controle de acesso refere-se ao controle físico de acesso a instalações, assim como, controle lógico de acesso a sistemas e dados.

2.2.6 Testes e Treinamento

O PCN estabelece procedimentos claros para a restauração rápida de sistemas críticos, minimizando assim o tempo de inatividade. Testes periódicos desses procedimentos garantem que a equipe esteja preparada para ações imediatas quando necessário, contribuindo para a eficácia global do plano, esses testes podem incluir simulações de violações de dados e ações de recuperação.

Além disso, o treinamento e a conscientização dos funcionários sobre as práticas de PCN pode aumentar a percepção sobre a importância da proteção de dados pessoais, haja vista que não adiantará implementar um plano de primeira grandeza se as pessoas não estiverem preparadas para colocá-lo efetivamente em prática.

Os funcionários precisam estar cientes de como os procedimentos de continuidade de negócios podem afetar a segurança e a privacidade dos dados pessoais. O treinamento pode fornecer orientações sobre como garantir os três pilares da segurança da informação: confidencialidade, integridade e disponibilidade dos dados.

Tendo em vista que a legislação e as melhores práticas podem evoluir, o treinamento contínuo é essencial para garantir que os funcionários estejam atualizados quanto às últimas mudanças na LGPD e nos procedimentos relacionados ao PCN.

O treinamento não apenas aumenta a resiliência da organização durante interrupções, mas também contribui para ocorrer *compliance* com as normas de privacidade, como a LGPD; deve ser considerado como uma parte essencial da estratégia geral de segurança da informação e conformidade com a privacidade de dados.

Apesar de toda a relevância dos testes e treinamento, segundo pesquisa da KPMG (2021), dentre as empresas respondentes que possuíam PCN, 48% não realizam nenhum tipo de teste e 45% não possuem um programa de treinamento e conscientização. Esses números destacam uma lacuna preocupante na eficácia da implementação dos PCNs, sugerindo que uma parte significativa das organizações pode estar subestimando a importância de avaliar e aprimorar regularmente seus planos de continuidade.

A ausência de testes pode comprometer a eficácia de respostas em situações de crise, dificultando a pronta avaliação dos sistemas e processos. Além disso, a falta de programas formais de treinamento e conscientização pode resultar em equipes despreparadas para lidar com eventos adversos, aumentando os riscos operacionais e a potencial exposição a ameaças à segurança da informação.

Esse cenário reforça a necessidade emergente de incentivar práticas mais robustas de testes e treinamento dentro das organizações, visando não apenas a conformidade com regulamentações, mas também a garantia da sua resiliência operacional.

2.2.7 Documentação e Auditoria

O PCN inclui documentação detalhada dos procedimentos e políticas relacionados à continuidade de negócios. Essa documentação é valiosa não apenas durante a execução de ações corretivas em momentos de crise, mas também no cenário de auditoria.

Pelo fato de apresentar uma visão abrangente dos processos de continuidade de negócios adotados pela organização, a documentação se configura em uma base sólida para avaliações tanto em auditorias internas quanto externas. Além de que, essa documentação desempenha um papel crucial na demonstração do comprometimento da organização com a conformidade normativa, particularmente no que diz respeito à LGPD.

A importância da documentação e auditoria em um plano de continuidade de negócios para a LGPD (Brasil, 2018) está diretamente relacionada à garantia da conformidade com os requisitos legais e à proteção dos dados pessoais, tais como: demonstrar transparência e responsabilidade, identificar lacunas na proteção de dados e garantir que sejam abordadas adequadamente para evitar violações à lei, assegurar que as medidas de segurança de dados sejam incorporadas ao processo e que sejam revisadas regularmente para garantir sua eficácia.

Um exemplo da relevância dessa documentação é a criação de políticas de acesso contingenciais, em casos de indisponibilidade dos sistemas principais, de acordo com a ISO/IEC 22301, o PCN deve prever políticas específicas que garantam que somente pessoas autorizadas tenham acesso aos dados pessoais. Dessa forma, é possível a prevenção de acessos indevidos e, além disso, manter o princípio de “acesso mínimo necessário” previsto pela LGPD.

Tão importante quanto a documentação, a auditoria é uma prática essencial dentro de um PCN que contribui diretamente para a conformidade com a LGPD, pois permite a verificação e o aprimoramento contínuo das práticas de segurança e proteção de dados. Por meio de auditorias regulares, a organização pode identificar falhas ou vulnerabilidades nos processos de tratamento de dados pessoais, e ainda, avaliar se os requisitos de segurança e privacidade estabelecidos pela LGPD estão sendo rigorosamente cumpridos.

Por exemplo, uma auditoria pode revelar que determinadas informações pessoais estão sendo acessadas por mais colaboradores do que o necessário. Com esse diagnóstico, a organização pode implementar ações corretivas, como o ajuste de permissões de acesso, garantindo que apenas pessoas autorizadas acessem esses dados e reforçando a proteção à privacidade dos titulares.

Segundo Módulo (2021) a condução futura das operações relacionadas à gestão de riscos, proteção de dados pessoais, privacidade, segurança da informação e cibernética é atuar em conjunto para obtenção de melhores resultados e otimização de recursos, uma vez que tais domínios são interdependentes e mutuamente correlacionados.

O alinhamento das práticas de continuidade de negócios com os requisitos da LGPD, não apenas fortalece a resiliência operacional da organização, mas também evidencia seu zelo pela proteção dos dados e privacidade, elementos fundamentais para a sustentabilidade e reputação corporativa no cenário atual da era de dados.

3. Metodologia

O desenvolvimento deste estudo adotou o método hipotético-dedutivo, empregando pesquisa bibliográfica, pesquisa documental e estudo de caso de um PCN implementado por uma empresa privada. A pesquisa bibliográfica foi conduzida em fontes como livros, artigos científicos, dissertações e outras publicações pertinentes, visando fundamentar o trabalho. Quanto à pesquisa documental, esta se concentrou na análise de PCNs disponibilizados para consulta pública, proporcionando *insights* relevantes para a investigação em questão.

Lakatos e Marconi (2021) definem que o método constitui um conjunto de atividades sistemáticas e racionais, as quais viabilizam a obtenção do objetivo, de maneira mais segura e eficiente, traçando o percurso a ser seguido, identificando equívocos e subsidiando as escolhas do pesquisador.

O fio condutor da pesquisa iniciou com a importância do PCN, seguido da sua utilização como ferramenta para adequação à LGPD, destacando os seus principais aspectos que podem efetivamente contribuir para um *compliance* com a lei em questão.

A próxima seção aborda uma breve análise de um PCN sob a óptica de sua eficiência no atendimento aos requisitos necessários para uma organização estar em conformidade com a LGPD. É importante ressaltar que o objetivo maior da pesquisa é fomentar uma reflexão sobre o potencial que um PCN possui para auxiliar as organizações no atendimento às premissas da LGPD.

4. Resultados e Discussões

A pesquisa constatou a relevância da implementação de um plano de continuidade de negócios como medida essencial para garantir os pilares da segurança da informação em organizações, e consequentemente, a sua eficácia enquanto ferramenta para adequação à LGPD.

Com o intuito de fundamentar a pesquisa, optou-se por uma breve análise de um PCN disponibilizado no site de uma empresa privada, sob a óptica de atendimento à confidencialidade, integridade e disponibilidade das informações.

4.1 Análise do PCN da empresa privada Macrebank

O Macrebank, instituição financeira digital, foi concebido como uma extensão estratégica da empresa Atacadão Macre, atuante no segmento de atacado e varejo alimentar, primordialmente na região sul do Pará, onde mantém estabelecimentos do tipo Atacarejo e minimercados.

Sua criação visa prover diretamente aos clientes benefícios tangíveis diante das dificuldades enfrentadas em áreas remotas, tais como infraestrutura viária precária, restrições de acesso a entidades governamentais e instituições financeiras convencionais. A proposta de um banco digital representa uma resposta eficaz a tais desafios, oferecendo serviços que transcendem as barreiras geográficas e fornecendo funcionalidades análogas às de uma instituição bancária tradicional.

A empresa publicou o seu PCN em 2022 (Macrebank, 2022) e o define como (PCN = PAC + PCO + PRD), sendo:

PAC - Programa de Administração da Crise: envolve todo os processos;

PCO - Plano de Continuidade Operacional: ênfase nos processos de negócio;

PRD - Plano de Recuperação de desastres: visa a recuperação e/ou restauração de componentes que sustentam o PCN.

A Tabela 1 ilustra os pontos importantes que destacam a fundamentação do PCN nos três pilares da segurança da informação:

Tabela 1 - Aspectos dos três pilares CID no PCN da empresa Macrebank

Confidencialidade	Integridade	Disponibilidade
políticas internas e normativas com papéis e responsabilidades;	monitoramento do ambiente de negócios e serviços de TI;	ambiente tecnológico redundante;
identificação, classificação e documentação dos processos críticos;	testes de validação dos <i>backups</i> ;	recuperação tempestiva das operações vitais;
sessões de divulgação para todos os colaboradores e envolvidos no processo;	boas práticas para manutenção dos <i>backups</i> .	armazenamentos dispostos em zonas de disponibilidades e contas diferentes no provedor de <i>Cloud</i> ;

Confidencialidade	Integridade	Disponibilidade
programa de treinamento para todos os colaboradores e envolvidos no processo.	-----	testes regulares de eficiência e efetividade;
-----	-----	plano de contingência de TI.

Fonte: Autoria própria, 2024

Certamente, os aspectos destacados na tabela podem contribuir significativamente para a conformidade com a LGPD. A abordagem abrangente adotada pela empresa Macrebank, abordando os pilares de Confidencialidade, Integridade e Disponibilidade em seu PCN, reflete um compromisso sólido com a segurança da informação.

O estabelecimento de políticas internas, a identificação e documentação de processos críticos, e as sessões de divulgação e treinamento evidenciam a preocupação com a Confidencialidade. Por sua vez, a realização de testes e boas práticas relacionadas a *backups* assegura a Integridade dos dados. Além disso, a redundância tecnológica, a recuperação tempestiva de operações vitais e o plano de contingência de TI destacam-se como medidas essenciais para manter a Disponibilidade dos serviços.

Essas práticas, quando implementadas de maneira consistente, não apenas fortalecem a segurança da informação, mas também posicionam a empresa de acordo com as exigências da LGPD, garantindo a proteção adequada dos dados pessoais.

5. Considerações Finais

O ambiente de negócios é dinâmico, e as ameaças potenciais podem evoluir ao longo do tempo, por isso, a revisão e adaptação contínua do PCN são imperativas. A análise regular de riscos, juntamente com a atualização dos procedimentos e tecnologias, assegura que o plano permaneça resiliente e alinhado com as demandas emergentes do cenário atual.

Portanto, um PCN não apenas fortalece a resiliência operacional de uma organização, ajudando a garantir a continuidade de suas operações em situações adversas, mas também desempenha um papel fundamental na proteção dos dados pessoais e na conformidade com a LGPD, abordando os pilares de confidencialidade, integridade e disponibilidade das informações.

Além disso, vale ressaltar que a LGPD não somente exige a proteção adequada dos dados, mas também promove a transparência e a responsabilidade no tratamento dessas informações. Nesse contexto, o PCN não apenas atende às exigências legais, mas também estabelece uma base sólida para a cultura de segurança da informação dentro da organização, o que é fundamental para a manutenção de uma postura proativa em relação à segurança.

Em resumo, a integração de políticas, práticas e tecnologias eficazes em um PCN reflete uma abordagem abrangente para enfrentar os desafios complexos associados à segurança da informação e à privacidade de dados, se alinhando aos princípios fundamentais da LGPD.

Referências

- ADVISERA. **NFPA 1600 vs. ISO 22301** – Similarities and differences, 2021. Disponível em: <https://advisera.com/27001academy/blog/2013/11/05/nfpa-1600-vs-iso-22301-similarities-and-differences/>. Acesso em 03 nov. 2023.
- BANCO DO BRASIL. **Política da gestão da continuidade dos negócios: segurança**, 2022. Disponível em: <https://www.bb.com.br/site/pra-voce/seguranca/politica-de-gestao-da-continuidade-de-negocios/#/>. Acesso em: 18 jan. 2024.
- BRASIL. **Lei geral de proteção de dados**: Lei nº 13.709, de 14 de agosto de 2018. Brasília/DF: Diário Oficial da República Federativa do Brasil Diário Oficial da União, Brasília, DF, 15 ago. 2018. p.59.
- BRUNO, Diogo; COSTA Margarida; RODRIGUES, Fernando. **Auditoria a planos de continuidade de negócio**. ISCAL, 2020. Disponível em: <http://hdl.handle.net/10400.21/12731>. Acesso em 20 dez. 2023.
- GONÇALVES, Luís. **Cinco mudanças que estão convergindo na atual era dos dados**. Forbes Collab, 2023. Disponível em: <https://forbes.com.br/forbes-collab/2023/04/luis-goncalves-cinco-mudancas-que-estao-convergindo-na-atual-era-dos-dados/> . Acesso em 27 jul. 2023.
- ISO/IEC 22301. INTERNATIONAL STANDARD. **Security and resilience: business continuity management systems: requirements**, 2019.
- ISO/IEC 27001. INTERNATIONAL STANDARD. **Information security, cybersecurity and privacy protection: information security management systems: requirements**, 2022.
- ISO/IEC 27002. INTERNATIONAL STANDARD. **Information security, cybersecurity and privacy protection: information security controls**, 2022.
- KPMG. **Pesquisa da maturidade dos planos de continuidade de negócios no Brasil**, 2021. Disponível em: https://assets.kpmg.com/content/dam/kpmg/br/pdf/2022/1/2021_Maturidade%20dos%20PCN_KPMG_final.pdf. Acesso em: 19 dez. 2023.
- KYNDRYL. **O que é um plano de continuidade de negócios?**. 2022. Disponível em: <https://www.kyndryl.com/br/pt/learn/plan#:~:text=O%20planejamento%20de%20continuidade%20de,in%C3%ADcio%20da%20d%C3%A9cada%20de%201970>. Acesso em: 23 nov. 2023.
- LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica 1**. 9. ed. São Paulo: Atlas, 2021. p.83.
- MACREBANK. **Plano de continuidade de negócios**. Macre Empreendimentos Financeiros

Ltda., 2022. Disponível em: <https://macrebank.com.br/plano-de-continuidade-de-negocio.pdf>. Acesso em: 19 jan. 2024.

MÓDULO. **Risk & privacy & cibersecurity**, 2021. Disponível em: <https://www.modulo.com.br/>. Acesso em: 18 jan. 2024.

OLIVEIRA, A. B. de, FERNANDES, G. H. M., LUZIA, B. B., & SEVERIANO JÚNIOR, E. (2024). **Mortalidade das micro e pequenas empresas: a importância de um plano de continuidade de negócios**. *Revista De Gestão E Secretariado*, 15(7), e3879. Disponível em: <https://doi.org/10.7769/gesec.v15i7.3879>. Acesso em: 08 nov. 2024.

PEREIRA, J. R. **Gestão de backup: um estudo de caso numa empresa prestadora de serviços de full outsourcing**. Trabalho de conclusão de curso em Tecnologia em Segurança da Informação. Faculdade de Tecnologia de Americana, Americana, 2018. Disponível em: <http://ric.cps.sp.gov.br/handle/123456789/3235>. Acesso em: 19 jan. 2024.

SANTOS, Paulino Ferreira dos. **Plano de continuidade de negócio**. Lisboa: Universidade Lusófona de Humanidades e Tecnologias. 2019. Disponível em: <http://hdl.handle.net/10437/10111>. Acesso em: 18 dez. 2023.

TI INSIDE. **Pandemia: apenas 12% das empresas tinham planos de continuidade de negócios ou gestão de crise**. TI Inside, 15 setembro 2020. Disponível em: <https://tiinside.com.br/15/09/2020/pandemia-apenas-12-das-empresas-tinha-planos-de-continuidade-de-negocios-ou-gestao-de-crises/>. Acesso em: 24 abr. 2024.