Universidade Federal de Ouro Preto
Instituto de Ciências Exatas e Aplicadas
Departamento de Computação e Sistemas

Política de *backup* e restauração: um estudo de caso em uma cooperativa de trabalho médico

Leonardo Sartori de Andrade

TRABALHO DE CONCLUSÃO DE CURSO

ORIENTAÇÃO:
Helen de Cassia Sousa da Costa Lima

Julho, 2023
João Monlevade–MG

Leonardo Sartori de Andrade

Política de *backup* e restauração: um estudo de caso em uma cooperativa de trabalho médico

Orientador: Helen de Cassia Sousa da Costa Lima

Monografia apresentada ao curso de Engenharia da Computação do Instituto de Ciências Exatas e Aplicadas, da Universidade Federal de Ouro Preto, como requisito parcial para aprovação na Disciplina "Trabalho de Conclusão de Curso II".

Universidade Federal de Ouro Preto

João Monlevade

Julho de 2023

SISBIN - SISTEMA DE BIBLIOTECAS E INFORMAÇÃO

A553p Andrade, Leonardo Sartori de.
Política de backup e restauração [manuscrito]: um estudo de caso em uma cooperativa de trabalho médico. / Leonardo Sartori de Andrade. - 2023.
73 f.: il.: color., tab..

Orientadora: Profa. Dra. Helen de Cassia Sousa da Costa Lima.
Monografia (Bacharelado). Universidade Federal de Ouro Preto. Instituto de Ciências Exatas e Aplicadas. Graduação em Engenharia de Computação .

1. Administração de risco. 2. Banco de dados - Medidas de segurança. 3. Ciberterrorismo. 4. Computadores - Medidas de segurança. 5. Cooperativas médicas. 6. Governança corporativa. 7. Proteção de dados. 8. Recuperação de dados (Computação). I. Lima, Helen de Cassia Sousa da Costa. II. Universidade Federal de Ouro Preto. III. Título.

CDU 004.056

Bibliotecário(a) Responsável: Flavia Reis - CRB6-2431

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
INSTITUTO DE CIENCIAS EXATAS E APLICADAS
DEPARTAMENTO DE COMPUTACAO E SISTEMAS

FOLHA DE APROVAÇÃO

Leonardo Sartori de Andrade

Política de *Backup* e *Restore*: um estudo de caso em uma cooperativa de saúde

Monografia apresentada ao Curso de Engenharia da Computação da Universidade Federal
de Ouro Preto como requisito parcial para obtenção do título de Bacharel em Engenharia da Computação

Aprovada em 01 de setembro de 2023.

Membros da banca

Doutora - Helen de Cassia Sousa da Costa Lima - Orientadora - Universidade Federal de Ouro Preto
Doutora - Lucnéia Souza Maia - Universidade Federal de Ouro Preto
Mestre - Alexandre Magno de Sousa - Universidade Federal de Ouro Preto

Helen de Cassia Sousa da Costa Lima, orientadora do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 16/09/2023.

Documento assinado eletronicamente por **Helen de Cassia Sousa da Costa Lima**, **PROFESSOR DE MAGISTERIO SUPERIOR**, em 16/09/2023, às 06:46, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0585016** e o código CRC **4B6FAF33**.

R. Diogo de Vasconcelos, 122, - Bairro Pilar Ouro Preto/MG, CEP 35402-163
Telefone: (31)3808-0819 - www.ufop.br

Dedico este trabalho aos meus pais por fornecerem a estrutura e apoio necessários para a minha formação. Aos meus avós, cujo amor e sabedoria transcenderam gerações. Por fim, dedico a mim mesmo por não desistir dos meus sonhos, por enfrentar as dificuldades com determinação, e por nunca deixar de acreditar em meu potencial.

Agradecimentos

Em primeiro lugar, gostaria de agradecer à Universidade Federal de Ouro Preto, que proporcionou a estrutura acadêmica necessária para o desenvolvimento do meu conhecimento e habilidades ao longo destes anos. Agradeço a todos os professores e funcionários que tornaram a minha jornada pela graduação enriquecedora e gratificante. Sobretudo àqueles educadores que se tornaram amizades, Alexandre Magno de Sousa, Anliy Natsuyo Nashimoto Sargeant e Adam James Sargeant, aos quais possuo extremo carinho e estima.

Um agradecimento especial a minha orientadora, Helen de Cássia Sousa da Costa Lima, que acreditou em mim, dedicou seu tempo, conhecimento e paciência para me guiar neste projeto.

Não posso deixar de mencionar meus colegas de classe e amigos. A parceria e vínculos criados durante esses anos são únicos. Vários foram os momentos de alegria, felicidade e risadas, mesmo em contextos dificultosos e caóticos. Estendo também, o sentimento de agradecimento pela parceria e cumplicidade, a minha namorada, que foi a maior incetivadora em momentos difíceis desta jornada.

Quero expressar meu agradecimento à Coop Saúde, que confiou no meu trabalho, me dando a oportunidade e fornecendo o suporte necessário para a realização deste trabalho.

Por último, e não menos importante, ao Eddie Vedder e à banda Pearl Jam, por existirem e produzirem as melhores melodias.

Agradeço profundamente a todos que contribuíram para a realização deste trabalho de conclusão de curso. Esta conquista não teria sido possível sem o apoio e incentivo de pessoas incríveis ao meu redor.

"The cosmos is within us. We are made of star-stuff. We are a way for the universe to know itself."

— Carl Sagan (1934 – 1996),
in: Cosmos.

Resumo

O crescente aumento do número de ciberataques no Brasil, somado à necessidade de adequação à LGPD, incentivou uma cooperativa de trabalho médico, organização do estudo de caso desse trabalho, a adotar medidas de melhoria na gestão da informação e proteção de dados, por meio da implantação de uma política de *backup* e restauração. A ausência de um modelo predefinido de política e a complexidade do tema motivou o desenvolvimento e proposta de uma metodologia para implantação de tal política na organização. Por meio de uma revisão bibliográfica e estudo de conceitos, normativas, legislações e *frameworks* relacionados à proteção de dados e gestão de cibersegurança, foi possível extrair uma metodologia. A partir disso, levantou-se a hipótese de que a metodologia pode ser implementada num cenário real e resultar em uma política de *backup* e restauração que atenderá as expectativas da organização. A construção da metodologia, baseada na fundamentação teórica estudada, considerando os aspectos específicos e contexto estratégico da organização, levou ao sucesso da criação e implantação da política de *backup* e restauração dentro da organização alvo. A implementação da política aprimorou a garantia de disponibilidade e segurança das informações da organização, apoiou no cumprimento de legislações e normativas e implementou procedimentos de restauração e recuperação de dados, mitigando riscos críticos da organização.

Palavras-chaves: *backup*. segurança da informação. restauração de dados. gestão de riscos. política corporativa. política de *backup*.

Abstract

The increasing number of cyberattacks in Brazil, coupled with the need for compliance with LGPD, encouraged a medical cooperative, the subject of this case study, to adopt measures to improve information management and data protection through the implementation of a backup and restoration policy. The absence of a predefined policy model and the complexity of the subject motivated the development and proposal of a methodology for implementing such a policy within the organization. Through a literature review and the study of concepts, regulations, laws, and frameworks related to data protection and cybersecurity management, it was possible to extract a methodology. Based on this, the hypothesis was raised that the methodology can be implemented in a real-world scenario and result in a backup and restoration policy that meets the organization's expectations. The construction of the methodology, based on the studied theoretical foundation, considering the specific aspects and strategic context of the organization, led to the successful creation and implementation of the backup and restoration policy within the target organization. The implementation of the policy improved the availability and security of the organization's information, supported compliance with regulations and laws, and implemented data restoration and recovery procedures, mitigating critical risks to the organization.

Key-words: *backup*. information security. data restoration. risk management. corporative policy. *backup* policy.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

ABNT Associação Brasileira de Normas Técnicas

ANS Agência Nacional de Saúde Suplementar

APF Administração Pública Federal

CFM Conselho Federal de Medicina

CIS *Center for Internet Security*

DPO *Data Protection Officer*

GDPR Regulamento Geral de Proteção de Dados

IEC *International Electrotechnical Commission*

IG Grupo de Implementação de Controles CIS

IGs Grupos de Implementação de Controles CIS

ISO *International Organization for Standardization*

LGPD Lei Geral de Proteção de Dados Pessoais

NIST *National Institute of Standards and Technology*

PCN Plano de Continuidade de Negócios

PwC *PricewaterhouseCoopers*

RN Resoluções Normativas

RPO *Recovery Point Objective*

RTO *Recovery Time Objective*

SGSI sistema de gestão da segurança da informação

SI Segurança da Informação

SLA *Service Level Agreement*

TI Tecnologia da Informação

Sumário

1 Introdução

A evolução do processo de proteção de dados, desde os eventos do atentado de 11 de setembro até a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD) Brasil (2018a), no Brasil, demonstra uma notável transformação na forma como a sociedade lida com a privacidade e a segurança das informações pessoais. Ao longo deste período, várias mudanças legais e tecnológicas moldaram esse cenário. Após os trágicos ataques de 11 de setembro de 2001, a segurança nacional tornou-se uma prioridade global. Isso levou a uma expansão significativa da vigilância governamental e das políticas de coleta de dados em nome da segurança nacional. Leis como o USA PATRIOT Act Government (2001) nos Estados Unidos permitiram uma maior coleta de informações pessoais sem o consentimento explícito dos cidadãos, levantando preocupações sobre privacidade.

Na última década, as redes sociais e as empresas de tecnologia começaram a desempenhar um papel cada vez mais importante na coleta e no uso de dados pessoais. O Facebook e o Google, por exemplo, foram alvo de críticas por suas práticas de privacidade e coleta de dados. Neste contexto, a União europeia começou a introduzir regulamentos mais rigorosos sobre a proteção de dados, como o Regulamento Geral de Proteção de Dados (GDPR) Europeu (2018), que entrou em vigor em 2018. A partir deste, instaurou-se um novo padrão global para a proteção de dados, dando aos cidadãos mais controle sobre suas informações pessoais e impondo penalidades significativas para o descumprimento da regulamentação. Isso incentivou outros países a adotar regulamentações semelhantes ou a fortalecer suas leis de proteção de dados. Em 2018, o Brasil promulgou a LGPD, inspirada pelo GDPR. Esta lei estabeleceu direitos individuais sobre dados pessoais, exigiu o consentimento explícito para a coleta e processamento de informações e impôs obrigações rigorosas às empresas no tratamento de dados pessoais, nos aspectos de proteção de dados e cibersegurança.

Uma pesquisa da *PricewaterhouseCoopers* (PwC) apontou aumento do investimento em cibersegurança por parte das empresas brasileiras, para o ano de 2022 (PWC, 2021). Todavia, apenas o investimento em tecnologia e infraestrutura não garantem a gestão e proteção da informação. O crescente aumento do número de ciberataques no Brasil (EFE, 2021), somado à necessidade de adequação à LGPD Brasil (2018a), incentivou uma cooperativa de trabalho médico, organização do estudo de caso desse trabalho, a adotar medidas de melhoria na gestão da informação e proteção de dados. Como parte integrante de seu programa de Segurança da Informação (SI) e proteção de dados, trazendo mais rigor e robustez aos procedimentos operacionais de *backup* já existentes, a cooperativa decidiu implantar uma política de *backup* e restauração.

De acordo com Sasso (2020), o armazenamento, *backup* e recuperação de dados são parte do processo da proteção de dados e da SI que, por sua vez, possui normas técnicas, como a *International Organization for Standardization* (ISO)/*International Electrotechnical Commission* (IEC) 27001 ABNT (2013a) e a ISO/IEC 27002 ABNT (2013b), bem como *frameworks* diretamente relacionados a ele, tais como o *Cybersecurity Framework* NIST (2018) da *National Institute of Standards and Technology* (NIST) e o *Critical Security Controls V.8* CIS (2021) da *Center for Internet Security* (CIS).

1.1 Definição do problema

Tratando-se da SI, mesmo que uma organização possua mecanismos de segurança e proteção dos dados, ainda existem riscos de perda, dano ou roubo da informação (HINTZBERGEN et al., 2018). Nesse contexto, a disponibilidade da informação é um princípio básico, que deve ser garantido com diretrizes e rotinas em conformidade com as demais políticas e plano de continuidade do negócio, fomentando a sustentação da empresa no mercado (PEREIRA, 2018).

A garantia de disponibilidade da informação, no processo de recuperação de um incidente envolvendo perda ou roubo de dados, se dá principalmente pela existência de cópias de segurança funcionais (KENNEDY et al., 2022). Evidentemente, os procedimentos de *backup* servem de sustentação para um plano de recuperação de desastre. Portanto, é vital determinar diretrizes e planos de *backup* e restauração eficientes e eficazes, que garantam a salvaguarda dos dados enquanto ativo, que proporcionem o sucesso da execução de uma recuperação de incidente ou desastre, e tragam segurança e confiança para as organizações. Por esses e outros motivos, a cooperativa do estudo de caso desta pesquisa decidiu implantar uma política de *backup* e restauração de dados.

Dado que não há um modelo de política de *backup* predefinido e que cada organização possui seu próprio contexto, esta lacuna no conhecimento instigou o autor deste estudo a apresentar uma metodologia para a concepção e implantação de políticas de *backup* e restauração. Acredita-se que essa metodologia possa ser implementada com êxito e resultar em uma política de *backup* e restauração que atenderá as expectativas de uma organização da área da saúde, no que tange ao seu processo de proteção de dados. Busca-se provar essa hipótese por meio da investigação das seguintes questões de pesquisa:

1. Como as necessidades específicas de proteção de dados da organização alvo influenciam o desenvolvimento da política de *backup* e restauração?

2. Em que medida a implementação da política de *backup* e restauração personalizada melhora a garantia da disponibilidade de dados na organização?

3. A política de *backup* e restauração desenvolvida está em conformidade com os regulamentos específicos da organização?

4. Como uma política de *backup* e restauração personalizada impacta a segurança de dados sensíveis e informações críticas de saúde da organização?

5. Como a política de *backup* e restauração afeta a capacidade de recuperação de dados críticos em situações de emergência, como desastres naturais ou violações de segurança?

6. Como os resultados da pesquisa apoiam ou refutam a hipótese de que a metodologia pode ser implementada com êxito e resultar em uma política de *backup* e restauração que atende às expectativas da organização alvo?

1.2 Objetivos

O objetivo geral desse trabalho é propor uma metodologia para o desenvolvimento de uma política de *backup* e restauração, aplicada em uma organização do ramo da saúde, trazendo um estudo de caso em uma cooperativa de trabalho médico.

Com a finalidade de alcançar o objetivo geral, tem-se os seguintes objetivos específicos:

- Avaliar as necessidades da organização de saúde alvo;
- Desenvolver a metodologia para implantação da política de *backup* e restauração personalizada;
- Aplicar a metodologia proposta em um cenário real (estudo de caso);
- Apresentar o estudo de caso;
- Validar a hipótese da pesquisa.

1.3 Metodologia

A partir de uma pesquisa na literatura sobre normativas do padrão ISO/IEC e de *frameworks* em gestão de riscos de segurança da informação, busca-se extrair uma metodologia para o desenvolvimento de uma política de *backup* e restauração. Em relação a sua natureza, este trabalho consiste em uma pesquisa aplicada, objetivando demonstrar a aplicação da metodologia proposta em um cenário real, de forma a validar ou refutar a hipótese de pesquisa proposta.

Considerando que o objetivo deste trabalho é propor uma metodologia, isto é, propor um caminho ou sistematização para alcançar um resultado, os passos daquele são assim definidos:

- Levantamento das necessidades da organização quanto a política de *backup* e restauração;
- Definição das variáveis de negócio;
- Definição das responsabilidades;
- Definição do escopo da política;
- Desenvolvimento do texto da política e aprovação das áreas responsáveis;
- Cronograma de implantação da Política;
- Manutenção e revisão da Política.

1.4 Resultados Obtidos

Por meio do estudo da bibliografia, foi possível extrair uma metodologia para implantação de uma política de *backup* e restauração em uma determinada organização, aplicá-la como um estudo de caso, responder as questões de pesquisa levantadas e demonstrar os principais resultados e impactos imediatos que a política trouxe para a empresa.

1.5 Organização do trabalho

O restante deste trabalho é organizado como se segue. O Capítulo 2 é responsável por apresentar conceitos relativos à *backup* e políticas de *backup* e *frameworks* utilizados como embasamento para a estruturação da política de *backup* e restauração, bem como os trabalhos relacionados presentes na literatura. No Capítulo 3, serão abordados cada um dos itens presentes na Seção 1.3 e o estudo de caso. No Capítulo 4, é apresentado o resultado do trabalho e da implantação da política na organização do estudo de caso. Por fim, no Capítulo 5, constam as conclusões deste trabalho, dificuldades enfrentadas, oportunidades de melhoria e considerações finais.

2 Revisão bibliográfica

Neste capítulo, serão apresentados conceitos relativos a *backup*, tipos de *backup* e política de *backup*, uma introdução às leis, normativas e *frameworks* que se relacionam com controles de *backup* e restauração e os trabalhos relacionados. Os conceitos abordados a seguir são fundamentais para o entendimento do objeto de estudo desse trabalho, seu objetivo e relevância para uma organização.

2.1 *Backup* e conceitos relacionados

Backup é um termo da língua inglesa que não possui tradução equivalente para a língua portuguesa, e pode ser descrito como cópia de segurança de arquivos. O principal objetivo do *backup* é prevenir ou proteger contra a perda de dados (ABNT, 2013b).

Diversos tipos de *backup* podem ser explorados - *backup* em nuvem, *backup* local, *backup* externo, *backup* remoto, dentre outros - e, essencialmente, diferem entre si pelo local onde são realizados. Contudo, apesar dessa distinção, os *backups* são caracterizados por uma estratégia composta por objetivo e características comuns que os definem. A essa estratégia a ISO 27002 (ABNT, 2013b) denomina abrangência do *backup*. As principais abrangências de *backup* são: *backup* total ou completo, *backup* incremental, *backup* clone e *backup* diferencial, sendo a primeira primordial para a existência das demais (SOMASUNDARAM; SHRIVASTAVA et al., 2009).

O *backup* total consiste em gravar exatamente todos os dados do recurso a ser *backupeado*[1] (SASSO, 2020). Na estratégia do *backup* diferencial, são gravados todos os dados novos ou alterados, baseando-se no último *backup* completo. Sempre haverá uma dependência em relação à última cópia completa (SASSO, 2020). No *backup* incremental, são copiados apenas os arquivos que sofreram alteração desde o último *backup* realizado, seja ele completo ou diferencial (SASSO, 2020). Por fim, o *backup* clone consiste em uma cópia exata dos dados originais do recurso de forma que todas as alterações realizadas nos dados originais são replicadas no arquivo de *backup* (SASSO, 2020).

Na Tabela 1 Sasso (2020) faz uma comparação entre essas diferentes estratégias de *backup*, demonstrando as vantagens e desvantagens práticas de cada uma delas.

[1] Termo que se refere a informação que passou pelo processo de cópia de segurança (*backup)*

Tipos de *Backup*	**Dados de *Backup***	**Tempo de *Backup***	**Tempo de Restauração**	**Espaço de Armazenamento**
Backup full	Todos os dados	Muito lento	Rápido	Grande
Backup incremental	Somente arquivos novos/modificados desde a última cópia	Rápido	Moderado	Pouco
Backup diferencial	Somente arquivos novos/modificados desde a última cópia completa	Moderado	Rápido	Moderado
Backup clone	Todos os dados	Muito rápido	Muito rápido	Muito grande

Tabela 1 – Comparação entre as estratégias de *backup*

Fonte: Sasso (2020)

2.1.1 Conceitos de recuperação

Recovery Point Objective (RPO) e *Recovery Time Objective* (RTO) são conceitos que irão apoiar o plano de recuperação de desastre e estão intimamente ligados ao plano de *backup* da organização (SASSO, 2020). O RPO está relacionado ao nível de tolerância a perdas aceito pela organização, isto é, em caso de um desastre, congelamento ou queda de algum ambiente, qual é o ponto de retorno, qual é o *backup* que será utilizado para retomada da atividade? Isso diz respeito à quantidade de perda de informação, trabalho e tempo de produção que a organização pode assumir. Por exemplo, se o RPO do sistema de gestão de uma empresa é de 4 horas, no mínimo, o banco de dados desse sistema deve ter um *backup* completo de 4 em 4 horas, já que toda alteração realizada desde o último *backup* até o momento do desastre pode ser perdida.

O RTO, por sua vez, está relacionado à quantidade de tempo que o sistema ou recurso pode ficar fora do ar, paralisado ou inacessível, sem que gere danos, financeiros ou reputacionais significativos (SASSO, 2020). O RTO irá influenciar na infraestrutura e tecnologias utilizadas pela organização, no que diz respeito à disponibilidade dos recursos e tempo de recuperação de ambientes, levando em consideração o *Service Level Agreement* (SLA) de terceiros, se necessário. Cada tecnologia ou estratégia de manutenção dos ambientes demanda um investimento, logo é aconselhável que haja um mapeamento dos ambientes, sistemas e recursos críticos para a empresa, qual irá nortear as definições de RPO e RTO (SASSO, 2020).

2.2 Política de *backup* e restauração

Antes de discorrer sobre a política de *backup*, é essencial compreender o conceito e a finalidade de uma política corporativa. Levando em consideração o contexto da segurança da informação, de acordo com a ISO 27003 ABNT (2020), a organização deve analisar aspectos internos e externos que afetam a segurança da informação. Ainda conforme a norma, as questões internas estão sujeitas ao controle da organização e a análise dessas questões pode incluir, mas não se limita a: cultura da organização; políticas, objetivos e estratégias para alcançá-los; normas, diretrizes e modelos adotados pela organização, que servirão para determinar o escopo do sistema de gestão, as ações para contemplar os riscos e dar suporte a análise crítica da direção (ABNT, 2020, p. 2 e 3). Em suma, a política corporativa é usada como instrumento de controle interno e é produto da análise das questões internas da organização, sendo o componente principal de um sistema de gestão.

De acordo com a ISO 27003 ABNT (2020, p. 17), uma política deve descrever a importância estratégica do sistema de gestão e deve conter declarações de intenção e direcionamentos breves, isto é, não compete à política descrever os processos e atividades

em baixo nível e detalhadamente. Este detalhamento deve ser abordado em procedimentos operacionais, que apoiam a política. No contexto da política de *backup*, a ISO 27002 ABNT (2013b, p. 66) sugere que procedimentos operacionais monitorem a execução das cópias de segurança e apontem falhas de *backup* programado, afim de garantir a integridade dos *backups*, de acordo com a política de *backup*.

Na norma ISO 27002 ABNT (2013b), existem orientações para as organizações utilizarem como referência no processo de seleção de controles para implementação de um sistema de gestão da segurança da informação (SGSI). No Capítulo 5, Seção 5.1.1 da norma, é sugerida a elaboração de um conjunto de políticas de segurança da informação que sejam: aprovadas pela direção, publicadas e comunicadas a todas as partes interessadas, bem como que a política de segurança da informação seja apoiada por políticas específicas, dentre as quais menciona-se a política de gestão dos *backups*, que compreende o processo de restauração das informações presentes nesses *backups*. Sendo a política de *backup* uma das políticas de segurança da informação e do SGSI, ela segue as mesmas diretrizes de construção e orientações previstas para a política de segurança da informação, presentes nas normas ISO.

2.3 Normas ISO/IEC

As Normas ABNT NBR ISO/IEC são um conjunto de normas brasileiras que adotam as normas internacionais ISO/IEC. São desenvolvidas pela Associação Brasileira de Normas Técnicas (ABNT) e têm como objetivo padronizar processos, produtos e serviços. A adoção dessas Normas é amplamente utilizada no Brasil por empresas, organizações governamentais e não governamentais e outros setores, para garantir a conformidade com os padrões nacionais e internacionais de qualidade e eficiência.

No contexto da SI e seus controles, existem três normas que são essenciais para o objeto desse trabalho: a ISO 27001 ABNT (2013a), a ISO 27002 ABNT (2013b) e a ISO 27003 ABNT (2020), sendo que a última

> "fornece orientações sobre os requisitos para um sistema de gestão de segurança da informação (SGSI) conforme especificado na ABNT NBR ISO/IEC 27001 e fornece recomendações (‘Convém que’), possibilidades (‘pode’) e permissões (‘pode’) em relação a eles.". (ABNT, 2020)

A ISO 27001 ABNT (2013a) dispõe sobre a adoção de um sistema de gestão da segurança da informação (SGSI) como uma decisão estratégica para uma organização e é uma norma que foi preparada para prover requisitos para estabelecer, manter e melhorar continuamente um SGSI dentro do contexto da organização. O SGSI é influenciado pelas necessidades, requisitos de segurança, processos organizacionais, tamanho e estrutura da

organização, sendo fundamental para preservar os princípios da SI - confidencialidade, integridade e disponibilidade da informação -, por meio da aplicação de gestão de riscos.

Dentre as contribuições presentes na ISO 27001, são relevantes para a metodologia proposta nesse trabalho:

- Seção 4.1, que dispõe sobre o contexto da organização, com o objetivo de determinar as questões internas e externas que são relevantes para o negócio;
- Seção 4.2, que dispõe sobre as necessidades e expectativas das partes interessadas, com o objetivo de determinar as partes interessadas que são relevantes para o SGSI, os requisitos dessas partes para a segurança da informação, dentre eles, requisitos legais e regulamentares, bem como obrigações contratuais;
- Seção 4.3, que dispõe sobre a determinação dos limites e aplicabilidade do SGSI, considerando as questões internas e externas do item 4.1, os requisitos do item 4.2 e as interfaces e dependências entre as atividades desempenhadas pela organização e aquelas desempenhadas por outras organizações;
- Seção 5.2, que dispõe sobre a implantação de uma política de segurança da informação que seja apropriada ao propósito da organização e que inclua os objetivos de segurança da informação (Seção 6.2) ou que forneça estrutura para estabelecer esses objetivos.

Dito que a ISO 27001 aborda as diretrizes da gestão da segurança da informação, a operacionalização dessas diretrizes é apresentada na ISO 27002 ABNT (2013b), na forma de controles de segurança da informação. Na Seção 0.1, a ISO 27002 estabelece que o alcance da segurança da informação se dá por meio da implementação de controles adequados, incluindo políticas, processos e procedimentos, além de uma estrutura organizacional que permitirá a efetividade dessas ações. A norma foi desenvolvida para as organizações:

> usarem como uma referência na seleção de controles dentro do processo de implementação de um sistema de gestão da segurança da informação (SGSI), baseado na ABNT NBR ISO/IEC 27001 ou como um documento de orientação para as organizações implementarem controles de segurança da informação comumente aceitos. (ABNT, 2013b, Seção 0.1)

Na Seção 0.2 da ISO 27002, são abordadas as principais fontes de requisitos de segurança da informação: a avaliação de riscos da organização; as legislações, estatutos, regulamentações e demais cláusulas contratuais atendidas pela organização e seus parceiros; e as particularidades da organização no que se refere aos princípios, objetivos e os requisitos de negócio envolvidos no tratamento de dados da organização. Ademais, a norma considera que a escolha dos controles a serem adotados dependem das decisões da organização, baseadas no gerenciamento dos riscos e nas legislações e regulamentações nacionais e

internacionais relevantes para o negócio. A estrutura da ISO 27002 se dá na forma de seções de controles de SI, objetivos desses controles e os controles propriamente ditos.

Considerando que uma política de *backup* compõe o escopo dos controles de um SGSI, pode-se afirmar que os fatores que influenciam o SGSI presentes na ISO 27001, assim como os requisitos de segurança da informação presentes na ISO 27002, influenciarão no desenvolvimento da política e, por isso, estão presentes na metodologia proposta neste trabalho.

2.4 Requisitos Legais

As organizações brasileiras, independentemente da área de negócio, devem obedecer determinadas legislações a fim de permanecerem em conformidade com o ordenamento jurídico, uma vez que o descumprimento de leis e normas enseja riscos legais, tais como aplicação de sanções por autoridades e órgãos reguladores e fiscalizadores de suas respectivas atividades e judicializações, além de riscos reputacionais. Estabelecer controles internos, através de políticas e diretrizes institucionais é uma forma de gerenciar riscos, conforme evidenciado nas normas ISO mencionadas na seção anterior, que tratam especificamente do gerenciamento de riscos de segurança da informação.

Nessa Seção, serão brevemente apresentados alguns artigos de algumas leis, que de alguma forma se relacionam com a segurança da informação, cujo descumprimento resulta em materialização de riscos para a organização, os quais podem ser mitigados através do desenvolvimento de uma política de *backup* e restauração.

Ressalta-se que não é objetivo deste trabalho, tampouco responsabilidade do relator de uma política de *backup* e restauração, realizar uma revisão completa e detalhada de todas as legislações que uma organização deve cumprir. Conforme descrito na ISO 27002 ABNT (2013b, Seção 0.2), os requisitos legais, presentes nas legislações e demais regulamentações serão traduzidos em requisitos de segurança da informação, gerenciáveis pelo sistema de gestão da segurança da informação e que poderão ser tratados pelas políticas e diretrizes internas da organização.

2.4.1 Lei Geral da Proteção de Dados

Promulgada no Brasil em 2018, a LGPD

> dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, 2018a, Art. 1º)

Mencionada lei se aplica a todas as organizações, públicas e privadas, que realizam tratamento de dados pessoais dos brasileiros, portanto é fundamental que as instituições estejam conscientes das exigências e obrigações dela decorrentes e adotem medidas adequadas de conformidade.

Em seu artigo 5º, a LGPD considera:

> 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; (BRASIL, 2018a, Art. 5º)

Sobre as atividades de tratamento de dados pessoais, no artigo 6º determina-se a observância dos princípios de segurança a fim de proteger os dados pessoais e a prevenção da ocorrência de danos em virtude do tratamento dos desses dados. Além disso, a responsabilidade das organizações, no que se refere a segurança das informações dos indivíduos, é reforçada nos artigos 46 e 50, nos termos de que as organizações devem adotar medidas de segurança, técnicas e administrativas capazes de proteger os dados pessoais de 'acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito'. Além disso, no âmbito de suas competências, os controladores e operadores de dados poderão criar regras de boas práticas e governança, a fim de estabelecer condições para a supervisão e mitigação de riscos relacionados ao tratamento de dados pessoais.

Tanto as formas de tratamento de dados, especialmente o arquivamento, o armazenamento e a eliminação, quanto os riscos de situações acidentais como destruição ou perda, fazem parte do escopo de uma política de *backup* e restauração. Ademais, os procedimentos de *backup* apoiam as organizações a cumprirem a LGPD, especialmente no que se refere à efetivação dos direitos dos titulares dos dados em seus diversos tipos de solicitações, previstos no Capítulo III, artigo 18 dessa lei.

2.4.2 Leis Tributárias

Toda organização brasileira deve cumprir obrigações tributárias, observando o disposto no Código Tributário Nacional, instituido pela Lei nº 5.172/1966 Brasil (1996a) que 'dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios'. Sobre essa lei, é possível extrair informações relativas ao tempo de guarda de determinadas informações de uma organização, como se infere do artigo 174, que determina um prazo de cinco anos para a União realizar uma ação de cobrança de um tributo, a partir da data em que este se tornou devido. Ou seja, o

prazo de guarda dos comprovantes de escrituração da pessoa jurídica é de 5 (cinco) anos, devendo-se considerar como prazo inicial os marcos indicados no artigo 173.

Ainda sobre o tempo de guarda de informações tributárias, desta vez com o foco no imposto de renda de pessoa jurídica, a Lei nº 9430/1996 Brasil (1996b), que dispõe sobre a legislação tributária federal e as contribuições para a seguridade social, prevê a guarda dos comprovantes de escrituração contábeis até a constituição de seus créditos, como também para evidência em possíveis auditorias e/ou fiscalizações, conforme dispostos nos artigos 37 e 40, a saber:

> Art. 37. Os comprovantes da escrituração da pessoa jurídica, relativos a fatos que repercutam em lançamentos contábeis de exercícios futuros, serão conservados até que se opere a decadência do direito de a Fazenda Pública constituir os créditos tributários relativos a esses exercícios. (BRASIL, 1996b)
>
> Art. 40. A falta de escrituração de pagamentos efetuados pela pessoa jurídica, assim como a manutenção, no passivo, de obrigações cuja exigibilidade não seja comprovada, caracterizam, também, omissão de receita. (BRASIL, 1996b)

2.4.3 Código de Defesa do Consumidor

O artigo 20, da Lei nº 8.078/1990 Brasil (1990) determina que:

> "o fornecedor de serviços responde pelos vícios de qualidade que os tornem impróprios ao consumo ou lhes diminuam o valor, assim como por aqueles decorrentes da disparidade com as indicações constantes da oferta ou mensagem publicitária, podendo o consumidor exigir (...) a restituição imediata da quantia paga, monetariamente atualizada, sem prejuízo de eventuais perdas e danos;"(BRASIL, 1990)

Isto é, para que uma organização tenha condições de cumprir com o disposto no artigo acima, é essencial que ela mantenha guarda de registros de pagamentos realizados pelos seus clientes, podendo o cliente solicitar reparação de danos até um prazo de cinco anos, a contar da data do conhecimento do dano ou de sua autoria, conforme previsto no artigo 27 dessa mesma lei.

2.4.4 Previdência Social

Outros registros que devem ser mantidos pela pessoa jurídica são as informações relacionadas no parágrafo 1º, do artigo 125-A, da Lei nº 8.213/1991 Brasil (1991), que determina que 'a empresa disponibilizará a servidor designado por dirigente do INSS os documentos necessários à comprovação de vínculo empregatício, de prestação de serviços e de remuneração relativos a trabalhador previamente identificado.'.

Se estabelece então uma conexão indireta entre o cumprimento desse artigo com os processos de guarda e *backup* de informações vigentes na empresa, pois esses processos devem ser capazes de respeitar o tempo de retenção (temporalidade) do dado e dar suporte ao ciclo de vida do dado dentro da organização.

2.4.5 Lei 13.787/18

Além das leis federais aplicáveis a todas as organizações, existem leis específicas para determinados ramos de negócio, a exemplo a Lei nº 13.787/2018 Brasil (2018b) que se aplica diretamente à Coop Saúde e outras instituições que trabalham com o manuseio de informações médicas de seus clientes.

A lei dispõe sobre a digitalização e o uso de sistemas informatizados para o armazenamento e o manuseio de prontuário de paciente. O artigo 2º deixa claro o papel dos controles de segurança da informação relacionados aos prontuários, determinando que o processo de digitalização de prontuário de paciente deve assegurar a confidencialidade, integridade e disponibilidade do documento digital, sendo que o artigo 6º prevê a eliminação desses dados somente após decorrido um prazo mínimo de vinte anos, a contar do último registro no prontuário do paciente.

Ao longo da Seção 2.4, foram citados componentes legislativos que referenciam o tempo de guarda (temporalidade) de documentos e registros importantes para qualquer organização. Além dos quesitos de segurança da informação relativos aos dados da organização, o tempo de guarda é o fator determinante para demarcar por quanto tempo um *backup* precisa existir e em qual momento a informação original e sua cópia de segurança poderão ser eliminadas, criando condições para que o ciclo de vida da informação seja cumprido. Isso significa que, um controle de temporalidade dos dados tratados dentro da organização é: um requisito para a existência de uma política de *backup* e restauração; e uma variável de negócio importante a ser definida; de modo que as diretrizes da política devem respeitar e resguardar o tempo de guarda determinado no controle de temporalidade.

Nesse contexto, a organização alvo do estudo de caso deste trabalho, possui um controle de temporalidade dos dados chamado "Matriz de Temporalidade", descrito no Anexo A, ao final do trabalho.

2.5 Normativas da área de negócio

A depender da área de negócio, dos interesses e dos objetivos estratégicos da organização, além de observar a conformidade com a legislação, há de se observar normativas de ministérios, órgãos reguladores e conselhos referentes àquele negócio, a exemplo dos profissionais médicos brasileiros, que devem seguir normas Conselho Federal de Medicina

(CFM)[2]. Nesse contexto, considerando que a área de negócio da Coop Saúde é a saúde suplementar, a organização deve seguir obrigações preconizadas pela Agência Nacional de Saúde Suplementar (ANS)[3]. Organizações de outros contextos de negócio devem atentar-se a normativas de órgãos fiscalizadores de seu respectivo setor.

A ANS é uma autarquia especial[4] vinculada ao Ministério da Saúde do Brasil. A agência é responsável por fiscalizar e regular o setor de saúde suplementar, com o objetivo principal de proteger os direitos dos beneficiários de planos de saúde, garantindo acesso à assistência de qualidade e promovendo sustentabilidade do setor. A ANS também estabelece normas, regras e padrões para as operadoras de planos de saúde, visando a transparência e a equidade no sistema de saúde suplementar. Essas normas expedidas pela agência são denominadas Resoluções Normativas (RN).

A grande maioria das RN da ANS são de cumprimento obrigatório pelas operadoras de planos de saúde, devido ao caráter regulatório e fiscalizador da agência, como é o caso da RN nº 566 (BRASIL, 2022f), que dispõe sobre a garantia de atendimento dos beneficiários de plano privado de assistência a saúde. Existem, ainda, normativas para tratar do processo de comercialização de planos privados de saúde (BRASIL, 2022e), das formas e condições de reajustes nos preços de planos (BRASIL, 2022c), da disponibilização do conteúdo mínimo obrigatório de informações referentes aos planos (BRASIL, 2022b) e etc. Considerando o foco deste trabalho, a RN nº 518 e a RN nº 507 são dois exemplos de normativas que serão abordados com mais detalhes.

2.5.1 RN 518

A RN nº 518 Brasil (2022d) é uma normativa obrigatória, que dispõe sobre a adoção de práticas mínimas de governança corporativa, com ênfase na gestão de riscos e controles internos. A normativa estabelece os seguintes conceitos:

- governança: ‘sistema pelo qual as operadoras são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre seus proprietários, administradores, órgãos de fiscalização e controle e demais partes interessadas;’
- controles internos: ‘conjunto de medidas adotadas para salvaguardar as atividades da operadora, assegurando o cumprimento de seus objetivos e obrigações em todos os níveis da organização;’
- gestão de riscos:

[2] <https://portal.cfm.org.br/>
[3] <https://www.gov.br/ans/pt-br>
[4] Autarquia Especial: Entidade administrativa que possui autonomia em sua atuação e gestão, mas está vinculada a um ministério ou órgão do governo, atuando dentro do âmbito de competência e supervisão desse órgão.

> processo de identificação, análise, avaliação, priorização, tratamento e monitoramento de riscos que possam afetar, positiva ou negativamente, os objetivos de processos de trabalho e/ou de projetos de uma operadora nos níveis estratégicos, tático e operacional. (BRASIL, 2022d)

Em seu artigo 6º, a normativa preconiza que as operadoras devem implementar controles internos voltados para suas atividades e sistemas de informações, com o objetivo de assegurar a confiabilidade das informações, buscar a utilização eficiente dos recursos e atender à legislação e às normas internas da operadora. No artigo 9º, através do inciso III, a normativa estabelece a relação da gestão de riscos com a continuidade e sustentabilidade da organização. No artigo 10, é previsto que a gestão de riscos deve ser adequada à estrutura e aos controles internos da operadora.

Essa RN é importante pois demonstra como os controles internos, a gestão de riscos e as normas internas da organização devem estar em conformidade entre si e como impactam diretamente nas necessidades que a organização deve atender, para além de seus objetivos estratégicos como negócio.

A seguir, será apresentada uma normativa, que não possui caráter obrigatório, e que está diretamente relacionada com a RN nº 518 e com os objetivos estratégicos que a Coop Saúde busca atingir.

2.5.2 RN 507

A RN nº 507 Brasil (2022a) é a resolução que dispõe sobre o Programa de Acreditação de Operadoras de Planos Privados de Assistência à Saúde. Esse programa

> é uma certificação de boas práticas em gestão organizacional e em gestão em saúde, de caráter voluntário, realizado por Entidades Acreditadoras, cujo objetivo é a qualificação da prestação dos serviços, induzindo a mudança no modelo de atenção à saúde existente, propiciando uma melhor experiência para o beneficiário. (BRASIL, 2022a, Art. 2º)

A operadora pode se submeter de forma voluntária ao programa de acreditação e deve atender os requisitos dispostos no artigo 11. Além disso, conforme disposto no artigo 12, o programa é composto de requisitos e itens de verificação, distribuídos em dimensões, a saber:

> I - Gestão Organizacional - a dimensão 1 busca avaliar a gestão das operadoras considerando aspectos relativos à estrutura organizacional, a processos de trabalho, a governança corporativa, a gestão de riscos corporativos, a sua sustentabilidade e a melhoria da qualidade;
>
> II - Gestão da Rede Prestadora de Serviços de Saúde - a dimensão 2 busca avaliar a gestão da rede assistencial das operadoras, considerando

> critérios de qualidade para sua conformação, bem como mecanismos de regulação do acesso dos beneficiários;
>
> III - Gestão em Saúde - a dimensão 3 busca avaliar a gestão do cuidado em saúde pelas operadoras, bem como ações de monitoramento relativas à qualidade da atenção à saúde de sua rede prestadora de serviços de saúde; e
>
> IV - Experiência do Beneficiário - a dimensão 4 busca avaliar o resultado da interação entre a operadora, seus beneficiários e a sociedade, incluído potenciais beneficiários, tendo como parâmetros a percepção dos beneficiários quanto ao atendimento de suas necessidades e expectativas, bem como as ações promovidas pela operadora com foco na melhoria da qualidade dos serviços prestados.
>
> Parágrafo único. Além de ser avaliada nos itens e requisitos estabelecidos nas Dimensões elencadas neste artigo, previstas no Anexo I desta Resolução Normativa, as operadoras também serão avaliadas em relação ao cumprimento dos requisitos referentes aos processos de governança, gestão de riscos e controles internos estabelecidos no corpo da Resolução Normativa e do Anexo IA da Resolução Normativa nº 443, de 28 de janeiro de 2019 '[5]'. (BRASIL, 2022a, Art. 12)

Para que a operadora obtenha a acreditação, será avaliada a sua conformidade com os requisitos constantes no Anexo I da normativa, conforme disposto no artigo 13. Tais requisitos se relacionam com a disponibilidade e *backup* de dados que serão abordados no Capítulo 3 desde trabalho.

Alcançar acreditação na RN 507 é um dos objetivos estratégicos da Coop Saúde. Isso significa que a organização deve implementar todos os controles necessários para atingir os requisitos da norma, impactando diretamente e demonstrando a relevância do primeiro passo da metodologia: realizar o levantamento das necessidades da organização quanto a política de *backup* e restauração (e demais políticas que se fizerem pertinentes).

2.6 *Frameworks* de segurança cibernética

Nesta seção, serão apresentados dois conjuntos de ferramentas (*frameworks*) de segurança cibernética que servirão como um guia orientativo de boas práticas para a confecção de uma política de *backup* e restauração. A escolha desses dois *frameworks* foi baseada nos modelos já utilizados pela organização do estudo de caso em sua Política de Segurança da Informação e pela relação de referências entre os dois *frameworks*.

Registra-se que existem outros *frameworks* disponíveis no mercado, mas de modo geral, todos são utlizados como um guia de boas práticas em segurança da informação, para implementação de controles de segurança.

[5] A Resolução Normativa nº 443 foi revogada pela Resolução Normativa nº 518.

2.6.1 NIST *Cyberframework*

O *Cyberframework* NIST (2018) é um guia de gerenciamento de riscos de segurança cibernética desenvolvido pelo *National Institute of Standards and Technology* (NIST)[6]. O NIST é um dos laboratórios de ciências físicas dos Estados Unidos e faz parte do Departamento de Comércio dos EUA, com a missão de 'promover a inovação e a competitividade industrial do país, avançando a ciência, os padrões e a tecnologia de medição de maneira a aumentar a segurança econômica e melhorar qualidade de vida dos norte americanos'.

O *framework* ou 'Guia', conforme referenciado pelos autores, não substitui o processo de gerenciamento de segurança cibernética de uma organização, trata-se de um complemento. A decisão sobre como aplicá-lo é de responsabilidade da organização. O *framework* oferece mecanismos para que as organizações, no que tange à segurança cibernética: descrevam sua situação atual; descrevam seus objetivos; identifiquem e priorizem oportunidades de aperfeiçoamento; avaliem o progresso frente aos objetivos e comuniquem-se com os interessados sobre os riscos.

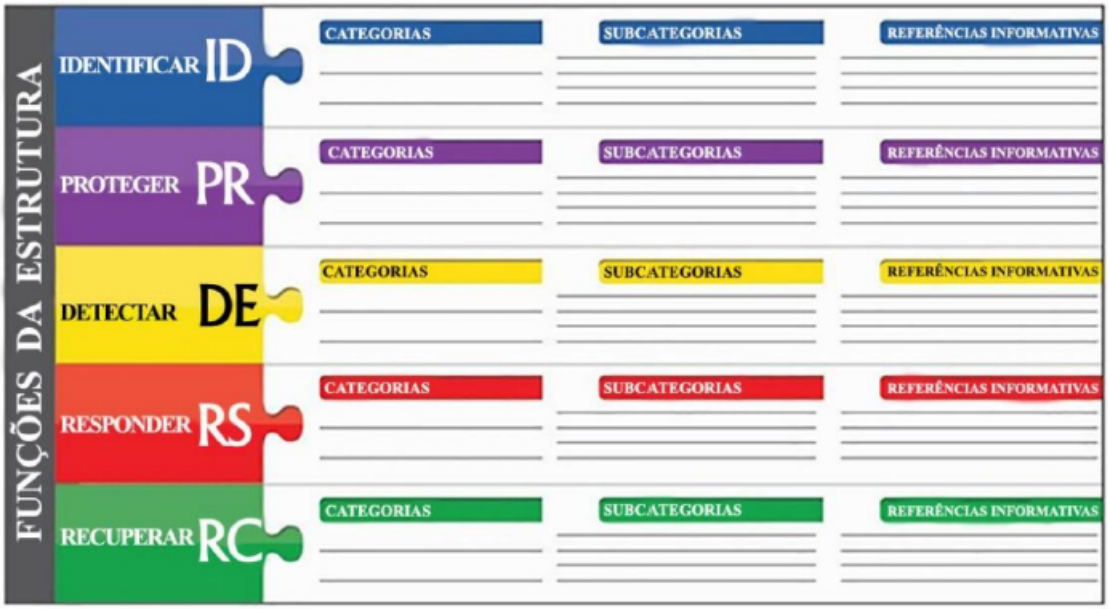
O Guia é composto por três partes: Estrutura Básica, Níveis de Implementação e Avaliações da Estrutura. A *Estrutura Básica* é um conjunto de atividades de segurança cibernética para alcançar resultados específicos, consistindo em cinco funções simultâneas e contínuas: identificar, proteger, detectar, responder e recuperar. As funções fornecem visão estratégica do ciclo de vida do gerenciamento do risco, permitindo a comunicação das atividades e dos resultados de segurança cibernética em toda a organização. Os elementos da Estrutura Básica, ilustrados na Figura 1, são:

- **Função**: é o nível mais alto das atividades básicas de segurança cibernética e auxiliam a organização a demonstrar seu gerenciamento de riscos cibernéticos, organizando as informações e possibilitando tomada de decisões.
- **Categorias**: são as subdivisões de uma Função em grupos de resultados ligados a necessidades específicas. Um exemplo de Categoria seria o "Gerenciamento de Ativos".
- **Subcategoria**: são as subdivisões de uma Categoria em resultados específicos de atividades técnicas. Através da conclusão dessas atividades mais específicas, pode-se embasar a concretização dos resultados de uma Categoria. Um exemplo de Subcategoria seria o "Mapeamento dos Ativos", afinal, não é possível gerenciar aquilo que não foi identificado/mapeado.
- **Referências Informativas**: são seções específicas de normas, diretrizes e práticas para alcançar os resultados relacionados a cada Subcategoria.

[6] <https://www.nist.gov/about-nist>

No Anexo A do Guia, constam informações detalhadas sobre a Estrutura Básica, as Classificações, Subclassificações e das Referências Informativas. No Capítulo 3, será desenvolvida a relação entre a Estrutura Básica do Guia e o processo de confecção da política de *backup* e restauração.

Figura 1 – *Organização da Estrutura Básica*



Fonte: NIST *Cyberframework*

O Guia (NIST, 2018) define as funções da seguinte forma:

1. **Identificar:** compreender o contexto da organização, dos recursos que suportam as funções críticas e dos riscos, para gerenciá-los no que tange a sistemas, pessoas, ativos, dados e recursos.

2. **Proteger:** desenvolver e implementar proteções para garantir a prestação dos serviços críticos da organização.

3. **Detectar:** desenvolver e implementar atividades para identificar a ocorrência de um evento/incidente de segurança cibernética.

4. **Responder:** desenvolver e implementar atividades para agir contra um incidente detectado.

5. **Recuperar:** desenvolver e implementar atividades para manter planos de resistência e restaurar qualquer recurso ou serviço prejudicado por um incidente de segurança cibernética.

Os *Níveis de Implementação da Estrutura* descrevem o grau em que o gerenciamento de risco implementado na organização se relaciona com as características definidas no Guia. Os níveis classificam as práticas da organização de Nível 1 a Nível 4 e auxiliam a determinar em que ponto o gerenciamento do risco de segurança se relaciona com as demandas e com as práticas de gerenciamento de risco da empresa. De acordo com o Guia, o processo de seleção de Nível deve considerar as práticas do gerenciamento de riscos atual da organização, as ameaças, os requisitos legais e regulamentares, as práticas de compartilhamento de informações, os objetivos de negócio, os requisitos de segurança e as restrições organizacionais. Ainda conforme o Guia, é responsabilidade da organização determinar o Nível desejado, garantindo que este atenda às metas, que sua implementação seja viável e que promova a redução dos riscos.

É importante ressaltar que essa divisão em níveis não representa os níveis de maturidade dos processos. O objetivo daquela é apoiar as tomadas de decisão organizacionais sobre como priorizar e gerenciar os riscos. A progressão de nível é recomendada quando uma análise de custo-benefício indica uma redução viável e econômica do risco (NIST, 2018).

A *Avaliação da Estrutura*, por sua vez, representa os resultados com base nas necessidades empresariais que a organização selecionou a partir das Categorias e Subcategorias da Estrutura Básica. Podem ser usadas para identificar oportunidades de aprimoramento, por meio da comparação de uma avaliação do "estado atual"com uma avaliação do "estado desejado". É através das avaliações que a organização poderá examinar até que ponto está atingindo suas metas e objetivos relacionadas ao seu processo de gerenciamento de riscos de segurança cibernéticos (NIST, 2018).

2.6.2 CIS *CONTROLS*

O CIS *CONTROLS*[7] CIS (2021) são um conjunto de ações prescritivas, priorizadas e focadas, sendo parte do processo de projetar, implementar, medir, relatar e gerenciar a segurança corporativa, desenvolvido pela *Center for Internet Security* (CIS)[8], uma organização sem fins lucrativos, que tem como objetivo 'tornar o mundo um lugar mais seguro, desenvolvendo, validando e promovendo soluções oportunas de melhores práticas que ajudam pessoas, empresas e governos a se protegerem contra ameaças cibernéticas'.

O CIS *CONTROLS* é embarcado por um ecossistema, ofertado pela CIS, onde existe uma comunidade de indivíduos, especialistas, empresas e organizações, possibilitando: a obtenção de treinamentos; informações; explicações; casos de uso da implementação das recomendações; explicações sobre como medir o progresso ou maturidade da implementação

[7] Licença: <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.pt>
[8] <https://www.cisecurity.org/>

e como ela se alinha com o arcabouço regulatório e de conformidade; para uma organização. Alguns serviços complementares que a CIS oferece são:

- Mapeamento dos controles para vários *frameworks* de Gestão de Riscos, tais como o NIST e a ISO;
- Casos de uso em empresas;
- Lista de referências aos Controles CIS em padrões nacionais e internacionais, legislação e regulamentação estadual e nacional;
- Medidas e métricas para os controles;
- Documentação de alinhamento com o *framework* NIST, entre outros.

A documentação apresenta um total de 18 controles de Segurança Cibernética. Os controles são organizados em Grupos de Implementação de Controles CIS (IGs), sendo que um Grupo de Implementação de Controles CIS (IG) representa um subconjunto dos Controles CIS e representa categorias autoavaliadas para as organizações (CIS, 2021). Cada Grupo de Implementação contempla todos os itens dos grupos anteriores, de forma que o mais elementar é o IG1 e o último nível é o IG3.

De acordo com o CIS *CONTROLS*, os IGs são caracterizados da seguinte forma:

1. **IG1:** é uma empresa de pequeno ou médio porte, com experiência limitada em Tecnologia da Informação (TI) e segurança cibernética dedicada à proteção de ativos e pessoal de TI. A sensibilidade dos dados tratados é baixa e a principal preocupação dessa empresa é manter o negócio operacional.

   As Medidas de Segurança devem ser implementáveis com experiência limitada em segurança e destinadas a impedir ataques gerais não direcionados.

2. **IG2:** a empresa emprega responsáveis por gerenciar e proteger a infraestrutura de TI. Oferecem suporte a departamentos com diferentes perfis de risco e podem ter encargos de conformidade regulatória. A empresa IG2 processa informações confidenciais de clientes. A preocupação da empresa está mais relacionada ao risco reputacional caso um incidente venha a ocorrer.

   As Medidas de Segurança auxiliam a equipe de segurança e as proteções podem depender de tecnologia de nível empresarial e conhecimento especializado para operação.

3. **IG3:** a empresa emprega especialistas em segurança, os ativos e dados contêm informações confidenciais que estão sujeitas à supervisão regulatória e de conformidade.

A empresa deve se preocupar com a disponibilidade, confidencialidade e integridade de dados sensíveis.

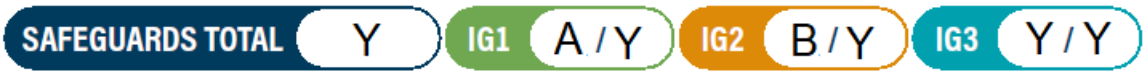
As Medidas de Segurança selecionadas devem diminuir os ataques direcionados e reduzir o impacto de ataques *zero-day*[9].

Cada controle é apresentado com as seguintes informações:

- **Visão geral:** Uma breve descrição da intenção do Controle e sua utilidade como ação defensiva.
- **Por que este controle é crítico?** Uma descrição da importância deste Controle no bloqueio, mitigação ou identificação de ataques, e uma explicação de como os invasores exploram ativamente a ausência deste Controle.
- **Procedimentos e ferramentas:** Uma descrição mais técnica dos processos e tecnologias que permitem a implementação e automação deste Controle.
- **Medidas de Segurança:** Uma tabela das ações específicas que as empresas devem realizar para implementar o Controle. (CIS, 2021, p. 6)

Outras informações presentes em cada controle são apresentadas na Figura 2.

Figura 2 – *Informações complementares do controle*



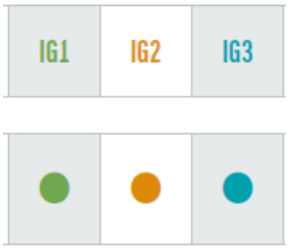
Fonte: Criado pelo autor

Na figura, a letra 'Y' representa o número de Medidas de Segurança ou salvaguardas (*safeguards*) totais daquele respectivo controle. A letra 'A' representa quantas salvaguardas são necessárias para a empresa se autoavaliar dentro da classificação do IG1. De maneira semelhante, a letra 'B' representa a quantidade de salvaguardas para alçancar a classificação IG2.

Cada salvaguarda possui: um número identificador, de acordo com o controle ao qual pertence; um título e uma descrição; uma referência ao tipo de ativo ao qual é atribuída e aplicada; e uma função de segurança relacionada ao *framework* NIST (Identificar, Detectar, Proteger, Responder e Recuperar). Além disso, é sinalizado em cada salvaguarda se ela é necessária ou não para um determinado IG. Conforme exemplificado na Figura 3, na linha de cima estão os três IGs e na linha debaixo, as marcações correspondentes para cada um deles.

[9] Um ataque de dia zero (*zero-day*) é quando um atacante explora uma vulnerabilidade antes que o desenvolvedor tenha a chance de identificar ou corrigir a falha. <https://www.kaspersky.com.br/resource-center/definitions/zero-day-exploit>

Figura 3 – *Classificação de uma salvaguarda quanto aos IGs*



Fonte: CIS *CONTROLS*

Com relação ao *frameworks* NIST, a organização alvo do estudo de caso possui sua própria própria metodologia de gerenciamento de riscos, e não emprega uma metodologia de gerenciamento específica para riscos de cibersegurança. Contudo, a metodologia empregada na organização muito se asemelha aos aspectos do NIST, no que tange as funções da estrutura básica. O processo de gerenciamento de riscos empregado na cooperativa tem foco em ações de identificação, detecção e resposta aos riscos, de forma que as atividades relacionadas a resposta ao risco envolvem ações de prevenção, mitigação e recuperação de incidentes. Ademais, esse *framework* foi pesquisado e apresentado no presente trabalho como uma sugestão de boas práticas em gerenciamento de risco que podem ser implementadas por organizações interessadas. Não é objetivo deste trabalho descrever e se aprofundar no processo de gerenciamento de risco de uma organização, apesar disso, reafirma-se a importancia desse processo como uma das principais fontes de requisitos para a implantação de uma política de *backup* e restauração.

No que se refere ao *CIS CONTROLS V.8*, as características da organização alvo do estudo se enquadram, quase que em sua totalidade, nas características de uma empresa IG3, faltando apenas atender os requisitos de segurança relacionados a ataques direcionados e mitigação do impacto de ataques *zero-day*. Isso ocorre, principalmente, pela falta de tecnologias especializadas, como sistemas automatizados de gerenciamento de vulnerabilidades. Alem disso, a organização ainda não possui condições de cumprir com todos os requisitos presentes nos controles do *framework* necessários para atender a classificação IG3. Contudo, o uso do *framework* se torna ainda mais valioso por nortear os próximos objetivos de segurança a serem cumpridos pela organização.

2.7 Trabalhos Relacionados

Esta seção aborda alguns trabalhos relacionados com a política de *backup* e restauração, como implantação e avaliação de planos de *backup*, política de segurança da informação, gestão de riscos e plano de continuidade do negócio.

O estudo de PEREIRA (2018) tem como foco principal a gestão de *backup* em uma empresa de serviços *full outsourcing*. O objetivo geral é analisar os conceitos, processos de instalação e implementação do *backup*, destacando a sua importância na garantia da disponibilidade dos dados e informações. O autor enfatiza que a proteção desses dados tem se tornado uma preocupação crescente, pois a informação é um ativo crucial para as empresas e investiga em seu trabalho se a solução de *backup* utilizada pela empresa atende às necessidades dessa e garante a disponibilidade dos dados. Foram levantadas quatro hipóteses relacionadas à interface, instalação, criação de tarefas de *backup* e envio de mensagens de *status*, quais sejam: a) a ferramenta possui uma interface de instalação amigável; b) o agente de *backup* requer instalação manual em cada dispositivo; c) conhecimento avançado é necessário para criar tarefas de *backup* e d) a ferramenta não oferece um método de envio de mensagens sobre o *status* das tarefas. Como conclusão, o estudo confirma a interface amigável, a instalação automatizada dos agentes de *backup*, a facilidade na criação de tarefas e os alertas por *e-mail* sobre o *status* das tarefas. O trabalho contribui para ampliar o conhecimento sobre a importância das cópias de segurança nas organizações.

O trabalho de PEREIRA (2018) reafirma que os dados são ativos de grande valor para as organizações e que os procedimentos de *backup* suportam a garantia de disponibilidade das informações. O presente trabalho se diferencia da pesquisa de PEREIRA (2018), uma vez que esta se preocupa com a operacionalização do procedimento de *backup* dentro da empresa estudada, aprofundando na ferramenta de *backup* utilizada pela empresa, ao passo que o presente trabalho foca em controles de alto nível, diretrizes que nortearão os procedimentos operacionais de baixo nível. A política de *backup* não irá descrever o processo de instalação ou configuração das ferramentas utilizadas na operação dos processos de cópia de segurança, mas definirá variáveis como a frequência de execução dos *backups* e nível de proteção dos arquivos.

Outra pesquisa relevante é a de Moraes (2007), que aborda o *backup* de dados sobre a perspectiva da gestão da Segurança da Informação e fornece uma visão abrangente e estratégica da gestão do *backup* de dados. A autora ressalta a importância dos dados armazenados nos computadores como ativos valiosos para as organizações modernas e destaca a necessidade de uma fonte segura de *backup* para garantir a recuperação dos dados em caso de perda. Além disso, o trabalho destaca a importância da participação da área administrativa, além da área de Tecnologia da Informação, no planejamento do *backup* de dados, considerando a relevância dos investimentos em segurança e *backup*.

Esse trabalho se aproxima da pesquisa de Moraes (2007), pois ela afirma que é possível definir estratégias genéricas, com requisitos básicos aplicáveis a diferentes organizações. A principal diferença entre os trabalhos é que a autora não optou por trazer um estudo de caso, aplicando as etapas de planejamento que ela propôs. Na metodologia

da sua pesquisa, Moraes (2007) entrevistou especialistas em segurança da informação, de algumas empresas, a fim de entender se as práticas vistas na revisão da literatura eram empregadas nas empresas e como essas práticas eram vistas por esses profissionais.

O estudo de Santos (2018) foca na governança e gestão dos *backups* de alta retenção, especialmente para instituições da Administração Pública Federal (APF) brasileira. A pesquisa identifica processos e práticas que contribuem para a construção de uma arquitetura eficiente de *backup* de longa retenção, oferecendo um modelo e uma matriz que auxiliam na tomada de decisões e implementação dessa estratégia. Segundo o autor, as organizações pesquisadas demonstraram um forte compromisso com a segurança e recuperação de sistemas e informações por meio do *backup*, o que é essencial para atender aos requisitos legais de retenção de dados. A pesquisa contribui para preencher uma lacuna de conhecimento nessa área e oferece subsídios importantes para a implementação de *backups* de longa retenção, considerando as necessidades específicas da APF brasileira e o aumento significativo de dados gerados pelas organizações.

O trabalho de Santos (2018) elucida uma questão importante, abordada também neste trabalho: a preocupação com a retenção e tempo de guarda dos dados gerados nas organizações e como isso impacta na implementação de procedimentos de *backup*. Para além da definição de diretrizes sobre o tempo de guarda das informações, uma organização deve se atentar a estrutura necessária para armazenar os arquivos de *backup* e em estratégias para manter procedimentos de *backup* sustentáveis.

Outro estudo relevante é o de Marques (2016), que aborda a implantação de políticas de segurança da informação em empresas de plano de saúde. A pesquisa destaca a importância dessas políticas para reduzir riscos e proteger os ativos e informações da organização. A partir da elaboração e adoção de políticas de inventário de ativos, classificação da informação e monitoramento da infraestrutura de TI, a empresa estudada obteve melhor controle do uso dos ativos, identificação e tratamento de eventos relacionados à segurança da informação, geração de indicadores para combater vulnerabilidades específicas e criação de uma cultura de segurança. O envolvimento da alta direção, a formação de uma equipe técnica de segurança da informação e a preservação da imagem da empresa foram pontos positivos identificados. O projeto foi avaliado como satisfatório, proporcionando maior segurança ao patrimônio da empresa.

O presente trabalho muito se aproxima da pesquisa de Marques (2016), no que se refere a implantação de políticas de segurança da informação em organizações, sobretudo, na importância dessas políticas para o controle de riscos e proteção dos ativos. Como verificado ao longo do capitulo 2, a política de *backup* é uma das políticas que constituem a implantação da SI e do SGSI dentro de uma organização. Essa pesquisa se diferencia do trabalho de Marques (2016), por estar voltada especificamente à construção e implantação da política de *backup* e restauração de dados.

Ainda na área da saúde, o estudo de Silva (2021) teve como objetivo a elaboração de um Plano de Continuidade de Negócios (PCN) para os serviços críticos de TI em um hospital público. O estudo envolveu pesquisa de campo e análise de impacto. Foram identificados os principais riscos e impactos relacionados a falhas nos sistemas de TI, destacando-se a indisponibilidade frequente das impressoras, que afeta o fluxo de trabalho nos setores estudados. O PCN proposto tem como objetivo mitigar os impactos de interrupções nos serviços de TI e garantir a continuidade das operações hospitalares. O plano identifica os riscos, define ações de tratamento e estabelece planos de resposta a incidentes e de recuperação de desastres, preparando a organização para situações atípicas. Os resultados da pesquisa destacam a importância de um plano de continuidade de negócios para lidar com incidentes e assegurar a operacionalidade dos serviços de TI no ambiente hospitalar, fornecendo um roteiro e artefatos para a gestão da continuidade dos negócios, considerando os riscos específicos desse contexto e as necessidades da equipe de TI.

O estudo de Silva (2021) demonstra como a indisponibilidade de recursos afeta o fluxo de trabalho de uma organização, é um risco importante a ser monitorado e mitigado e demonstra a importância de planos de recuperação de desastres. Análogo ao estudo de Silva (2021), o presente trabalho apresenta uma política de *backup* e restauração de dados, com o objetivo de mitigar a indisponibilidade de dados e definir diretrizes para processo de restauração desses dados como forma de mitigar o impacto de incidentes com esses ativos.

O trabalho de PEREIRA (2018) reforça o papel do *backup* para as organizações para a garantia das disponibilidades dos dados, um dos pilares fundamentais da segurança da informação. Reforça, nesse sentido, a importância do investimento na proteção das informações, observando que parte desse investimento são os planos e ações de *backup* e restauração dos dados. Nesse contexto, os trabalhos de Moraes (2007), Santos (2018) e Marques (2016) aproximam os planos de *backup* dos processos de governança em TI, gestão de riscos e segurança da informação, ilustrando que é possível pensar em estratégias e arquiteturas de *backup* que possam ser aplicadas em difrentes negócios. Moraes (2007) aborda os principais requisitos para implantação de um plano de *backup*, enquanto Santos (2018) e Marques (2016) trazem dois casos distintos sobre a implementação de procedimentos de *backup* e política de segurança da informação, respectivamente.

Por fim, a pesquisa de Silva (2021) traz a ideia de continuidade do negócio atrelada a gestão de riscos, identificação de processos críticos e garantia de disponibilidade dos serviços, sendo este último um dos principais objetivos de uma política de *backup* e restauração.

Essa pesquisa permeia os aspectos de governança de TI, segurança da informação, gestão de riscos e continuidade do negócio, foco no processo de criação e implantação de uma política de *backup* e recuperação de dados, e ilustra como a política apoia o cumprimento de legislações e normativas, trazendo um estudo de caso em uma organização

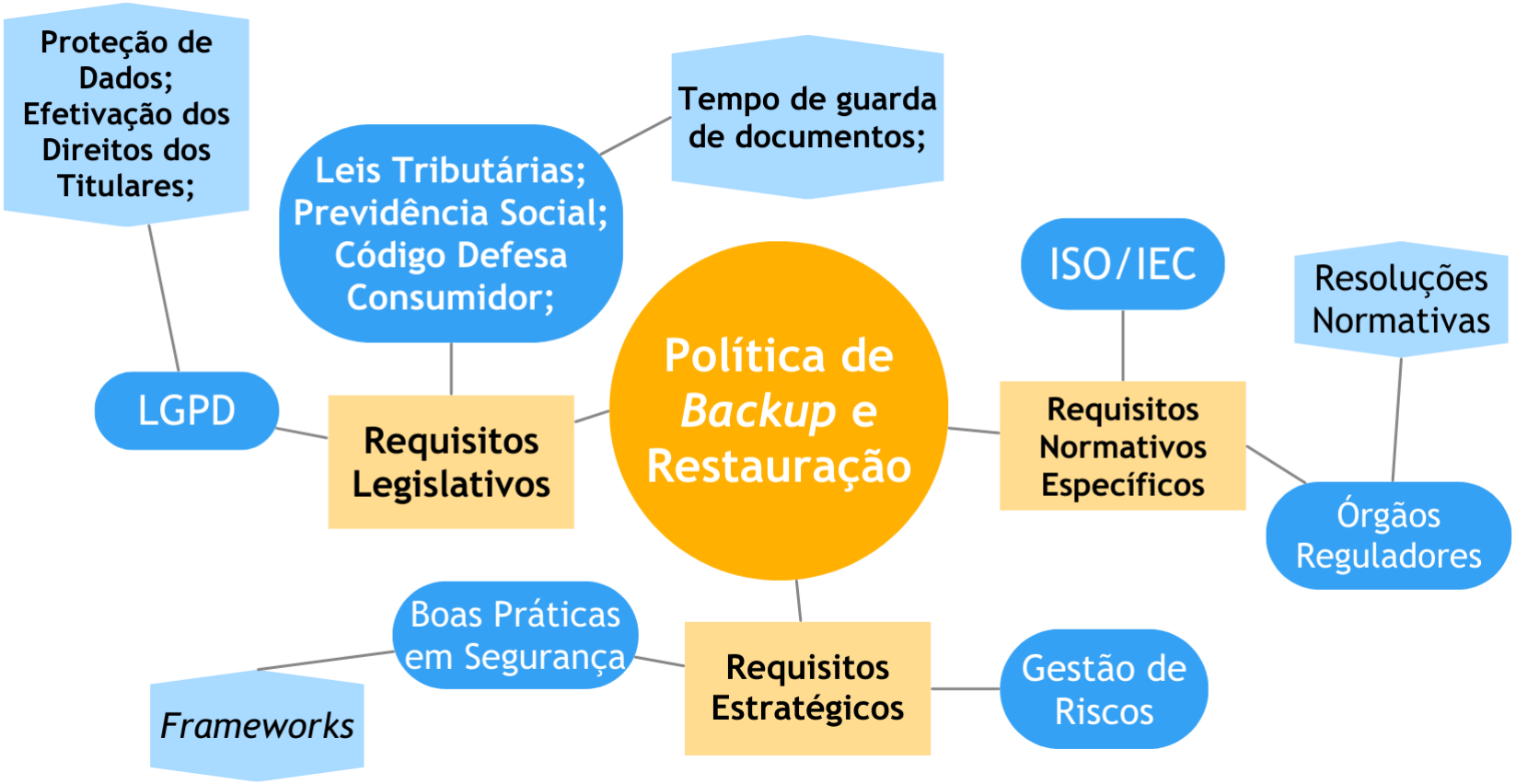
da área da saúde suplementar.

2.8 Considerações Finais

A aplicação das contribuições dos itens explicitados ao longo da fundamentação teórica serão demonstradas mais detalhadamente no Capítulo 3. Com efeito, a Figura 4 apresenta um mapa mental do conteúdo visitado na revisão da literatura, as contribuições que eles trazem para e como se relacionam com a política de *backup* e restauração.

A implantação de uma política de *backup* e restauração deve possuir objetivos claros, que se relacionam com as necessidades da organização. Os objetivos se traduzem em requisitos que esse documento visa atender, sendo as principais fontes desses requisitos as legislações, normativas e os objetivos estratégicos da organização. Na Figura 4, é apresentado as contribuições dos itens da revisão bibliográfica e como eles se relacionam com os objetivos da política.

Figura 4 – Mapa mental da fundamentação teórica



Fonte: Elaborado pelo autor

3 Desenvolvimento

Este capítulo descreve o desenvolvimento do trabalho. Cada subseção a seguir corresponde a um passo da metodologia proposta na Seção 1.3, explicitando a importância de cada passo a ser executado na escrita da política de *backup* e restauração, sua relação as referências de padrões e *frameworks* reconhecidos no ambiente corporativo, e sua aplicação no estudo de caso. A Seção 3.2 apresenta o estudo de caso aplicado a partir da metodologia proposta.

3.1 Desenvolvimento da metodologia

3.1.1 Levantamento das necessidades da organização

O primeiro passo para a construção de uma política corporativa, é determinar qual(is) objetivo(s) aquele controle busca atingir. Deve-se entender as necessidades da organização e das partes interessadas acerca dos requisitos que buscam atender e das metas que buscam alcançar. O levantamento dessas necessidades cumpre com o primeiro objetivo específico do presente trabalho.

Conforme disposto no Capítulo 2, requisitos podem vir de diversas fontes. Toda organização deve cumprir requisitos legais, considerando legislações de âmbito federal, estadual ou municipal, e até normativas específicas relacionadas a área de negócio em que atua. O Capítulo 18 da ISO 27001 também prevê a conformidade com requisitos legais e contratuais, direitos de propriedade intelectual, proteção de registros e proteção de dados pessoais.

No caso da cooperativa estudo de caso, todo arcabouço legal de cunho obrigatório, citado no Capítulo 2, foi levado em consideração pela organização, que possui outros processos, controles e regramentos, a fim de cumprir essas obrigações legais. Sendo assim, nesse capítulo, o foco estará especificamente nos requisitos a serem atendidos pela política de *backup* e restauração e, a exemplo de requisito normativo, será abordada a Resolução Normativa nº 507 da ANS Brasil (2022a).

Entre os requisitos que a cooperativa deve cumprir, em relação à normativa nº 507 e a política de *backup*, estão:

- **Requisito 1.4.3:** 'O plano diretor de tecnologia da Informação contempla plano de contingência de serviços de TI para garantir a disponibilidade dos serviços em situações emergenciais.' (BRASIL, 2022a, Anexo I)

- **Requisito 1.5.3:** 'Os registros contendo a documentação cadastral da rede prestadora de serviço e as informações cadastrais e clínicas dos beneficiários são armazenados de forma a garantir a sua disponibilidade, integridade e confidencialidade.' (BRASIL, 2022a, Anexo I)
- **Requisito 1.6.7:** 'A Operadora possui um Plano de Continuidade de Negócios visando a manutenção das atividades em caso de catástrofes ou outras situações que possam afetar o funcionamento da Operadora.' (BRASIL, 2022a, Anexo I)

Os requisitos acima evidenciam a necessidade de uma política de guarda de informações, guarda das cópias de segurança dessas informações e plano de contingência dos serviços críticos, que servirão de apoio para o plano de continuidade do negócio. Para a operacionalização efetiva desses requisitos, a cooperativa implementou um mapeamento de dados, com o objetivo de identificar como o tratamento de dados funciona dentro da cadeia de valor da organização, classificar esses dados quanto a sua sensibilidade, quem são os responsáveis por esses dados, em quais atividades esses dados estão envolvidos e o local onde ocorre o tratamento das informações. Também foi implementado procedimentos de *backup* das informações dos processos críticos e da infraestrutura tecnológica necessária para a execução desses processos, como cópia de segurança dos banco de dados dos sistema informatizados, cópia de segurança de caixas de *e-mail* estratégicas, cópias de segurança da configuração e dos ambientes virtuais alocados nos servidores.

Observa-se que, anterior à existência da política de *backup* e restauração, devem existir outros procedimentos, práticas, condutas e documentos que irão suportar a existência da política, bem como o cumprimento de demais legislações, como é o caso do mapeamento de dados que serve de apoio ao cumprimento com a LGPD (BRASIL, 2018a). Tanto o mapeamento dos dados, quanto outros controles, documentos e levantamentos, que sustentarão a política de *backup* (e outros planos e políticas de interesse da organização) serão tratados nesse trabalho como "variáveis de negócio"e serão abordados na Seção 3.1.2.

Os requisitos de uma política também podem vir dos objetivos estratégicos da organização, como a obtenção de alguma certificação de qualidade de serviço, implantação de um projeto ou melhoria nos indicadores da organização. Conforme visto no Capítulo 2, toda política corporativa deve estar alinhada aos objetivos e planejamento estratégico da organização. A ISO 27001 dispõe que um sistema de gestão da segurança da informação 'seja parte de, e esteja integrado com, os processos da organização'. Espera-se que a implementação de SGSI esteja alinhada com as necessidades da organização. A norma aborda as necessidades das partes interessadas na Seção 4.2, na qual prevê que

> A organização deve determinar: a) as partes interessadas que são relevantes para o sistema de gestão da segurança da informação; e b) os requisitos dessas partes interessadas relevantes para a segurança da informação. NOTA Os requisitos das partes interessadas podem incluir

> requisitos legais e regulamentares, bem como obrigações contratuais. (ABNT, 2013a)

De acordo com a Seção 5.2 da ISO 27001, a alta direção deve estabelecer uma política que: seja apropriada ao propósito da organização; inclua os objetivos de segurança da informação ou forneça estrutura para tal; inclua o comprometimento em satisfazer os requisitos; inclua o comprometimento com a melhoria contínua. De maneira análoga, esses mesmos requisitos são aplicados à política de *backup* e restauração.

Outra fonte importante de requisitos a serem implementados é a Gestão de Riscos. Conforme disposto na RN nº 518 Brasil (2022d), a gestão de riscos tem o objetivo de identificar, analisar, avaliar, priorizar, tratar e monitorar riscos que possam afetar os objetivos da operadora de plano de saúde, em nível estratégico, tático e operacional. Por esse motivo, uma getão de risco bem executada trará diversos requisitos de segurança a serem implementados na organização.

Em relação a política de *backup*, o principal risco a ser monitorado é o risco da perda de dados, sendo que existe uma seção específica na ISO 27002 (ABNT, 2013b) acerca desse risco. A ISO 27002, em sua Seção 12.3, prevê que os *backups* das informações, dos *softwares* e sistemas sejam efetuados e testados regularmente e as diretrizes para implementação desse controle são assim definidas:

> Convém que a política de *backup* seja estabelecida para definir os requisitos da organização relativos às cópias de segurança das informações, dos *software* e dos sistemas.
>
> Convém que a política de *backup* defina os requisitos para proteção e retenção.
>
> Convém que os recursos adequados para a geração de cópias de segurança sejam disponibilizados para garantir que toda informação e os *software* essenciais possam ser recuperados após um desastre ou a falha de uma mídia. (ABNT, 2013b, Seção 12.3)

Os requisitos sugeridos para o cumprimento das diretrizes acima são:

> **a)** registros completos e exatos das cópias de segurança e documentação apropriada sobre os procedimentos de restauração da informação, os quais convém que sejam produzidos;
>
> **b)** convém que a abrangência (por exemplo, completa ou diferencial) e a frequência da geração das cópias de segurança reflitam os requisitos de negócio da organização, além dos requisitos de segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da organização;
>
> **c)** convém que as cópias de segurança sejam armazenadas em uma localidade remota, a uma distância suficiente para escapar dos danos de um desastre ocorrido no local principal;
>
> **d)** convém que seja dado um nível apropriado de proteção física e ambiental das informações das cópias de segurança (ver Seção 11), consistentes com as normas aplicadas na instalação principal;

> **e)** convém que as mídias de *backup* sejam regularmente testadas para garantir que elas sejam confiáveis no caso do uso emergencial; convém que isto seja combinado com um teste de restauração e checado contra o tempo de restauração requerido. Convém que os testes da capacidade para restaurar os dados copiados sejam realizados em uma mídia de teste dedicada, não sobrepondo a mídia original, no caso em que o processo de restauração ou *backup* falhe e cause irreparável dano ou perda dos dados;
>
> **f)** em situações onde a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação. (ABNT, 2013b, Seção 12.3)

Além de requisitos relacionados ao plano de *backup*, também há recomendações acerca do processo de recuperação de informações, em caso de desastre. A norma sugere que sejam estabelecidos o 'período de retenção para informações essenciais ao negócio'. Nesse sentido, entende-se que o período de retenção de informações também seja uma variável de negócio, uma vez que cada organização é detentora de informações que exigem diversos tempos de retenção a depender de sua natureza.

Ao encontro dos requisitos da ISO 27002 citados acima, o CIS *CONTROLS V.8* propõe em seu Controle 11 que a organização estabeleça procedimentos de recuperação de dados capazes de restaurar ativos para um estado confiável. De acordo com o *framework*, os procedimentos de recuperação de dados devem incluir 'procedimentos de *backup* com base no valor dos dados, sensibilidade ou requisitos de retenção'. Dessa forma, será possível estabelecer a frequência e o tipo de *backup* a ser empregado. Os requisitos para sucesso da recuperação dos dados sugeridos pelo CIS *CONTROLS V.8* e aplicados no estudo de caso são:

> Uma vez por trimestre (ou sempre que um novo processo ou tecnologia de *backup* for introduzido), uma equipe de teste deve avaliar uma amostra aleatória de *backups* e tentar restaurá-los em um ambiente de teste. Os *backups* restaurados devem ser verificados para garantir que o sistema operacional, a aplicação e dados do *backup* estejam intactos e funcionais. No caso de infecção por *malware*[1], os procedimentos de restauração devem usar uma versão do *backup* que se acredita ser anterior à infecção original. (CIS, 2021, p. 38)

Até aqui, foram discutidas as necessidades da organização e compreendida a relevância de se determinar e entender os objetivos a serem alcançados e os requisitos, legais, normativos e estratégicos, a serem cumpridos pela política de *backup* e restauração. Demonstra-se como as necessidades específicas da organização determinam os requisitos a serem atendidos e, por sua vez, influenciam no desenvolvimento da política. Por meio desta, são sanadas as questões de pesquisa 1 e 3 e parte da questão 6, no que se refere a eficácia da política em relação as expectativas da organização. De forma abrangente, a

[1] *Malware:* termo genérico para qualquer tipo de *software* malicioso projetado para prejudicar ou explorar qualquer dispositivo, serviço ou rede programável. <https://www.mcafee.com/pt-br/antivirus/malware.html>

seção 3.2.2 apresenta a expectativa que a organização busca atingir com a implementação da política.

O próximo passo é levantar informações, definições de regras de negócio e outras diretrizes que vão apoiar e também nortear as regras e o escopo da política de *backup* e restauração. Essas informações, definições e diretrizes são, nesse trabalho, denominadas de variáveis de negócio.

3.1.2 Definição das variáveis de negócio

Após elencar os requisitos e os controles que serão definidos na política de *backup* e antes de escrevê-la, há questões que devem ser respondidas, definições a serem tomadas e levantamento de informações importantes, tais como as variáveis de negócio, que são informações necessárias à construção da política e que apoiarão e nortearão os procedimentos operaionais implementados para cumprir com suas diretrizes. O objetivo desse passo da metodologia é entender e determinar essas variáveis.

Durante a idealização da política de *backup* do estudo de caso, foram discutidas e definidas as questões abaixo, com base em informações sugeridas nas normas ISO, nos *frameworks* estudados e na operacionalização dos requisitos identificados no levantamento das necessidades da organização:

1. Quais são os recursos que suportam os processos críticos para a organização, que necessitam de cópia de segurança?
2. Quais são os serviços que não podem sofrer interrupções ou se ficarem indisponíveis, causarão grandes impactos?
    a) Caso ocorra indisponibilidade, qual a tolerância de tempo da indisponibilidade (RTO)?
    b) Se esse serviço depende de um fornecedor, qual a garantia esse fornecedor entrega?
    c) Caso seja necessária uma recuperação, qual o ponto de retorno (RPO)?
    d) Quanto tempo levaria para realizar uma restauração, em caso de desastre?
3. Quais são os serviços que podem sofrer indisponibilidades sem maiores impactos?
    a) Por quanto tempo esses serviços podem ficar indisponíveis?
    b) Quanto tempo levaria para realizar a restauração desses serviços, caso ocorra indisponibilidade?
    c) Se esse serviço depende de um fornecedor, qual o tempo solicitado pelo fornecedor, em caso de indisponibilidade?

4. Como decidir quais serviços ou informações entrarão no escopo dos procedimentos de *backup*?
    a) Quais critérios serão adotados para elencar esses serviços?
    b) Quem poderá solicitar inclusão ou exclusão de algum serviço ou informação nos procedimentos de *backup*?
    c) Quem será o responsável por autorizar e controlar essa relação de serviços?
    d) Com que frequência deverá ocorrer a cópia de segurança desses serviços ou informações?
    e) Por quanto tempo essas cópias de segurança devem existir?
5. Como será organizada a forma de armazenamento das cópias de segurança, e como serão classificados, catalogados e identificados os arquivos de *backup*?
6. Os arquivos de *backup* serão copiados para outro local, distinto e distante do local onde as informações originais se encontram?
7. Com que frequência serão enviados para este local?
8. Como será o processo de teste de integridade e recuperação das cópias de segurança?
    a) Quem será o responsável por testar a integridade das cópias de segurança?
    b) Com que frequência serão realizados esses testes?
    c) Em caso de um desastre e interrupção completa das atividades, qual a ordem de recuperação dos serviços?
9. Em caso de falha no processo do *backup* ou do teste de recuperação, o que fazer?
    a) Como será relatada ou registrada a falha?
    b) Quem será acionado para investigar as possíveis causas da falha?
10. Quem poderá acessar, mover e excluir os arquivos de cópia de segurança?
    a) Como se dará o processo de descarte das mídias de cópia de segurança?
    b) Como será relatado ou registrado o descarte das cópias de segurança?
11. A organização possui infraestrutura suficiente para manter os procedimentos de *backup* dos serviços?

Buscou-se responder essas questões antes da produção política de *backup* e restauração, uma vez que essas definições compõem as diretrizes que a organização irá seguir, no que tange aos procedimentos de *backup* e restauração.

Algumas definições acima não farão parte do escopo integral do estudo de caso, mas serão material de suporte e referência para o conteúdo da política, como é o caso do documento chamado "Matriz de Temporalidade", que objetiva documentar e controlar os diversos tempos de guarda de documentos, arquivos e informações. Além da "Matriz de Temporalidade", também há na organização do estudo de caso um documento chamado "Mapeamento de Dados", através do qual são documentadas e controladas as operações de tratamento de dados pessoais, sobretudo dados sensíveis, dentro da organização. Esse mapeamento apóia os processos de Gestão de Dados, citado no Controle 03 do CIS *CONTROLS V.8* CIS (2021).

3.1.3 Definição das responsabilidades

Assim como as demais políticas instituicionais, existem responsabilidades acerca da manutenção da política, sendo objetivo desse passo da metodologia, definir todas as responsabilidades relacionadas ao processo de implantação da política de *backup* e restauração.

A ISO 27001, na Seção 5, aborda de maneira geral o papel da liderança e o comprometimento que a alta direção da organização possui, no que se refere à implantação da política de segurança da informação. De acordo com a norma, a alta direção deve, dentre outras ações, assegurar os recursos necessários para o SGSI e promover a melhoria contínua.

Contudo, as responsabilidades acerca da política de *backup* não se limitam à alta direção. Conforme visto da Seção 3.1.2, há definições a serem tomadas sobre quem são os responsáveis por incluir ou excluir serviços no escopo dos procedimentos de *backup*. Além disso, a própria política deve possuir um responsável, que seja considerado o dono desse documento dentro da organização, que deverá manter a política atualizada, em conformidade e em funcionamento. A ISO 27001, em sua Seção 7.2, prevê que a organização deve:

> **a)** determinar a competência necessária das pessoas que realizam trabalho sob o seu controle e que afeta o desempenho da segurança da informação;
>
> **b)** assegurar que essas pessoas são competentes, com base na educação, treinamento ou experiência apropriados;
>
> **c)** onde aplicável, tomar ações para adquirir a competência necessária e avaliar a eficácia das ações tomadas; e
>
> **d)** reter informação documentada apropriada como evidência da competência.
>
> NOTA Ações apropriadas podem incluir, por exemplo: fornecimento de treinamento para os facilitadores, os funcionários atuais ou pessoas competentes, próprias ou contratadas. (ABNT, 2013a, Seção 7.2)

Também é papel da organização, de acordo com a ISO 27001, conscientizar e comunicar as partes interessadas da existência da política, sendo essa atividade também delegada a uma pessoa ou equipe responsável.

No tocante à melhoria contínua, a Seção 9 da ISO 27001, trata da avaliação do desempenho da segurança da informação, dentro da organização. Convém que a instituição avalie e monitore os processos de segurança da informação, e também realize auditorias internas. É importante, ainda, que os responsáveis por monitorar, avaliar e realizar as auditorias internas não sejam os mesmos responsáveis por implantar e conceber os controles criados, e demais procedimentos operacionais que suportam as diretrizes da política. Isso é chamado de segregação de função e é abordado na ISO 27002, Seção 6.1.2. A segregação tem o objetivo de reduzir as oportunidades de modificação não autorizada ou não intencional, ou uso indevido de ativos. No caso da auditoria, a pessoa ou equipe que implantou os procedimentos não pode ser a pessoa ou equipe que irá auditar esses procedimentos, pois há a presença do conflito de interesses, prejudicando a qualidade e a integridade do processo de auditoria.

3.1.4 Definição do escopo da Política

O objetivo desse passo é determinar o conteúdo da política de *backup* e restauração, a qual deve conter, no mínimo, os assuntos abordados nas Seção 3.1.1, Seção 3.1.2 e Seção 3.1.3. Devem constar na política: os seus objetivos e o comprometimento da alta direção e/ou da organização acerca dos objetivos (apresentado na seção 3.2.2); a abrangência da política e quais são os públicos alvo e a quem ela de aplica (apresentado na seção 3.2.2); as diretrizes norteadoras dos controles que serão implantados; os responsáveis pelas diretrizes ou responsáveis pela execução dos procedimentos que irão operacionalizar a política dentro da organização; o responsável pela manutenção e atualização da política; a frequência com que a política deve passar por processo de revisão e atualização (presentes na seção 3.2.5; e outras informações que a organização considere pertinentes, como por exemplo, a relação da política com fornecedores e terceiros ou com outras políticas internas da organização, siglas, termos e definições importantes para que todos os públicos alvo possam ler e compreender o texto da política (seção 3.2.3).

Por outro lado, não devem constar informações de nível operacional na política, ou seja, não é cabível o detalhamento dos procedimentos operacionais de *backup*, como um descritivo de como realizar uma cópia de segurança do banco de dados a partir do *software SQL Server* ou em qual diretório armazenar as cópias de segurança, etc. Essas são informações de nível operacional e devem constar em outros tipos de documentos. De maneira geral, este e os demais passos da metodologia, abordados nas próximas seções, serão influenciados pela cultura e diretrizes de cada organização.

A partir do disposto nesta seção, na seção 3.1.3 e na seção 3.1.1 pode-se responder

as questões de pesquisa 2, 4 e 5. As definições de variáveis de negócio, responsabilidades e escopo da política, sobretudo das diretrizes de criticidade das informações, frequência dos *backups*, adoção, rastreio e teste de procedimentos de restauração de dados, presentes ao longo do estudo de caso, promovem melhoria na garantia da disponibilidade e da proteção dos dados. Além disso, as definições de ordem de recuperação dos serviços, são de extrema importância para fomentar a capacidade e eficiência de recuperação dos dados em caso de incidentes ou desastres.

3.1.5 Escrita e aprovação da Política

A escrita da política deve obedecer as normas internas de produção de documentos institucionais adotadas pela organização, levando em conta formatação e *layout*. É importante atentar-se à linguagem utilizada no texto: a política deve ser legível e de fácil compreensão por todos os públicos aos quais ela se direciona. Nesse contexto, a seção 3.2.3 desempenha papel importante, contribuindo para a garantia da legibilidade do documento.

Após a escrita do texto, este deve ser apresentado nas diversas alçadas de aprovação, seguindo o fluxo definido dentro do organização. A respeito da organização do estudo de caso, a política é apresentada ao Comitê de Privacidade e Proteção de Dados. Após aprovada pelos membros do Comitê, a política segue para aprovação no Conselho de Administração da organização, presente no estudo de caso, na seção 3.1.5. A política deve ser publicada e estar acessível aos públicos aos quais ela se aplica, conforme prevê a Seção 5.2 da ISO 27001.

3.1.6 Cronograma de implantação da Política

Convém que o processo de implantação da política siga um cronograma, contemplando os levantamentos iniciais a serem realizados; a produção e escrita do texto; aprovação da política; a comunicação e conscientização dos públicos alvo; a eventual capacitação dos envolvidos, de acordo com suas responsabilidades definidias na política.

3.1.7 Manutenção e revisão da Política

Toda política corporativa deve possuir um ciclo definido de revisão e atualização do documento. Isso garante a conformidade do documento com os objetivos, processos e demais diretrizes organizacionais. De acordo com a ISO 27001, Seções 7.5.2 e 7.5.3, a organização deve assegurar a identificação e descrição da política, controlar a distribuição, acesso, armazenagem e preservação e controle de mudanças (controle de versão) do documento (apresentado na seção 3.2.8).

Na organização do estudo de caso, todos os documentos possuem número único de referência, controle de acesso, incluindo permissões de acesso, controle de versão, e as

Atividades	Meses						
	01/23	02/23	03/23	04/23	05/23	06/23	07/23
Levantamento de requisitos da política	X	X	X				
Definição das variáveis de negócio	X	X	X				
Definição das responsabilidades	X	X	X				
Definição do escopo da política	X	X	X	X			
Escrita e revisões do texto		X	X	X	X		
Apresentação da política ao Comitê				X	X		
Aprovação					X		
Comunicação e Treinamentos					X	X	X

Tabela 2 – Cronograma de Implantação da Política

Fonte: Elaborado pelo autor

alterações realizadas conforme cada atualização de versão. As atualizações da política devem ser realizadas sempre que um ciclo de revisão do documento se encerra ou quando se fizer necessário, por exemplo, para a incorporação de um novo controle devido a identificação de um novo risco pelo processo de gestão de riscos.

Destaca-se que o ciclo de revisão e atualização deste documento desempenha um papel fundamental na garantia da contínua adequação da política ao contexto da organização, assim como na sua aderência aos regulamentos específicos da instituição. Isso reitera que a política em questão permanece em conformidade e é plenamente capaz de atender às expectativas da organização, temas das questões de pesquisa 3 e 6.

3.2 Estudo de caso

3.2.1 Contextualização da organização alvo

De acordo com a classificação da ANS, a organização alvo do estudo é uma cooperativa considerada de pequeno porte. Possui uma estrutura organizacional própria, contando com conselhos, diretoria, gerência, setores críticos e setores de suporte. Além disso, possui um setor dedicado à riscos e *compliance*, segurança da informação, tecnologia da informação e um *Data Protection Officer* (DPO), todos estes envolvidos no projeto de implantação da LGPD dentro da cooperativa. A política de *backup* e restauração é um dos itens de controle de um plano de ação da segurança da informação e da gestão de riscos, que faz parte do projeto de implantação da LGPD, o qual contou com a implantação de diversas outras políticas de controle interno da organização.

A cooperativa possui seu próprio processo de gestão de riscos, no qual há o controle de todos os riscos identificados em todas as áreas da organização, organizados por setor e

classificados em níveis de criticidade. O reporte desses riscos é realizado periodicamente às partes interessadas. Apesar de não seguir estritamente um *framework* de Gestão de Risco, como o *Cyberframework* NIST NIST (2018) ou o CIS *CONTROLS V.8* CIS (2021), as práticas adotadas na cooperativa, naquilo que é possível e aplicável, seguem as práticas sugeridas nesses guias.

A organização possui ainda:

- Política de segurança da informação, que determina os controles de segurança, medidas técnicas e administrativas, diretrizes e definição de processo de resposta a incidentes de segurança da informação adotadas pela empresa;
- Política de privacidade e proteção de dados;
- Política de qualidade dos dados, que determina os controles de confidencialidade das informações, os diferentes níveis de proteção, anonimização e criptografia, sobretudo de dados sensíveis tratados dentro da organização;
- Sistema próprio de controle de acesso dos usuários a todos os sistemas informatizados da empresa;
- Mapeamento de Dados, documento que registra informações sobre o tratamento de dados pessoais dentro da organização. Descrito no Anexo A do presente trabalho.
- Matriz de Temporalidade, documento que registra o prazo de guarda dos diversos documentos/arquivos da organização. Descrito no Anexo A do presente trabalho.
- Plano de ação de implantação da *LGPD* na organização, contemplando cronograma do projeto e que engloba a produção e implantação da política de *backup* e restauração;
- Equipe de TI, composta por um líder, três analistas de suporte a sistemas, um analista de infraestrutura, um assistente de suporte a sistemas, um assistente de infraestrutura e um analista de segurança da informação;
- Um Encarregado de Dados, responsável geral pela implantação da LGPD;
- Um analista de riscos, responsável pelo processo de gestão de risco dentro da organização;
- Um *data center* contando com servidores da fabricante DELL, sistemas operacionais *Microsoft Windows Server*, sistema de anti-vírus contratado e espaço de armazenamento com cinquenta *terabytes* de capacidade expansível;
- Os servidores contam com 12 máquinas virtuais em ambientes *VMware vSphere*, com garantia do fornecedor;

- Um *firewall PF Sense*;
- Um sistema de monitoramento de ativos e um sistema de gestão à vista, responsável por exibir os dados de monitoramento em tempo real.
- Um *storage* com mais cinquenta *terabytes* de capacidade expansível, geograficamente distante do *data center*;
- Sistema gerenciador de banco de dados Microsoft SQL Server, Firebird e Oracle.

Todos os recursos acima estão, de alguma forma, envolvidos com o processo de implantação da política de *backup* e restauração de dados, seja promovendo requisitos, apoiando nas definições das variáveis de negócio, executando ações previstas pela política, dando suporte as diretrizes apontadas na política e criando condições para a instauração e manutenção da política dentro da organização.

Espera-se que, com a implantação da política, procedimentos operacionais de *backup* sejam atualizados, procedimentos de teste e restauração de dados sejam criados e devidamente documentados, riscos cibernéticos sejam mitigados e que a organização tenha condições de, efetivamente, cumprir com os tempos de guarda dos dados tratados e com o ciclo de vida das informações dentro da organização.

As subseções a seguir seguem as mesmas seções presentes na política, sendo um espelho do documento.

3.2.2 Objetivo

A presente Política de *Bakcup* e Recuperação de Dados tem como objetivo estabelecer diretrizes para o processo de cópia e armazenamento dos ativos de dados envolvidos, direta ou indiretamente, nas atividades da cooperativa, visando garantir a segurança, integridade, disponibilidade, redundância e recuperação das informações vinculadas aos recursos de Tecnologia da Informação.

Esta Política visa ainda demonstrar o comprometimento da organização em sustentar o plano de continuidade do negócio, adotar processos e regras que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas ao armazenamento de dados. Identificar, analisar e mitigar, de forma continuada, os riscos presentes nos ativos de dados, evitando a ruptura dos preceitos de integridade, confiencialidade e disponibilidade das informações, minimizando perdas em caso de desastre e viabilizar a recuperação de dados através do processo de restauração.

3.2.3 Siglas e Definições

Administrador de *backup* e *restore*: responsável final pelos controles de *backup* e *restore*;

Administrador de Banco de Dados: responsável técnico pelo serviço de instalação, configuração e gerenciamento do ambiente ou *software* de gestão de banco de dados;

Administrador da Virtualização: responsável técnico pelo serviço de instalação, configuração e gerenciamento de ambientes virtuais baseados em virtualização;

***Backup* à quente:** modalidade de *backup* realizado em dados que se encontram em ambiente de produção, com os serviços em funcionamento, dentro da janela de produção;

***Backup* Completo:** modalidade de *backup* na qual todos os dados são copiados integralmente;

***Backup* Diferencial:** modalidade de *backup* na qual somente os arquivos novos ou modificados desde o último *backup* completo são copiados;

***Backup* Incremental:** modalidade de *backup* na qual somente os arquivos novos ou modificados desde o último *backup* são copiados;

***Backup* de primeiro nível:** *backup* armazenado em disco local;

***Backup* de segundo nível:** *backup* armazenado em mídia externa;

***Backup offline*:** modalidade de *backup* na qual os dados são armazenados em uma mídia física, isolada de qualquer conexão de rede;

***Backup off-site*:** modalidade de *backup* que abrange a replicação de dados do *backup* em local geograficamente separado do local das informações originais;

Catálogo de Serviços: listagem com todos os serviços e ativos que necessitam de *backup*;

Equipe de *backup*: equipe técnica responsável pelos procedimentos de configuração, execução, monitoramento e testes de *backup* e restauração;

***Log*:** arquivos que guardam registros das alterações e operações realizadas num determinado serviço, sistema ou banco de dados;

Mídia: meio físico no qual, efetivamente, armazenam-se os dados de um *backup*;

Retenção: período de tempo em que o conteúdo da mídia de *backup* deve ser preservado;

Recuperação de Desastre: estratégia de recuperação de serviços motivada por sinistros de grave amplitude física ou lógica;

Responsável pela Infraestrutura de TI: colaborador responsável pela área de infraestrutura do setor de Tecnologia da Informação;

Responsável pelo Serviço: colaborador responsável pela operação de determinados serviços ou recursos computacionais;

Restauração: procedimento operacional de recuperação de dados;

Serviço de *Backup*: todo ativo que possui informações ou dados e foi incluído no Catálogo de Serviços;

TOPdesk: Central de Serviços Compartilhados;

3.2.4 Abrangência

Este documento é aplicável a todos os diretores, membros de conselho, membros de comitês, cooperados, colaboradores, estagiários e jovens aprendizes, em quaisquer das dependências da cooperativa ou locais onde estes se façam presentes por meio do armazenamento das informações, cujo o *backup* e a redundância sejam essenciais.

3.2.5 Diretrizes

1. Dos domínios de dados

1.1 Os serviços que serão contemplados nesta Política de *backup* e restauração estarão divididos em categorias, de acordo com a Tabela 3, para que cada tipo de dado possa ser tratado com maior especificidade, atendendo da melhor forma, cada tipo de serviço, critérios de segurança, legislações vigentes e regras de retenção.

CATEGORIAS	EXEMPLO DE SERVIÇO	CRITICIDADE	ORDEM DE RECUPERAÇÃO
LDAP (*Lightweight Directory Acces Protocol*)	Serviços que possuem autenticação integrados ao Serviço de Diretórios do Sistema Operacional	Alta	03
Banco de Dados	Arquivos de configuração, base de dados e *log* de banco de dados	Alta	04
Infraestrutura	Arquivos de configuração de servidores e dispositivos de rede	Alta	02
Hospedagem	Arquivos hospedados em *sites*	Baixa	07
Sistemas Críticos	Arquivos de configuração, inicialização e *log* de sistemas críticos	Alta	04
Sistemas Secundários	Arquivos de configuração, inicialização e *log* de sistemas secundários	Baixa	05
Sistema Legado	Arquivos de configuração, inicialização e *log* de sistemas legado	Baixa	10
Sistemas e Plataformas WEB	Arquivos de configuração, inicialização e *log* de sistemas e plataformas *WEB*	Baixa	06
Virtualização	Máquinas e ambientes virtuais	Alta	01
Compartilhamento de Arquivos	Arquivos em rede corporativa	Média	04
E-mail	Arquivos de contas de *e-mail*	Média	08
Arquivos da Matriz de Temporalidade	Documentos e arquivos que não se encaixam nas demais categorias e são registrados na Matriz de Temporalidade	Alta	09

Tabela 3 – Categorias de Dados

1.2 Os serviços catalogados terão atribuições de nível de criticidade, refletindo sua importância para a continuidade do negócio.

1.3 Os serviços catalogados deverão ter indicação sobre sua respectiva ordem de recuperação, em caso de eventual acionamento do plano de recuperação de desastre.

2 Das atribuições e responsabilidades

2.1 O Administrador de *backup* e restauração será o responsável pela Equipe de *backup*, delegando assim as atribuições de manter a política e procedimentos relativos aos serviços de *backup* e recuperação, bem como de guardar as mídias e assegurar o cumprimento das normas aplicáveis.

2.3 São atribuições do Adminstrador de *backup* e restauração:

1. Propor modificações visando a melhoria contínua desta Política;
2. Gerenciar as mídias;
3. Configurar e operar os serviços e ambientes de restauração;
4. Garantir os recursos necessários para alocação dos arquivos de *backup*;
5. Em uma eventual recuperação de dados, avaliar todo o processo através de um relatório;
6. Criar e manter *backup* de segundo nível;
7. Analisar, junto à Equipe de *backup* e o solicitante, os pedidos de inclusão e exclusão de serviços no Catálogo de Serviços;

NOTA. Para todos os efeitos desta Política, o Administrador de *backup* e *restore* é o responsável pela Infraestrutura de TI, e a Equipe de *backup* é constituída pelos responsáveis dos serviços listados no Catálogo de Serviços.

2.4 São atribuições da Equipe de *backup* e restauração:

1. Propor modificações visando a melhoria contínua desta Política;
2. Criar e manter *backup* de primeiro nível;
3. Executar procedimentos de teste de restauração e eventuais restaurações;
4. Configurar a ferramenta de *backup* conforme necessidade;
5. Realizar a verificação, por amostragem aleatória, dos arquivos de *backup* produzidos;

2.5 Todo e qualquer serviço deverá ser ponderado e estudado antes de sua inclusão no Catálogo de Serviços, e por sua vez, no processo de *backup* e restauração. Após incluído, obrigatoriamente deverá seguir os procedimentos de restauração.

2.5.1 O responsável pelo serviço deverá definir quais servidores e respectivos diretórios e arquivos serão incluídos no *backup*, tendo como prioridade:

1. Arquivos de configurações de ambientes e aplicações referentes a serviços deste servidor em questão;
2. Dados e configurações de banco de dados;
3. Arquivos de *log* dos aplicativos, inclusive *log* da ferramenta de *backup* e restauração;
4. Arquivos de usuário final e E-mail.

2.5.2 A Equipe de *backup* deverá definir quais diretórios e arquivos não serão incluídos no *backup*, tendo como referência:

1. Arquivos do sistema operacional ou de aplicações que podem ser obtidos através de uma nova instalação;
2. Arquivos temporários;
3. Arquivos salvos nas unidades locais das estações de trabalho;
4. Arquivos da área de transferência;
5. Arquivos particulares dos usuários.

2.5.3 Para aplicativos e/ou banco de dados de terceiros, devem ser seguidas as recomendações sugeridas pelo desenvolvedor e/ou fabricante, desde que estas não infrinjam nenhuma das diretrizes descritas nesta ou em outra política institucional, que trate de tratamento de dados.

2.6 Os procedimentos de *backup* deverão ser atualizados quando houver:

1. Novas aplicações desenvolvidas ou instaladas;
2. Novos locais de armazenamento de dados;
3. Novos arquivos com relevância para o funcionamento do serviço;
4. Novas instalações de banco de dados.

2.7 Para a especificação de um *backup*, o Responsável pelo Serviço deverá efetuar uma solicitação de *backup*, contendo as informações necessárias, via chamado no TOPdesk.

2.7.1 O *backup* deverá ser programado, seguindo as orientações da solicitação, observando-se o caráter da solicitação (demanda agendada ou emergencial).

2.7.2 Todos os *backups* deverão ser testados antes da entrega. Estes testes devem incluir uma restauração para comprovar a eficácia do *backup*, que deverá ser formalmente aprovada pelo Responsável pelo Serviço.

2.8 A configuração e monitoramento das funcionalidades relativas ao *backup* de banco de dados será de responsabilidade do Administrador de Banco de Dados.

2.9 O monitoramento dos *backup* relativos aos sistemas críticos, sistemas secundários e sistemas legados será de responsabilidade do colaborador responsável pelo respectivo sistema.

2.10 A Coop Saúde deverá disponibilizar os recursos de infraestrutura capazes de atender ao modelo de continuidade da instituição em nível de recuperação de desastres, a fim de que se torne viável a implementação de uma estratégia de *backup off-site* e/ou *backup offline*.

3 Diretrizes de operação

3.1 A criação e operação dos *backup* deverá obedecer às seguintes orientações:

1. Criação de *backup*:

    a) O *backup* deverá ser programado para execução automática, sempre que possível, em horários de menor ou nenhuma utilização dos sistemas e da rede, visando a redução do impacto no desempenho dos sistemas e da rede;

    b) *Backup* urgentes e/ou à quente devem ser solicitados acompanhado de devida justificativa. A execução destes *backup* deverá ser autorizada pelo Administrador de *backup*, e em sua ausência, pelo Responsável pela Segurança da Informação da Coop Saúde;

    c) Caso o solicitante do *backup* não especifique qual o tipo do *backup* a ser executado, deve, ao menos, explicar, detalhadamente, qual a sua necessidade, para que a Equipe de *backup* decida qual a modalidade de *backup* executar.

2. Operação de *backup*:

    a) O *backup* deverá ser monitorado pela Equipe de *backup*;

b) Para todos os *backups* realizados com sucesso, deve ser gerado um registro, se possível de modo automatizado, pela própria ferramenta de *backup*, confirmando a execução da atividade;

c) Aos *backups* que apresentarem falhas, a Equipe de *backup* deverá registrar um relatório de acompanhamento, no qual deverá constar a data, o horário, o objeto e o Responsável pelo Serviço, a causa da falha e a ação corretiva adotada.

3.2 Quaisquer procedimentos programados que impliquem em riscos de funcionamento em serviços ou equipamentos da instituição, somente deverão ser executados após a realização de um *backup* de seus dados ou arquivos de configuração, quando possível.

3.3 O *backup off-site* deverá armazenar os dados em fita ou em *storage* (servidor de armazenamento dedicado).

3.3.1 A armazenagem do *backup off-site* deve estar, geograficamente, em local distinto do que se encontra o *data center* do ambiente de produção.

3.3.2 Os dados transportados ao *backup off-site* deverão estar criptografados.

3.3.3 O armazenamento do *backup off-site* deve seguir os mesmos padrões e diretrizes de segurança que os dados originais, conforme esta Política e a Política de Segurança da Informação.

4 Do procedimento de *backup*

4.1 Os *backups* de dados serão efetuados seguindo os Procedimentos Operacionais Padrão, de acordo com as categorias de dados da Tabela 3.

4.2 Quando um serviço for descontinuado, o Responsável pelo Serviço notificará a Equipe de *backup*, que então providenciára um *backup* final do serviço, envolvendo banco de dados e configurações deste, quando necessário. Este *backup* deverá ser retido pelo tempo determinado na Matriz de Temporalidade, de acordo com o tipo de dado tratado nesse serviço.

5 Da guarda dos dados

5.1 Em caso de *backup offline*, os *backup* do tipo completo, realizados em fita magnética, devem ser guardados mensalmente, no primeiro dia útil de cada mês, em cofre de segurança antichamas, com devido controle de acesso, juntamente com uma identificação física do conjunto de fitas.

NOTA. Deve ser armazenado junto às fitas, um controle de identificação, com o objetivo de viabilizar e otimizar o uso dessas fitas em recuperação de desastres.

5.2 Para definição dos prazo de guarda, em conformidade com a diversidade de serviços e legislações aplicáveis, os seguintes requisitos devem ser atentidos:

1. O tempo de guarda dos *backup* devem seguir o período de retenção documentado na Matriz de Temporalidade, a depender do conteúdo do *backup*;

2. As mídias de *backups* mensais terão sua informação descartada decorridos 12 (doze) meses da sua criação. A mídia será sobrescrita ou descartada, caso tenha atingido sua vida útil ou apresente sinais de degradação.

3. O Administrador de *Backup* deve comunicar seu gestor, caso o uso do *storage* ou cofre atinja 80% de sua capacidade total, havendo tempo hábil para plano de ação.

6 Da frequência de *backup*

6.1 A frequência de realização dos *backup* deve seguir a Tabela 4, de acordo com as Categorias de Dados.

CATEGORIAS	FREQUÊNCIA	RPO	RTO
LDAP (*Lightweight Directory Acces Protocol*)	01 vez a cada serviço integrado	N/A	N/A
Banco de Dados	Diariamente ou com mais frequência	24 h	30 min a 1 h
Infraestrutura	Mensalmente ou antes de uma atualização dos servidores ou dispositivos	N/A	30 min
Hospedagem	Mensalmente	1 mês	N/A
Sistemas Críticos	Mensalmente ou antes de uma atualização dos sistemas	N/A	20 min
Sistemas Secundários	Mensalmente ou antes de uma atualização dos sistemas	N/A	20 min
Sistema Legado	Não se aplica. 01 unidade de *backup* final	N/A	20 min
Sistemas e Plataformas *WEB*	01 vez a cada novo serviço	N/A	N/A
Virtualização	Mensalmente ou antes de uma atualização do ambiente	N/A	30 min a 1 h
Compartilhamento de Arquivos	Diariamente ou com mais frequência	24 h	N/A
E-mail	Diariamente ou com mais frequência	04 h	N/A
Arquivos da Matriz de Temporalidade	A depender de solicitação	N/A	N/A

Tabela 4 – Frequência de backup

7 Do descarte de mídias

7.1 O descarte de mídias de *backup* deverá ser feito mediante solicitação, via chamado TOPdesk, pela Equipe de *backup* ao Administrador de *backup*, que então fará p descarte da mídia.

NOTA. As mídias físicas a serem descartadas deverão ser destruídas fisicamente, seguindo orientações do fabricante, de forma a impedir a sua reutilização ou acesso indevido.

7.2 O descarte de mídias físicas deve ser realizado adequadamente, seguindo as normativas de proteção ao meio ambiente.

8 Do procedimento de restauração

8.1 A restauração dos *backup* deverá obedecer as seguintes orientações:

1. Todo e qualquer usuário que precise recuperar arquivos, deve realizar a solicitação via chamado no TOPdesk;
2. A solicitação deve contemplar, obrigatoriamente: nome e setor do solicitante, identificação do arquivo a ser recuperado (nome ou aproximação do nome), diretório e subdiretório em que se encontrava e a data da versão que deseja recuperar;
3. O chamado será encaminhado à Equipe de *backup*, que após conclusão das ações, aguardará o aceite de fechamento da solicitação;
4. Deve ser mantido, pela Equipe de *backup*, registro de todos os arquivos cuja restauração foi solicitada, juntamente com as informações relativas à solicitação, em relatório de recuperação;
5. O solicitante terá total responsabilidade pela validação da recuperação solicitada;
6. A restauração dos arquivos somente será possível nos casos em que o arquivo tenha sido contemplado nos procedimentos e rotinas de *backup* e tenha passado por esse procedimento. Isto é, arquivos criados e eventualmente apagados ou alterados antes de passarem pela rotina de *backup* não poderão ser restaurados.

NOTA. Para efeitos práticos, o chamado no TOPdesk pode servir como Relatório de Restauração, desde que as informações sejam descritas pela Equipe de *backup*.

9 Dos testes de restauração

9.1 As cópias de segurança armazenadas deverão ser testadas mensalmente. A cada mês serão testados domínios de dados distintos, em amostragem aleatória, para que em um período de um ano, todos as Classificações de Dados passem por testes de restauração.

9.1.1 A Equipe de *backup* deverá definir um cronograma para os testes de restauração.

9.1.2 O teste será realizado com o intuito de validar a suficiência dos dados e a integridade das mídias de *backup*.

9.1.3 Para todos os testes realizados, deverá ser gerado um relatório, com parecer da Equipe de *backup*, que será enviado ao Administrador de *backup*, a título de registro e controle.

10 Das auditorias

10.1 A auditoria interna desta Política deve constar no ciclo anual de auditorias internas da cooperativa.

10.2 A Equipe de Auditoria poderá consultar o Administrador de *backup* e/ou a Equipe de *backup*, para definir os requisitos a serem auditados.

10.3 O Administrador de *backup* e colaboradores da Equipe de *backup* não podem compor a Equipe de Auditoria.

3.2.6 Registros

11 Essa Política gera os seguintes registros:

1. Relatório de execução de *backup*;
2. Relatório de teste de *backup* e recuperação;
3. Relatório de recuperação de *backup*

3.2.7 Referências Bibliográficas

AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR. Resolução Normativa - RN n∘ 507. Distrito Federal, 11 de março de 2022.

AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR. Resolução Normativa - RN n∘ 518. Distrito Federal, 29 de abril de 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001 : Tecnologia da informação — técnicas de segurança — sistemas de gestão da segurança da informação — requisitos. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002 : Tecnologia da informação — técnicas de segurança — código de prática para controles de segurança da informação. Rio de Janeiro, 2013.

CENTER FOR INTERNET SECURITY. CIS Critical Security Controls: Simplified and prioritized cyber defense guidance. East Greenbush, New York, 2021.

3.2.8 Histórico de Revisões

Revisão	Data	Responsável	Descrição
000	01/06/2023	Leonardo Sartori de Andrade	Emissão Inicial

Tabela 5 – Histórico de revisões

3.2.9 Aprovação

Documento aprovado pelo Conselho de Administração em: xx/xx/xxxx

Nome	Responsabilidade	Assinatura
	Diretor Presidente	
	Diretor Administrativo	
	Diretor Financeiro	
	Diretor Vogal	
	Diretor Vogal	
	Diretor Vogal	
	Diretor Vogal	

Tabela 6 – Aprovações

4 Resultados

Conforme explanado na Seção 2.2 e no Capítulo 3, uma organização deve analisar aspectos, internos e externos, que a afetam antes de produzir uma política corporativa. Dessa forma, para que uma política de *backup* e restauração seja produzida, uma organização deve possuir conhecimento sobre quais são os dados que devem ser protegidos e *backupeados*, quais são os sistemas e recursos críticos que devem possuir maior controle, segurança e salvaguardas quanto a sua disponibilidade, realizar um mapeamento dos ativos da empresa e classificá-los quanto ao nível de confidencialidade, quanto ao tempo de retenção da informação, quanto aos responsáveis pela informação (todo ativo deve possuir um responsável, durante todo seu ciclo de vida na empresa), considerar os riscos levantados no processo de gestão de riscos da organização e ainda, considerar o SLA de fornecedores de sistemas e recursos importantes para a operação da organização.

No 3, foi apresentado um estudo de caso em uma cooperativa de trabalho médico, aplicando a metodologia proposta. Evidentemente, para o estudo de caso, o contexto da organização é relevante para a produção da política de *backup* e restauração. A cultura organizacional, os processos de gestão de riscos, segurança da informação, políticas de privacidade e proteção de dados e de segurança da informação, o processo de implantação da LGPD, e todas as questões internas citadas no parágrafo anterior, já estavam consolidados dentro da organização, fazendo com que a política de *backup* e restauração tenha suporte de outras políticas e documentos e seja focada, especificamente, nos procedimentos de cópia de segurança das informações.

Deve-se considerar que a implantação da política de *backup* e restauração na cooperativa se deu em um cenário onde já existia uma cultura organizacional de segurança da informação, de proteção de dados e cumprimento com a LGPD, conforme disposto na seção 3.2.1. Por conseguinte, a organização deve avaliar qual é o seu nível de maturidade no processo de proteção de dados e aplicar a metodologia proposta no presente trabalho, respeitando esse nível, a infraestrutura e recursos disponíveis para a implantação da política. Em suma, uma organização não deve ter expectativas de aplicar a metodologia proposta por esse trabalho em um cenário inicial de implantação do processo de proteção de dados, onde não há controles básicos para a segurança da informação, tais como gerenciamento de ativos e o gerenciamento de acesso.

A análise do nível de maturidade pode ser observada nos *frameworks* estudados. No NIST NIST (2018) existem as Funções da Estrutura Básica, que devem ser executadas simultaneamente, ou seja, não é possível executar uma função sozinha, sem que as outras não estejam envolvidas. Por exemplo, não é possível responder um incidente que não foi

detectado, e não é possível detectar um incidente com um ativo que não foi identificado.

No CIS *CONTROLS* CIS (2021), existe uma estrutura hierarquisada de Grupos de Implementação, que determinam uma ordem de implementação de controles, tal que o IG2 embarca todos os controles do IG1 e o IG3 embarca todos os controles do IG1 e IG2. Nesse sentido, todas os controles básicos já implementados pela cooperativa do estudo de caso dão condições para implementação de controles de alto nível, como é o caso da política de *backup* e restauração.

Os produtos da implantação da política na organização foram:

- Atualização dos procedimentos operacionais de *backup* pré-existentes;
- Criação de procedimentos operacionais de teste dos arquivos de *backup*;
- Criação de procedimentos operacionais de recuperação de serviços e dados;
- Mitigação de riscos críticos da empresa, sobretudo riscos relacionados a disponibilidade de dados, resposta a incidentes de segurança e recuperação de desastre;
- Cumprimento de ações e diretrizes previstos na política de segurança da informação e no suporte à efetivação dos direitos dos titulares de dados, previstos na Brasil (2018a);
- Atribuição de novas responsabilidades aos colaboradores da organização, sobretudo dentro do setor de TI.

Por meio da revisão da literatura, dos trabalhos relacionados, das boas práticas sugeridas nos *frameworks* estudados, da investigação das questões de pesquisa, da aplicação da metodologia em um cenário real e dos resultados da implantação da política na organizaçao, pode-se validar a hipótese de pesquisa levantada pelo presente trabalho. Foi proposta uma metodologia de implantação de política de *backup* e restauração para uma organização da área da saúde, aplicada em uma cooperativa de trabalho médico, gerando um documento que foi capaz de atender as necessidades da cooperativa. Assim como a pesquisa de Moraes (2007) e as normas ISO/IEC abordadas sugerem, um plano de *backup* deve ser alinhado aos objetivos da organização, com a gestão de riscos e com os processos de segurança da informação, conduz ao desenvolvimento de uma política implementável e funcional. A metodologia proposta nessa pesquisa cumpre com esse planejamento, através do levantamento das necessidades da organização, da definição dos requisitos da organização quanto a política de *backup*, da classificação dos dados a serem guardados, das definições de tempo de retenção, frequência, responsabilidades dos *backups* (variáveis de negócio), e finalmente, da abrangência, escopo e conteúdo da política de *backup* e restauração.

5 Conclusão

Diante do cenário exposto no Capítulo 1, uma cooperativa de trabalho médico buscou aprimorar seus processos de proteção de dados e conformidade com a LGPD por meio da implantação de uma política de *backup* e restauração, levando o autor do presente trabalho a propor uma metodologia para o desenvolvimento da política e considerar a hipótese de que a metodologia possa ser implementada com êxito e resultar em uma política de *backup* e restauração que atenderá as expectativas de uma organização da área da saúde, no que tange ao seu processo de proteção de dados.

Para a construção deste trabalho foi realizado um estudo da literatura objetivando entender os principais conceitos relacionados a *backup*, qual a importância dos procedimentos de *backup* para as corporações e como eles se relacionam com a estratégia e os processos internos das organizações. A partir dessa pesquisa, foi ponderada uma metodologia, uma estratégia a ser seguida, para a construção de uma política de *backup* e restauração para uma organização do ramo da saúde.

O primeiro passo da metodologia é o levantamento das necessidades da organização, disposto na Seção 3.1.1, quanto a política de *backup* e restauração. O segundo passo, disposto na Seção 3.1.2, e o terceiro passo, disposto na Seção 3.1.3, consistem na definição das variáveis de negócio e das responsabilidades dos envolvidos, que contribuem para determinar diretrizes do escopo da política. Por conseguinte, o passo seguinte é a definição do escopo da política.

O desenvolvimento desses 4 passos iniciais contribuem para responder as questões de pesquisa do presente trabalho: 1 - como as necessidades específicas da organização alvo influenciam o desenvolvimento da política; 2 - em que medida a implementação da política melhora a garantia da disponibilidade dos dados na organização; 3 - se a política está em conformidade com os regulamentos específicos da organização; 4 - como a política impacta a segurança dos dados sernsíveis e informações críticas da organização; 5 - como a política afeta a capacidade de recuperação dos dado e 6 - no que tange à garantia de atendimento às expectativas da organização.

Os passos seguintes da metodologia são o desenvolvimento do texto e aprovação das áreas responsáveis e consideração de um cronograma de implantação, contribuem para atender sugestões presentes na ISO 27001 ABNT (2013a). Por fim, o último passo, disposto na Seção 3.1.7, referente a manutenção e revisão da política, contribui para responder as questões de pesquisa 3 e 6.

Este trabalho apresentou uma metodologia para desenvolvimento de uma política de *backup* e restauração, aplicada em um cenário real, por meio de um estudo de caso,

utilizando a metodologia considerada. Essa política apoia a conformidade com a LGPD Brasil (2018a) garantindo, sobretudo, a disponibilidade e integridade de dados, seguindo boas práticas de gestão de riscos e segurança da informação propostas pelas ISO/IEC 27001 ABNT (2013a), ISO/IEC 27002 ABNT (2013b) e ISO/IEC 27003 ABNT (2020) e *frameworks*, NIST NIST (2018) e CIS *CONTROLS V.8* CIS (2021).

Esta pesquisa também estudou e apresentou dois *frameworks* de gestão de riscos de segurança da informação, que podem ser seguidos por organizações diversas, para o processo de implementação da gestão da segurança da informação e controles relacionados, como, no caso específico desta pesquisa, uma política de *backup* e restauração de dados. Também foram apresentadas normativas da ISO/IEC relacionadas à gestão da segurança da informação e uma metodologia para a produção de uma política corporativa de *backup* e restauração de dados, a qual respeita e colabora com o regimento, estrutura organizacional e processos internos de uma organização alvo, com o objetivo de cumprir seus objetivos legais e estratégicos.

As dificuldades encontradas na presente pesquisa se resumem a encontrar trabalhos que abordem, especificamente, como se dá o processo de produção de um plano ou política de *backup* e restauração corporativo. Apesar de ser evidente, na literatura, a importância dsses procedimentos para as organizações e quais são as boas práticas acerca desses procedimentos, não foram encontrados muitos exemplares que ilustram o processo e as etapas de elaboração de uma política de *backup* e restauração.

Para melhorar esse modelo, pode-se incorporar um estudo mais detalhado do cenário da organização, no que diz respeito aos recursos de infraestrutura para armazenamento das cópias de segurança, durante a fase de levantamento das necessidades da organização. Cada *backup* possui um tamanho, uma quantidade de espaço que ocupa com o seu armazenamento em disco. É importante que a organização tenha ciência disso e de como é o crescimento da extensão desses arquivos, conforme afirma Santos (2018), uma organização deve se atentar a estrutura necessária para armazenar os arquivos de backup e em estratégias para manter procedimentos de *backup* sustentáveis.

Além do estudo de recursos de infraestrutura, como trabalho futuro pode-se propor o levantamento de métricas e indicadores técnicos para avaliar a eficácia dos procedimentos implementados pela política, no cumprimento de seus objetivos dentro da organização. A avaliação da eficácia irá contribuir para o processo de manutenção, revisão e melhoria da política e também da metodologia proposta neste trabalho. Um ponto interessante de aprimoramento dessa metodologia seria transformá-la numa metodologia aplicável em organizações de diversas áreas de negócio, porte e contexto organizacional.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27001*: Tecnologia da informação — técnicas de segurança — sistemas de gestão da segurança da informação — requisitos. Rio de Janeiro, 2013. Citado 6 vezes nas páginas 14, 20, 42, 46, 65 e 66.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27002*: Tecnologia da informação — técnicas de segurança — código de prática para controles de segurança da informação. Rio de Janeiro, 2013. Citado 8 vezes nas páginas 14, 17, 20, 21, 22, 42, 43 e 66.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27003*: Tecnologia da informação — técnicas de segurança — sistemas de gestão da segurança da informação - orientações. Rio de Janeiro, 2020. Citado 3 vezes nas páginas 19, 20 e 66.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Citado na página 24.

BRASIL. Lei nº 8.213, de 24 de julho de 1991. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 1991. Dispõe sobre os Planos de Benefícios da Previdência Social e dá outras providências. Citado na página 24.

BRASIL. Lei nº 5.172, de 25 de outubro de 1996. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 1996. Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios. Citado na página 23.

BRASIL. Lei nº 9.430, de 27 de dezembro de 1996. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 1996. Dispõe sobre a legislação tributária federal, as contribuições para a seguridade social, o processo administrativo de consulta e dá outras providências. Citado na página 24.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Citado 6 vezes nas páginas 13, 22, 23, 41, 64 e 66.

BRASIL. Lei nº 13.787, de 27 de dezembro de 2018. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 2018. Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Citado na página 25.

BRASIL. Resolução normativa rn nº 507, de 30 de março de 2022. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 2022. Dispõe sobre o Programa de Acreditação de Operadoras de Planos Privados de Assistência à Saúde. Citado 4 vezes nas páginas 27, 28, 40 e 41.

BRASIL. Resolução normativa rn nº 509, de 30 de março de 2022. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 2022. Dispõe sobre a transparência das informações no âmbito da saúde suplementar e estabelece a obrigatoriedade da

disponibilização do conteúdo mínimo obrigatório de informações referentes aos planos privados de saúde no Brasil. Citado na página 26.

BRASIL. Resolução normativa rn nº 512, de 31 de março de 2022. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 2022. Dispõe sobre a definição de índice de reajuste pela Agência Nacional de Saúde Suplementar - ANS - a ser aplicado pelas operadoras de planos de assistência à saúde aos seus prestadores de serviços de atenção à saúde em situações específicas e revoga as Resoluções Normativas nº 364, de 11 de dezembro de 2014 e nº 391, de 04 de dezembro de 2015. Citado na página 26.

BRASIL. Resolução normativa rn nº 518, de 29 de abril de 2022. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 2022. Dispõe sobre adoção de práticas mínimas de governança corporativa, com ênfase em controles internos e gestão de riscos, para fins de solvência das operadoras de plano de assistência à saúde. Citado 3 vezes nas páginas 26, 27 e 42.

BRASIL. Resolução normativa rn nº 543, de 02 de setembro de 2022. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 2022. Dispõe sobre a concessão de Autorização de Funcionamento das Operadoras de Planos de Assistência à Saúde e sobre o Registro de Produtos. Citado na página 26.

BRASIL. Resolução normativa rn nº 566, de 29 de dezembro de 2022. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 2022. Dispõe sobre a garantia de atendimento dos beneficiários de plano privado de assistência à saúde. Citado na página 26.

CENTER FOR INTERNET SECURITY. *CIS Critical Security Controls*: Simplified and prioritized cyber defense guidance. East Greenbush, New York, 2021. Citado 9 vezes nas páginas 14, 31, 32, 33, 43, 46, 50, 64 e 66.

EFE, A. *Brasil é 2º maior alvo mundial de ciberataques, revela estudo*. 2021. Disponível em: <https://noticias.r7.com/tecnologia-e-ciencia/brasil-e-2-maior-alvo-mundial-de-ciberataques-revela-estudo-27062022>. Acesso em: 01 dez. 2022. Citado na página 13.

EUROPEU, P. Regulamento (ue) 2016/679. *Jornal Oficial da União Europeia*, Estrasburgo, FR, 2018. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Citado na página 13.

GOVERNMENT, U. Public law no. 107-56. *U.S. Government Printing Office*, Washington, D.C, 2001. H.R.3162 - 107th Congress (2001-2002): Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. Citado na página 13.

HINTZBERGEN, J. et al. *Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002*. Rio de Janeiro: Brasport, 2018. Citado na página 14.

KENNEDY, C. G. et al. On information technology disaster recovery and its relevance to business continuity. In: SPRINGER NATURE SINGAPORE. *Proceedings of 2nd International Conference on Smart Computing and Cyber Security: Strategic Foresight,*

Security Challenges and Innovation (SMARTCYBER 2021). Singapore, 2022. p. 90–99. Citado na página 14.

MARQUES, M. E. P. Definição e implantação de políticas de segurança da informação numa empresa de gestão da saúde: um estudo de caso. *Monografia - Especialização em Rede de Computadores com ênfase em Segurança - Instituto CEUB de Pesquisa e Desenvolvimento, Centro Universitário de Brasília*, Brasília, 2016. Citado 2 vezes nas páginas 36 e 37.

MORAES, E. M. *Planejamento de backup de dados*. Dissertação (Mestrado) — Gestão e Desenvolvimento Regional - Universidade de Taubaté, Taubaté, SP, 2007. Citado 4 vezes nas páginas 35, 36, 37 e 64.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Cybersecurity Framework*: Framework for improving critical infrastructure cybersecurity. Gaithersburg, Maryland, 2018. Citado 7 vezes nas páginas 14, 29, 30, 31, 50, 63 e 66.

PEREIRA, J. R. Gestão de backup: um estudo de caso numa empresa prestadora de serviços de full outsourcing. *Trabalho de conclusão de curso - Tecnologia em Segurança da Informação - Faculdade de Tecnologia de Americana*, Americana, 2018. Citado 3 vezes nas páginas 14, 35 e 37.

PWC, R. *Global Digital Trust Insights Survey 2022*. 2021. Disponível em: <https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2021/global-digital-trust-insights-survey-2022.html>. Acesso em: 01 dez. 2022. Citado na página 13.

SANTOS, B. B. A. d. Backup corporativo com alta retenção: subsídios para contrução da arquitetura. *Dissertação (Programa Stricto Sensu em Gestão do Conhecimento e da Tecnologia da Informação) - Universidade Católica de Brasília*, Brasí'lia, DF, 2018. Citado 3 vezes nas páginas 36, 37 e 66.

SASSO, J. *TEM BACKUP?: Conceitos Básicos*. Amazon Prime: Amazon e-Book Kindle, 2020. Disponível em: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjzw-SL5IuAAxVgspUCHdV3BXIQFnoECA0QAQ&url=https%3A%2F%2Fwww.amazon.com.br%2FTEM-BACKUP-Conceitos-Jeferson-Sasso-ebook%2Fdp%2FB08LHJG4HY&usg=AOvVaw1YS-xwHQ8K-M2O3BaC2LVl&opi=89978449>. Citado 4 vezes nas páginas 14, 17, 18 e 19.

SILVA, E. P. Proposta de plano de continuidade de negócio em ti para um hospital norte catarinense. *UniSociesc*, Blumenau, SC, 2021. Citado na página 37.

SOMASUNDARAM, G.; SHRIVASTAVA, A. et al. *Armazenamento e gerenciamento de informações: como armazenar, gerenciar e proteger informações digitais*. EMC Education Services: Bookman Editora, 2009. Citado na página 17.

Anexos

ANEXO A – Mapeamento de Dados

O mapeamento de dados é uma forma de controle das operações de tratamento de dados pessoais de uma organização, através do qual são especificados, de acordo com os processos desenvolvidos pelas áreas da organização, quais os dados pessoais tratados, se são dados sensíveis ou não, qual a finalidade do tratamento e a base legal que o justifica, as medidas de segurança aplicadas para proteger o dado e o período de retenção.

O mapeamento de dados deve ser preenchido conforme exemplo abaixo:

Tabela 7 – Exemplo de preenchimento

Setor	Recursos Humanos
Processo	Recrutamento e seleção
Titular do dado	Candidato
Dado pessoal	Nome
Dado sensível	Não
Categoria de dados	Dado de identificação
Origem dos dados	Fornecido diretamente pelo titular
Tipo do tratamento	Coleta, Acesso, Armazenamento
Finalidade do tratamento	Identificar o candidato
Base legal	Consentimento
Legislação	Art. 7º, I, da Lei 13.709/18
Período de retenção	Indeterminado
Medidas de segurança	Controle de acesso, login e senha individuais de acesso ao sistema, termo de compromisso de sigilo e confidencialidade, armário com chaves
Forma de tratamento	Formulário web, sistema de processo seletivo, documentos produzidos ao longo do processo seletivo
Observações	O dado deve ser armazenado apenas durante o processo de recrutamento e seleção. Tão logo seja concluído, caso o candidato não seja contratado, deverá ser eliminado, salvo consentimento do candidato para armazenamento pelo período de 2 anos, na oportunidade de processos seletivos futuros

Fonte: Elaborado pelo autor

Esse mapeamento deve ser construído com a participação de todas as áreas da organização, haja vista que cada área terá conhecimento dos seus respectivos processos e, portanto, condições de indicar quais os dados pessoais envolvidos nas atividades. Nesse sentido, compete aos responsáveis pela área, seja o líder ou alguém que este designar, preencher a planilha, conforme roteiro previamente definido. Para conclusão do trabalho

de levantamento dos dados, é também possível que sejam feitas entrevistas.

No tocante à definição das bases legais que justificam o tratamento de dados, considerando que depende de conhecimento específico com relação à legislação aplicável, deverá ser feita pelo Encarregado de Dados da organização. A indicação das medidas de segurança, a seu turno, depende do suporte da área de Segurança da Informação.

É ideal que o mapeamento de dados seja revisitado periodicamente, de modo a garantir que ele reflita a realidade das atividades da organização. Além disso, é imprescindível que cada área notifique o Encarregado de Dados ao realizar um novo projeto, modificar um processo, desenvolver uma nova atividade ou qualquer alteração que tenha como consequência mudança no tratamento de dados, para viabilizar a atualização do mapeamento.

O mapeamento de dados é essencial à definição do ciclo de vida dos dados, que tem início com a coleta, perpassa pelo processamento e outras atividades, incluindo o armazenamento, e termina com a sua eliminação. Trata-se de documento que dá suporte à Política de Backup, uma vez que possibilita a identificação das informações com as quais a organização trabalha e, como consequência, oferece parâmetros para definições com relação àquilo que deverá ser objeto de backup, bem como o tempo de armazenamento desses dados.

ANEXO B – Matriz de Temporalidade

A matriz de temporalidade é o documento através do qual a organização identifica, por setores, quais os documentos, suas respectivas finalidades, prazo de guarda e o fundamento legal desse prazo e o local de arquivamento. Trata-se de um importante instrumento para a gestão documental e para a segurança dos processos, bem como instrumento de controle interno com relação ao risco de armazenamento de documentos e, consequentemente de dados, sem finalidade e justificativa legal que o ampare, e ao o risco de descarte ou eliminação indevido de documentos.

A matriz de temporalidade deve ser preenchida conforme exemplo abaixo:

Setor	**Documento**	**Finalidade**	**Prazo de guarda**	**Fundamento legal**	**Local de arquivamento**
Recursos Humanos	Contrato de trabalho	Formalização da relação trabalhista	2 anos, contados da rescisão contratual	Art. 7º, XXIX, da Constituição Federal	Pasta do colaborador armazenada em armário com chaves

Tabela 8 – Exemplo de preenchimento

Fonte: Elaborado pelo autor

Assim como o mapeamento de dados, a matriz de temporalidade deve ser elaborada com a participação das áreas, uma vez que compete a estas indicar quais os documentos com os quais trabalha, porque e onde arquiva. Não é cabível que apenas um colaborador assuma a responsabilidade de construir toda a matriz, sem respaldo das áreas, pois não tem condições de ter conhecimento amplo de todos os processos e atividades realizados na organização e quais os documentos envolvidos em cada um.

Ressalta-se a importância da matriz de temporalidade como documento acessório à Política de Backup, considerando a relação de complementariedade entre as duas. Isso porque a Política estabelece as diretrizes para a realização do backup, para que se tenha parâmetros para a realização das cópias de segurança e o devido armazenamento das informações. A matriz, por sua vez, estabelece o tempo que o documento deve ser armazenado, servindo de base para definição daquilo que será objeto de backup, por quanto tempo será mantido o backup e também para otimização dos recursos usados para fins de backup, considerando a quantidade de espaço que será necessária e o ciclo dos documentos na organização.