DISSERTAÇÃO DE MESTRADO PROFISSIONAL

UMA PROPOSTA DE OTIMIZAÇÃO DA COMUNICAÇÃO SIGILOSA NO SISBIN COM O USO DA COMPUTAÇÃO EM NUVEM PRIVADA

CILENO DE MAGALHÃES RIBEIRO

Programa de Pós-Graduação Profissional em Engenharia Elétrica
DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

UMA PROPOSTA DE OTIMIZAÇÃO DA COMUNICAÇÃO SIGILOSA NO SISBIN COM O USO DA COMPUTAÇÃO EM NUVEM PRIVADA

CILENO DE MAGALHÃES RIBEIRO

Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica

Banca Examinadora

Prof. Rafael Rabelo Nunes, Dr, FT/UnB _____
Orientador

Prof. Robson de Oliveira Albuquerque, Dr, FT/UnB _____
Coorientador

Prof. Selma Lúcia M. Gonzales, Dr, ESD/MD _____
Examinador externo

Prof. William Ferreira Giozza, Dr, FT/UnB _____
Examinador interno

Prof. Fábio Lucio Lopes de Mendonça, Dr, FT/UNB _____
Examinador interno

FICHA CATALOGRÁFICA

RIBEIRO, CILENO DE MAGALHÃES
UMA PROPOSTA DE OTIMIZAÇÃO DA COMUNICAÇÃO SIGILOSA NO SISBIN COM O USO DA COMPUTAÇÃO EM NUVEM PRIVADA [Distrito Federal] 2023.
xvi, 68 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2023).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Sisbin	2. Comunicação Sigilosa
3. Segurança da Informação	4. Nuvem privada
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

RIBEIRO, C.M. (2023). *UMA PROPOSTA DE OTIMIZAÇÃO DA COMUNICAÇÃO SIGILOSA NO SISBIN COM O USO DA COMPUTAÇÃO EM NUVEM PRIVADA*. Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 68 p.

CESSÃO DE DIREITOS

AUTOR: CILENO DE MAGALHÃES RIBEIRO
TÍTULO: UMA PROPOSTA DE OTIMIZAÇÃO DA COMUNICAÇÃO SIGILOSA NO SISBIN COM O USO DA COMPUTAÇÃO EM NUVEM PRIVADA.
GRAU: Mestre em Engenharia Elétrica ANO: 2023

CILENO DE MAGALHÃES RIBEIRO
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Aos meus pais Olecino (*in memoriam*) e Celia (*in memoriam*) que sempre me motivaram a estudar e me desenvolver profissionalmente. À minha esposa Micheline e filhos, Celine e Lenon, pela compreensão e constante apoio mesmo nos momentos de ausências durante a elaboração desse trabalho.

AGRADECIMENTOS

Agradeço inicialmente a Deus pelo dom da vida, pela saúde e pela motivação que me permitiram ultrapassar todos os obstáculos encontrados ao longo da realização deste trabalho.

À minha família pelo apoio incondicional, pelo companheirismo e pela compreensão nas minhas ausências necessárias para me dedicar ao mestrado.

Aos professores Rafael Rabelo Nunes (orientador) e Robson de Oliveira Albuquerque (co-orientador) pelas correções e orientações transmitidas que foram fundamentais para eu chegar até aqui.

Aos professores do PPEE/UnB que ministraram as disciplinas do curso do mestrado. Os ensinamentos transmitidos certamente contribuíram muito para o amadurecimento e surgimento de novas ideias ao longo do processo de construção de conhecimentos.

Aos colegas do mestrado profissional PPEE/UnB pelas conversas, pelos trabalhos em conjunto e pelas amizades formadas ao longo deste período. Que o vínculo formado seja a base para novas conquistas.

À ABIN e à UnB, instituições promotoras deste mestrado, que esta parceria possa continuar a produzir frutos em benefício da transformação dos assuntos de Inteligência em algo mais acadêmico e difundido dentro da sociedade brasileira.

RESUMO

O Sistema Brasileiro de Inteligência (Sisbin) é considerado elemento fundamental para o assessoramento em informações ao chefe do poder executivo e atualmente é uma ferramenta utilizada para troca de conhecimentos e dados que não vêm atendendo a agilidade necessária aos interesses do Estado. Nesse intuito, este trabalho teve como objetivo propor procedimentos e uma arquitetura para a otimização do processo de comunicação sigilosa entre os órgãos do Sistema Brasileiro de Inteligência (Sisbin) com a proposta de utilização da computação em nuvem privada. Para alcançar o objetivo proposto, primeiramente foi elaborado um Modelo de negócio de valor (canvas) do processo de comunicação sigilosa como forma de compreensão da situação atual, contando com envolvimento de dezessete servidores de seis órgãos federais integrantes do sistema. Em prosseguimento, foi desenvolvido e aplicado um questionário para cento e trinta e sete pessoas de treze órgãos do Sisbin, como meio de valorar e obter apreciações técnicas sobre as informações do canvas. As opiniões e fundamentação teórica foram analisadas com base na Doutrina de Inteligência, Normativos e legislações específicas que tratam sobre a segurança da informação, cibernética e protocolos atuais, tudo diretamente relacionado ao fluxo de informações. Os resultados demonstram a necessidade da adoção de uma ferramenta tecnológica para otimização da troca de informações, motivo pelo qual foi proposto uma arquitetura de referência como uma solução utilizando nuvem privada. Como principal contribuição do trabalho, tem-se estabelecida a diretriz para o emprego de uma ferramenta de compartilhamento de trabalho integrado sobre uma proposta de nuvem privada, com possibilidade de elaboração conjunta, armazenamento seguro e suporte tecnológico centralizado.

ABSTRACT

The Brazilian Intelligence System (Sisbin) is considered a fundamental element for advising the head of the executive branch in information and is currently a tool used to exchange knowledge and data that has not been meeting the necessary agility to the State's interests. In this sense, this work aimed to propose procedures and an architecture to optimize the secret communication process between the agencies of the Brazilian Intelligence System (Sisbin) with the proposed implementation of private cloud computing. To achieve the proposed objective, first a canvas of the classified communication process was elaborated as a way to understand the current situation, with the involvement of seventeen servers from six federal agencies that are part of the system. Next, a questionnaire was developed and applied to one hundred and thirty-seven people from thirteen organs of Sisbin, as a means of evaluating and obtaining technical appraisals about the information in the canvas. The opinions and theoretical foundation were analyzed based on the Intelligence Doctrine, Normative and specific legislation that deal with information security, cybernetics and current protocols, all directly related to the flow of information. The results show the need to adopt a technological tool to optimize the exchange of information, which is why a solution architecture using a private cloud was proposed. As a main contribution of the work, a guideline has been established for the implementation of a work sharing tool implemented on a private cloud proposal, with the possibility of joint development and centralized technological support.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

5W2H	*5W: What – Why – Where – When – Who 2H: How – How much*
Abin	Agência Brasileira de Inteligência
ABNT	Associação Brasileira de Normas Técnicas
ADI	Ação Direta de Inconstitucionalidade
AES	*Advanced Encryption Standard*
AI	Atividade de Inteligência
APF	Administração Pública Federal
BPM	*Business Process Management*
BPVM	*Business Process Value Modeling*
CCAI	Comissão Mista de Controle das Atividades de Inteligência
CEPESC	Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações
CIDR	*Classes Inter-Domain Routing*
CIS	*Center for Internet Security*
CISET/SG/PR	Secretaria de Controle Interno da Presidência da República
COAF	Conselho de Controle de Atividades Financeira
CPU	*Central Processor Unit*
DSI	Departamento de Segurança da Informação e Cibernética
EB	Exército Brasileiro
END	Estratégia Nacional de Defesa
Enem	Exame Nacional do Ensino Médio
Enint	Estratégia Nacional de Inteligência
FA	Forças Armadas
FNSP	Força Nacional de Segurança Pública
FQDN	*Fully Qualified Domain Name*
GDPR	*General Data Protection Regulation*
Gefron	Grupo Especial de Fronteira
GPS	*Global Positioning System*
GRSIC	Gestão de Riscos de Segurança da Informação e Comunicações
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
IaaS	*infrastructure as a service*
Ibama	Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis
IBGE	Instituto Brasileiro de Geografia e Estatistica
INEP	Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira
IP	*Internet Protocol*
ISO	*International Organization for Standardization*

Continua na próxima página

LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados
MD	Ministério da Defesa
MJ	Ministério da Justiça
MP	Medida Provisória
NIST	*National Institute of Standards and Technology*
PaaS	*plataform as a service*
PCP	Plataforma Criptográfica Portátil
PF	Polícia Federal
PNI	Política Nacional de Inteligência
PNSI	política Nacional de Segurança da Informação
PRF	Polícia Rodoviária Federal
PSB	Partido Socialista Brasileiro
Risti	Revista Ibérica de Sistemas e Tecnologias de Informação
RSA	Rivest-Shamir-Adleman
SaaS	*software as a service*
SDDC	*Software-Defined Data Center*
Senasp	Secretaria Nacional de Segurança Pública
Serpro	Serviço Federal de Processamento de Dados
SI	Segurança da Informação
Sisbin	Sistema Brasileiro de Inteligência
Sisfron	Sistema Integrado de Monitoramento de Fronteiras
SRF	Secretaria Especial da Receita Federal do Brasil
SSL	*Secure Sockets Layer*
STF	Supremo Tribunal Federal
STF	Supremo Tribunal Federal
SWOT	*strengths, weaknesses, opportunities e threats*
TCU	Tribunal de Contas da União
TIC	Tecnologia da Informação e Comunicação
TLS	*Transport Layer Security*
VPN	*Virtual Private Network*

Fim da Lista de Siglas

1 INTRODUÇÃO

O governo federal vem fomentado a integração de órgãos do sistema de inteligência, prevendo na legislação, a atuação de forma conjunta, como enfatizado na Política Nacional de Inteligência (PNI) [1] e na Estratégia Nacional de Inteligência (Enint) [2]. Tais documentos regulamentam os aspectos de cooperação entre órgãos, atuação em rede, compartilhamento e intercâmbio de informações e do trabalho coordenado e integrado [3].

A importância de trocar conhecimentos entre as estruturas de Inteligência com objetivos similares é um consenso entre aqueles que se dedicam a identificar, gerir e analisar informações de interesse do Estado em todo o mundo. No Brasil, o assunto está previsto na PNI , e na instituição do Sistema Brasileiro de Inteligência (Sisbin) e criação da Agência Brasileira de Inteligência (Abin), nos seus 1º, 2º e 3º artigos previstos na Lei 9.883, de 7 de dezembro 1999, com o objetivo de integrar as ações de planejamento e execução das atividades de Inteligência do país [4] [5].

O Sisbin foi criado para integrar ações de planejamento e execução das atividades de inteligência do Brasil. Sua função é realizar a troca de informações relevantes, facilitando a tomada de decisão pelo governo brasileiro [6]. Logo após sua implantação em 2002, com 22 órgãos, passou-se a avaliar a adesão de novos órgãos federais por meio do Conselho Consultivo do Sisbin. A relevância da atividade ocasionou uma expansão gradativa, chegando a alcançar 48 órgãos em 2021.

O processo de troca de informações de inteligência ocorre por meio de tramitação de documentos no Sisbin por dois canais: o hierárquico, que obedece à subordinação baseada na precedência funcional e o técnico, que se caracteriza por ligações de cooperação, em função da necessidade de conhecer. Esses canais devem possibilitar pronta e eficaz comunicação entre si e entre os diferentes níveis de decisão de um mesmo órgão, subsidiando o Poder Executivo na tomada de decisões.

Os conhecimentos obtidos pelo Sisbin são concentrados na Abin, órgão central do sistema, transmitindo ao decisor por meio do órgão a que estiver subordinado. Porém, no âmbito dos demais integrantes do sistema, as frações de inteligência também devem obedecer à cadeia hierárquica própria, conforme o artigo 5º da lei nº 9883, de 7 de dezembro 1999, de criação da Abin (Brasil, 1999).

No contexto atual, as mídias sociais têm impulsionado o fluxo de informações por aplicativos e *"chats online"*, como exemplo: *WhatsApp, Telegram, Signal, Facebook, Instagram,* dentre outros. Contudo, muitas vezes esses meios desinformam e publicam *fake news*, o que demanda agilidade no trâmite informacional, com a finalidade de melhor assessorar os decisores do Poder Executivo do Estado brasileiro. Assim, mesmo cercados por informação, nem sempre é possível contar com dados reais, verificados oportunamente. Desta forma, esses meios de comunicação informais potencializam a necessidade de uma estruturação organizada, com rápida capacidade de processamento e checagem dos dados por meio de fontes confirmadas, aumentando ainda mais a importância do Sisbin atuar conjuntamente [7].

Considerando a breve contextualização apresentada, o objetivo deste trabalho é propor procedimentos e uma arquitetura para a otimização do processo de comunicação sigilosa entre os órgãos do Sisbin com a implementação da computação [8] em nuvem privada no processo de comunicação sigilosa não classificada entre os órgãos do sistema, para agilizar, garantir e assegurar a troca de informações, tomando documentos basilares como a Lei de Acesso a Informação (LAI), [9], a PNI, a ENINT e normativos do Departamento de Segurança da Informação e Cibernética (DSIC) visando assegurar o cumprimento da legislação vigente, agilizando o fluxo de informações por canais seguros e padronizados para o Sisbin, com intuito de reduzir o tempo de tramitação de dados, possibilitar auditorias e ainda permitir trabalhos colaborativos de inteligência.

1.1 PROBLEMA DE PESQUISA

A produção de informações é um dos principais processos finalísticos da Abin, onde a premência do tempo acarreta um problema para o fluxo de informações de inteligência, de forma oportuna e que permita o uso de sistemas informatizados, com armazenamento disponível e compartilhado, com vistas a elaboração colaborativa de documentos. No que tange ao aspecto de sigilo documental, os órgãos do Sisbin tendem a empregar o esquema convencional de armazenamento, em que a equipe de infraestrutura de Tecnologia da Informação e Comunicação (TIC) atua com permissão total sobre os conhecimentos produzidos.

Neste modelo proposto de troca de informações via nuvem privada, tanto gestores e as partes interessadas conhecem o fluxo da informação e possuem a garantia de que o conhecimento só seja acessado por quem tem a credencial de acesso, contribuindo para a compreensão do problema.

1.2 OBJETIVO GERAL

Propor procedimentos e uma arquitetura de referência para a otimização do processo de comunicação sigilosa entre os órgãos do Sisbin utilizando a computação em nuvem privada.

1.2.1 Objetivos específicos

Com o objetivo geral proposto, os objetivos específicos foram definidos e cumpridos, quais sejam:

1. Diagnosticar o fluxo de informações no Sisbin.
2. Apresentar aspectos do processo de troca de informações no Sisbin.
3. Sugerir um processo de acreditação de pessoa ou órgão no Sisbin.
4. Propor referências tecnológicas que atendam aos requisitos de controle nas informações, permitindo auditar o uso da troca de informações no Sisbin.

1.3 JUSTIFICATIVAS

Os modelos utilizados para troca de informações sigilosas, se baseiam em estruturas que não possibilitam agilidade no trato da informação, construção de trabalho conjunto via rede privada [10] e a busca do viés de confirmação, deixando os gestores de alto nível hierárquico em situação de dificuldade para a tomada de decisão.

Com a adoção de um modelo que empregue a gestão da informação e a construção do conhecimento por vários integrantes do sistema, diversos pontos de vista podem ser confirmados para auxiliar no processo da tomada da decisão, assim como acompanhar os trâmites o fluxo da informação, possibilitando a realização de auditorias. A partir do momento em que as partes interessadas são incluídas no processo, via pedido de busca da informação, a visão dos gestores começa a se confrontar com as partes interessadas, indicando os pontos de controle, riscos envolvidos e atividades críticas, resultando em um problema estruturado e de fácil compreensão.

1.4 CONTRIBUIÇÕES DESSE TRABALHO

- A publicação do artigo "Um diagnóstico sobre o processo de comunicação sigilosa entre os órgãos do Sistema Brasileiro de Inteligência" 2022 na Revista Ibérica de Sistemas e Tecnologias de Informação (2022): 169-183 (Risti) [7] propiciou como contribuições: a necessidade de atualização da ferramenta para troca de informações, o tratamento de alguns fatores críticos, uma diretriz para uma nova ferramenta com nuvem privada, processos definidos, possibilitar a construção conjunta de documentos e prover suporte centralizado ao Sisbin.
- Também foi publicado o artigo "Mitigação dos Riscos à Privacidade através da Anonimização de Dados" 2022 na Revista Ibérica de Sistemas e Tecnologias de Informação (2022): 573-585 (Risti) [11], trazendo como contribuições a necessidade da seleção correta da técnica de anonimização, evitando a identificação dos registros e a importância da anonimização para proteção de dados, salvaguardando a privacidade de pessoas e evitando possíveis cruzamentos de informação.
- Outro trabalho já submetido e aceito em fase de elaboração na Revista Ibérica de Sistemas e Tecnologias de Informação (2023) trata sobre "O compartilhamento de dados e o uso dual do Sistema Integrado de Fronteiras do Exército (Sisfron)" onde a principal contribuição do trabalho está em fomentar o tratamento dos dados do Sisfron, incentivando a sua utilização por sistemas afins, como o Sisbin e orgãos da Administração Pública Federal. Por meio de tecnologias disruptivas, potencializando a indústria de defesa brasileira e o fortalecimento da segurança integrada do entorno estratégico brasileiro.

1.5 ESTRUTURA DA DISSERTAÇÃO

Esta dissertação está dividida da seguinte maneira: uma introdução, constando as publicações resultantes desse trabalho e a estrutura adotada.

No Capítulo 2 são abordados os referenciais teóricos e os trabalhos correlatos a respeito do tema deste trabalho. Nesse capítulo apresenta-se uma descrição sobre o Sisbin, Avaliação de Processos de Negócios, Mitigação de Riscos relacionados a privacidade de dados pessoais, Segurança da Informação, Compartilhamento de Informações de outros sistemas, Computação em Nuvem Privada, Requisitos voltados para Gestão de riscos na nuvem, Previsões Legais e Auditoria.

Em seguida, no Capítulo 3, apresenta-se a discussão do problema e proposta de solução, sendo subdivididas em método, considerações sobre problema e considerações sobre a pesquisa aplicada [12].

Em prosseguimento, o Capítulo 4 discute os resultados obtidos no Modelo de negócio de valor (canvas), o questionário aplicado e a proposta da nuvem privada a partir da aplicação da computação em nuvem, onde procurou-se propor uma solução para o problema e identificar controles de segurança e auditoria que podem ser utilizados em uma possível implementação.

Por fim, o trabalho apresenta as Conclusões no Capítulo 5 e elenca as premissas para os trabalhos futuros que podem ser realizados a partir desta pesquisa.

2 REFERENCIAL TEÓRICO E TRABALHOS CORRELATOS

Os aspectos teóricos sobre a comunicação sigilosa no Sisbin, as legislações que salvaguardam os assuntos sigilosos e estudos afins serão apresentados. Para tanto, merece destaque a definição de **Informação segundo a LAI, como sendo todos os dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato, sendo adotada nos órgãos nacionais** [9].

O conceito de informação sigilosa é anterior a Lei de Acesso a Informação. O Quadro 2.1 traz um compilado de legislações e demonstra a evolução dos dispositivos que tratam sobre a salvaguarda de informações.

Após breve histórico, atualmente entende-se que a **Informação Sigilosa é aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, ou ainda, aquelas abrangidas pelas demais hipóteses legais de sigilo, nos termos do Art. 4º da LAI, e nos termos do Art 3º do Decreto sobre acesso as informações** [9]. Vale destacar que hipóteses legais de sigilo contemplam as informações que não precisam ser classificadas, pois já tem seu sigilo garantido por outras legislações específicas [9].

Quadro 2.1: Legislações sobre salvaguarda de assuntos sigilosos

Decreto Nr	Data	Assunto
27.583	14/12/1949	Aprova o Regulamento para a Salvaguarda das Informações que interessam à Segurança Nacional
27.930	27/03/1950	Dispõe sobre a aplicação do Decreto nº 27.583, 14/12/1949.
60.417	11/03/1967	Aprova o regulamento para a salvaguarda de assuntos sigilosos.
69.534	11/11/1971	Altera dispositivos do regulamento para a salvaguarda de assuntos sigilosos.
79.099	06/01/1977	Regulamenta o Art.23 da Lei n° 8.159, 8 de janeiro de 1991, que dispõe sobre a categoria de assuntos sigilosos.
99.347	26/06/1990	Modifica o Art. 6º do Decreto nº 79.099, de 6 de janeiro de 1977, relativo a salvaguarda de assuntos sigilosos.
2.137	24/01/1999	Regulamenta o Art. 23 da Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a categoria dos documentos públicos sigilosos e o acesso a eles, e dá outras providências.
2.910	29/12/1998	Estabelece normas para a salvaguarda de documentos, materiais, áreas, comunicações e sistemas de informação de natureza sigilosa, e dá outras providências.
4.497	04/12/2002	Altera o art. 17 do decreto nº 2.134, de 24/01/1997, que dispõe sobre a categoria dos documentos públicos sigilosos e o acesso a eles, e dá outras providências.
4.553	27/12/2002	Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do estado, no âmbito da administração pública federal, e dá outras providências.
7.845	14/11/2012	Regulamenta procedimentos para o credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o núcleo de segurança e credenciamento.

Fonte: Autores

Informação Classificada é regida como aquela submetida temporariamente à restrição de acesso público em razão do seu teor e da sua imprescindibilidade para a segurança da sociedade e do Estado, possuindo três graus de restrições:

- Ultrassecreta, cujo tempo de restrição dura 25 anos;
- Secreta, cujo tempo de restrição dura 15 anos; e
- Reservada, cujo tempo de restrição dura 5 anos.

Assim, toda a informação classificada é sigilosa, porém nem toda a informação sigilosa é classificada. Esse ponto gera inúmeros conflitos de organização, difusão, controle e acesso à informação, já que para determinados tipos de controle, a informação classificada no executivo federal deve usar premissas próprias de criptografia de Estado e não deve ser realizada de qualquer maneira [7].

2.1 SISTEMA BRASILEIRO DE INTELIGÊNCIA (SISBIN)

O objetivo do Sisbin é fornecer subsídios aos tomadores de decisão vinculados ao poder executivo. Consoante o art. 1º, caput, da Lei 9.883/1999, o Sistema tem como objetivo integrar "as ações de planejamento e execução das atividades de inteligência do País, com a finalidade de fornecer subsídios ao Presidente da República nos assuntos de interesse nacional". O art. 2º, §1º, da mesma lei prevê a responsabilidade do Sistema pela "salvaguarda da informação de inteligência contra o acesso de pessoas ou órgãos não autorizados".

O Sistema foi composto por dezenas de órgãos e entidades da Administração Pública Federal (APF) que, direta ou indiretamente, produzem conhecimentos e realizam ações em defesa dos interesses do Estado e da Sociedade Brasileira, conforme figura 2.1. Onde a atuação do Sisbin consiste na articulação integrada e coordenada dos órgãos que o constituem, respeitada a autonomia funcional de cada instituição. O Sistema também se articula com órgãos estaduais e municipais, por meio das Superintendências Estaduais da Abin, presentes em todas as unidades da Federação.

Figura 2.1: Membros do Sisbin
Fonte:Abin

A Abin, portanto, enquanto órgão central do Sisbin, tem a responsabilidade de coordenar a obtenção de dados e a produção de conhecimentos de inteligência, promovendo a infraestrutura necessária para a interação e a capacitação de seus membros. Essa atuação em rede proporciona a formação de grupos de trabalho, regionais e nacionais, que contribuem para o fortalecimento do Sistema. O pleno funcionamento do Sisbin – e da própria Abin – exige constante compartilhamento de dados e conhecimentos de inteligência [13].

Nesse contexto, a atividade de inteligência vem demonstrando muitas experiências de integração de sistemas e comunidades de inteligência como uma forma relevante e bem-sucedida para se antepor as complexidades atuais. Os conhecimentos oriundos de uma única fonte, muitas vezes não são capazes de responder a contento, assim equipes multidisciplinares para produção de conhecimento oportuno e integrado tem fortalecido o emprego do Sisbin.[3]

O Sisbin, no ponto de vista jurídico, possui amparo na PNI que preconiza o intercâmbio de dados

nos termos da legislação vigente no âmbito do Sisbin, mas não dá mais detalhes sobre quais seriam estes dados [14]. Em agosto de 2021, o Supremo Tribunal Federal (STF), provocado pelos Partidos Políticos Rede Sustentabilidade e pelo Partido Socialista Brasileiro (PSB), deferiu parcialmente medida cautelar na Ação Direta de Inconstitucionalidade (ADI) número 6529 e impôs limites ao compartilhamento de dados, quando este, atender a interesses pessoais ou privados.

Assim, **o Sisbin "somente pode fornecer dados e conhecimentos específicos à Abin quando for comprovado o interesse público da medida, afastando qualquer possibilidade desses dados atenderem a interesses pessoais ou privados.** Os ministros também decidiram que, mesmo se houver interesse público, os dados referentes às comunicações telefônicas ou sujeitos à análise da Justiça não podem ser compartilhados com base no artigo 4o da Lei 9.883/1999, que instituiu o Sisbin e criou a Abin, em razão de limitação aos direitos fundamentais. **O STF declarou, ainda, que, nas hipóteses cabíveis de fornecimento de informações e dados à Abin, é imprescindível a instauração de procedimento formal e a existência de sistemas eletrônicos de segurança e registro de acesso, inclusive para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos."** [15].

A Atividade de Inteligência (AI) utiliza dispositivos legais que abrangem hipóteses de sigilo para garantir o fluxo de informações confidenciais em diferentes níveis [16]. De acordo com a PNI, o Sisbin e a Abin preveem o uso de técnicas e meios sigilosos como forma de preservar a ação, os métodos e processos, a obtenção de dados negados por meio de operações de Inteligência, a doutrina comum e os valores profissionais. Desta forma, a combinação do sigilo, obtenção dos dados negados com métodos próprios e flexíveis dentro de um sistema integrado são necessidades urgentes, visando o atingimento do estado da arte no que tange a informação, pois permitem gerar credibilidade e viés de confirmação por serem checados por diferentes fontes de observação.

Por agirem de forma autônoma, as agências aportam ao orgão central do sistema informações por ela obtidas ou produzidas, mediante livre conveniência. Nesse ponto, localizamos limitadores a uma integração para além da acepção de coordenação que vem se reproduzindo até hoje [3].

No âmbito do Sisbin, muito se fala sobre compartilhamento de dados e informações, bem como de ações coordenadas, sobretudo no campo da segurança pública [3]. Porém, os dados ou conhecimentos compartilhados, raramente são processados de maneira conjunta. Ainda que contenham alguma colaboração de outras instituições, o produto final geralmente é resultado do trabalho de análise de um único órgão, fortalecendo a necessidade de modernização tecnológica para facilitar as trocas de informações e trabalhos conjuntos. Tal compartilhamento de conhecimentos e dados ainda é realizado via Plataforma Criptográfica Portátil (PCP), tecnologia proprietária de segurança composta por um *hardware* criptográfico e respectivos módulos, que cifra/decifra qualquer tipo de documento digital, de modo a torná-los protegidos contra interpretação do conteúdo por quem não de direito. Esse equipamento, desenvolvido pelo Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (CEPESC) da Abin, começou a ser usado no fim de 2007 em organizações estratégicas do governo. [13].

Assim, como [3] relata a necessidade de maior integração no compartilhamento de dados e infor-

mações, [17] reforça também a importância do trabalho conjunto em todos os projetos de análise, como esforços de equipe, já que a colaboração é vista como o único futuro prático para uma inteligência relevante e bem sucedida. Desta maneira, a união de esforços de forma colaborativa e a integração são reforçadas por ambos os autores supramencionados.

Tendo em vista que o trabalho da inteligência se baseia fundamentalmente na análise de dados e informações, é imprescindível a comunicação ágil com outros órgãos e entes da sociedade, bem como a execução de operações de inteligência, com vista à obtenção de informação de difícil acesso. Vale destacar que as deficiências no processo de troca de informações são em verdade um entrave na própria operação e funcionamento do Sisbin. Em parte, devido à ampla gama de tecnologias de comunicação digitais disponíveis – mas não só por isso –, cada vez mais a integração e a cooperação entre órgãos públicos tornam-se o *modus operandi* da AI. Segundo [18], a AI é um trabalho essencialmente inter agências, cujo produto final é a disseminação do conhecimento produzido aos usuários envolvidos no processo sequencial de geração desse conhecimento.

2.2 AVALIAÇÃO DE PROCESSOS DE NEGÓCIOS

Como forma de gerenciar esses processos para que eles sejam executados com o máximo do seu potencial, extraindo deles os melhores resultados possíveis, algumas estratégias podem ser utilizadas, como o Business Process Management (BPM) ou Gerenciamento de Processos de Negócio [19]. Para [20], o BPM é conceituado como "um conjunto de métodos, técnicas e ferramentas para identificar, descobrir, analisar, redesenhar, executar e monitorar processos de negócios a fim de otimizar o seu desempenho" (tradução nossa).

Nessa linha, é perceptível que o BPM tem como objetivo analisar os processos oportunizando conhecer o seu fluxo de operação ou informacional, componentes e participantes de forma detalhada para, em seguida, promover melhorias sistêmicas e contínuas, visando alcançar a sua máxima eficiência [21]. Segundo [22], a Avaliação de Processos de Negócios foi uma teoria utilizada para determinar se os processos propostos para a gestão da comunicação sigilosa, estavam de acordo com as premissas elegidas e se geraram resultados satisfatórios.

A tomada de decisão, que pode ser conceituada como "o processo de identificação de um problema ou de uma oportunidade e a seleção de uma linha de ação para resolvê-lo" [23], se apresenta de maneira incessante no dia-a-dia de qualquer organização, sendo aplicável com um nível de maior ou menor complexidade a depender do aspecto organizacional que esteja sujeito àquela determinada escolha. As particularidades inerentes aos ambientes de negócios modernos implicam uma acentuação na complexidade das demandas direcionadas às organizações, as quais são constantemente pressionadas a atingir altíssimos patamares com o propósito de garantir a sua subsistência em um ambiente competitivo no qual apenas as entidades mais aptas são exitosas.

Como consequência, os processos que concretizam os objetivos de negócio dessas organizações tam-

bém se tornam mais complexos, sendo necessário o uso de técnicas como as de gerenciamento de processos de negócios para torná-los mais eficientes. Sob essa perspectiva, a aplicação do gerenciamento de processos de negócios [24] também envolve decisões dos mais diversos tipos que devem ser tomadas pelos atores que fazem parte dessa estrutura de gestão.

Esse tipo de avaliação possibilita a antecipação e tratamento dos problemas e permite o monitoramento do desempenho das atividades preconizadas. Segundo [25] a gestão com ênfase em processos pode ser essencial para trazer sucesso a longo prazo para uma organização, se baseada em estruturas flexíveis, receptíveis a demanda e que, ao mesmo tempo, promovam eficiência.

A percepção de [26] corrobora com outros autores sobre a aplicabilidade do BPM nas organizações pela sua contribuição para solucionar problemas organizacionais; muitas vezes causados pela competitividade, pelo crescimento da complexidade organizacional e pelo maior uso das tecnologias nas organizações.

Nesse contexto, vale reforçar que os processos são gerenciados para que sejam executados com o máximo do seu potencial, extraindo deles os melhores resultados possíveis, tendo por objetivo a análise dos processos, seu fluxo de operação informacional, assim como, seus componentes e participantes de forma detalhada, promovendo melhorias sistêmicas e contínuas, alcançando alto nível de eficiência.

Por outro lado, [22] destaca que os fluxos informacionais são implementados através das etapas de criação/aquisição, exibição, armazenamento, recuperação, compartilhamento e/ou uso das informações, o que contribui diretamente na realização dos objetivos institucionais, bem como apoia na tomada de decisão.

Assim, se torna fundamental o estabelecimento de critérios claros e a submissão desses critérios a uma tomada de decisão guiada por técnicas específicas que viabilizem a realização da melhor escolha possível, viabilizando a seleção do BPM mais compatível com os seus processos de negócios e com os objetivos estratégicos que serão alcançados por meio deles [20].

A avaliação de Processos de Negócios é realizada por meio de ferramentas úteis para a melhoria dos processos das organizações, devendo “ser utilizadas como tarefas permanentes e necessária à gestão de processos”. Diversas são as técnicas utilizadas para esse fim, e uma lista não exaustiva dessas técnicas poderia incluir *Brainstorming*, Diagrama de Espinha de Peixe (ou de Ishikawa), 5W2H, análise SWOT, dentre outras [27].

Essas técnicas clássicas são bastante úteis na compreensão de um processo. O modelo adotado desenvolve uma ferramenta Business Process Value Modeling (BPVM) onde um mapa visual facilita a percepção do processo como um todo e a análise das partes fundamentais na geração de valor de um processo [28]. O uso de ferramentas do tipo “canvas” são úteis para composição visual de uma estrutura analítica de modelo de processos, e visam explorar o potencial de resposta da demanda com base na proposta de valor, criação e entrega de valor e captura de valor [29] [30]. Isso viabiliza agilidade e assertividade no ciclo de melhoria de processos com maior aderência de resultados as necessidades da organização [28].

Autores recentes como [29] e [30] utilizam e ressaltam a importância do uso do Canvas para composição visual de uma estrutura analítica de modelo de processos, visando explorar o potencial de resposta da demanda com base na proposta de valor, criação e entrega de valor e captura de valor. Desta forma, o canvas foi preenchido dentro do contexto da organização, de forma visual, facilitando o mapeamento da concepção do processo e identificando suas partes importantes e críticas, sendo apresentado na seção de resultados.

No início da construção do canvas, a figura ilustrativa foi dividida em três colunas. Na primeira, tem-se as partes interessadas do processo; os seus participantes, a proposta de valor e a visão de futuro do processo. Na segunda coluna constam as principais atividades críticas em cujos resultados impactam diretamente o processo; os riscos; e as informações de controle (indicadores). Na terceira coluna tem-se o escopo do processo; sendo relatadas as suas entradas no início e suas entregas no final da análise em saídas. Desta forma, o desenvolvimento do modelo de negócio de valor, desenhado na metodologia canvas foi fundamental para compreender a comunicação entre os órgãos do Sisbin, sendo apresentado na seção de resultados.

2.3 A MITIGAÇÃO DE RISCOS NA PRIVACIDADE DE DADOS PESSOAIS

De acordo com a Lei Geral de Proteção de Dados (LGPD) [31] [32], dado pessoal é a informação relacionada à pessoa natural identificada, tais como nome, sobrenome, registro geral e cadastro de pessoa física ou identificável, assim como no caso dos dados de geolocalização, através do GPS, endereço IP e identificação de dispositivo [33]. Desta forma, as informações sigilosas que englobam dados pessoais terão que seguir o pressuposto na Lei n. 13.079, de 14 de agosto de 2018, que regulamenta os dados pessoais sobre todas as operações de tratamento de dados pessoais [34], 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 [35].

A LGPD prevê diversos tratamentos possíveis: "coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração". Dessa forma, os agentes de tratamento (como são chamados aqueles que realizam tratamento de dados) devendo observar os princípios previstos no artigo 5 da LGPD, onde define-se **"Anonimização: como a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo"** [35].

Nos órgãos públicos e privados, segundo a LGPD, é importante que se tenha uma política de governança onde seja indicada a condução do processo de anonimização de dados pessoais e sensíveis [36]. Dessa forma, evita-se caso de quebra de privacidade com dados insuficientemente anonimizados [37], possibilitando que todos os campos de dados confidenciais sejam anonimizados, a fim de remover informações

pessoais e reter o que for necessário para análise ou pesquisa posterior [38], fortalecendo a necessidade de conhecer, aspecto fundamental em inteligência de estado [39].

No estudo sobre proteção de dados pessoais a utilização da bases de dados anonimizada em fluxo informações é extremamente útil e eficiente, atendendo com êxito a LGPD [40] e a necessidade de conhecer, fundamental na atividade de inteligência, o que permite com eficiência a compartimentação dos dados trafegados. As técnicas simples de ofuscação de informações, também anonimizadas devem ser utilizadas em ambientes de redes controladas [41].

Assim, as ameaças de possíveis cruzamentos maliciosos nas informações podem ser minimizadas com a aplicação de técnicas de processamento de dados que remove das mensagens a possibilidade de identificar uma pessoa [41] , porém é importante a avaliação de cenário no caso concreto para evitar a redução significativa de utilidade do dado com a anonimização muito ampla das informações [11].

2.4 SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação (SI) pode ser compreendida como ações e medidas que visam à "proteção da confidencialidade, da integridade e da disponibilidade das informações" [42]. Somando-se a esses princípios também é comum se encontrar outras propriedades relacionadas à SI, tais como confiabilidade, não-repúdio, responsabilidade e autenticidade. Essa última, que está relacionada com a "propriedade de que uma entidade seja o que ela afirma ser" [42], se junta àquelas três primeiras para compor os requisitos mínimos de SI que são considerados pelo DSIC, do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), segundo a Política Nacional de Segurança da Informação (PNSI) [43].

Segundo o Glossário elaborado pelo DSIC, do GSI/PR, a SI "trata de ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações". Além de abranger todos os ativos de informação, que, conforme o Glossário de SI, são "meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização".

Conforme o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a PNSI, assim como a Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, definem que a SI abrange:

- a segurança cibernética;
- a defesa cibernética;
- a segurança física;
- a proteção de dados organizacionais; e

- as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação [44].

A Avaliação de Conformidade nos aspectos de segurança da informação proporciona adequado grau de confiança a um determinado processo, mediante o atendimento de requisitos definidos em políticas, procedimentos, normas ou em regulamentos técnicos aplicáveis. As atribuições relacionadas à avaliação de conformidade para a alta administração e para os agentes responsáveis pela avaliação estão descritas nos arts. 41 e 43 da IN GSI/PR nº 3, de 28 de maio de 2021. Dessa forma, pessoas, objetos, sistemas, plataformas, *softwares*, aplicativos, redes de dados ou qualquer fonte que contém, transmite ou processa dados, apresenta suas vulnerabilidades que devem ser estudadas e reduzidas utilizando mecanismos e práticas de segurança da informação [45].

Diversos padrões internacionais procuram traçar diretrizes sobre como essa disciplina deve ser gerenciada pelas organizações. Entre eles pode-se citar a série de normas da Associação Brasileira de Normas Técnicas/International Organization for Standardization (ABNT/ISO) 27000; o *CiberSecurity Framework* publicado pelo *National Institute of Standards and Technology* (NIST); o CIS Controls v8, publicado pelo *Center for Internet Security* (CIS).

Destaca-se que em todos esses padrões é consenso de que riscos de SI surgem e são mitigados por tecnologias, processos e pessoas. As pessoas são a base humana para desenvolver processos, ou seja, forma como as tarefas são executadas e a tecnologia o meio facilitador para estas implementações. De nada adiantará ter as melhores tecnologias e todos os processos bem arquitetados na empresa se o funcionário não estiver consciente do que faz parte e de que é responsável pela Segurança da Informação dos órgãos e instituições como um todo [46]. Os processos deverão criar controles e indicadores para a mensuração dos resultados. E as tecnologias, garantem que processos mapeados estejam em conformidade, caso contrário poderá iniciar um processo de impacto ao negócio [47].

2.5 SEGURANÇA CIBERNÉTICA

A Segurança Cibernética é definida como ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis [48].

Por outro lado, a Defesa cibernética compreende ações realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os ativos de informação de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e buscar superioridade sobre os sistemas de informação do oponente [43].

Vale ressaltar como princípios diretamente ligados a comunicação de informações sigilosas [49], amparadas na PNSI:

- a articulação entre as ações de segurança cibernética, de defesa cibernética e de proteção de dados e ativos da informação;
- o dever dos órgãos, das entidades e dos agentes públicos de garantir o sigilo das informações imprescindíveis à segurança da sociedade e do Estado e a inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas;
- o *need to know* para o acesso à informação sigilosa, nos termos da legislação;
- o consentimento do proprietário da informação sigilosa recebida de outros países, nos casos dos acordos internacionais; e a cooperação entre os órgãos de investigação e os órgãos e as entidades públicos no processo de credenciamento de pessoas para acesso às informações sigilosas; e
- integração e cooperação entre o Poder Público, o setor empresarial, a sociedade e as instituições acadêmicas.

2.6 EXEMPLO DE USO DE COMPARTILHAMENTO DE INFORMAÇÕES

O fluxo informacional no Sisbin pode ser abastecido com dados e conhecimentos fornecidos pelos órgãos componentes do Sisbin. Um exemplo muito efetivo é o Sistema Integrado de Fronteiras (Sisfron) [50]capitaneado pelo Exército Brasileiro (EB) [51], pois o sistema pretende atender a fiscalização e controle dos crimes transnacionais nas fronteiras, que é um dever e uma obrigação do Estado, particularmente no que tange a manutenção da segurança pública [52] nesse espaço vital da fronteira brasileira, com dez países vizinhos e 16.885 quilômetros de extensão [53], representando um desafio a administração pública, a constante vigilância e o monitoramento dessa região.

O Sisfron [54] é um sistema integrado de sensoriamento, de apoio à decisão e de emprego operacional cujo propósito é fortalecer a presença e capacidade de ação do Estado na faixa de fronteira brasileira [55]. Sua concepção foi idealizada pelo Comando do Exército, de acordo com a Estratégia Nacional de Defesa (END), em 2008, que orienta a organização das Forças Armadas (FA) com capacidades de monitoramento/controle, mobilidade e presença [56].

Esse sistema enfatiza o adensamento de órgãos militares nas fronteiras e potencializa a indústria nacional, enfatizando a necessidade de aplicar incentivos; frequência de utilização desses insumos; como são decididos os planejamentos de recursos; e sua eficácia na aplicação em modelos industriais, visando a execução de projetos estratégicos[57], alcançando tecnologias indispensáveis à defesa e à segurança. Dessa forma, pretende-se fomentar a integração do Sisfron com o Sisbin [58] potencializando ambos os sistemas de forma conjunta e integrada, conforme figura 2.2.

Nesse contexto, vale reforçar que que as fontes de informação, são dados não processados colhidos em

exercícios táticos [59], denominadas “Operações” [60], como a Operação Sentinela e a Operação Fronteiras Sul, inclusas no projeto Policiamento Especializado de Fronteiras e no Gefron ambos com o objetivo de atuar contra delitos fronteiriços [61] que podem favorecer significativamente a geração de conhecimentos de inteligência.

Figura 2.2: Possibilidades de integração do Sisfron
Fonte:Adaptado pelo autor (informação verbal)

A intenção é usar o Sisfron [62] enquanto provedor de informações concernentes às áreas de alto risco e com grande volume de crimes na faixa de fronteiras [63]. Os exercícios táticos são coordenados pelo Ministério da Justiça (MJ), contando com a participação integrada da Polícia Federal (PF), da Polícia Rodoviária Federal (PRF), da Força Nacional de Segurança Pública, da Secretaria Nacional de Segurança Pública (Senasp), da Sistema de Receita Federal (SRF), do Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis (Ibama) e das polícias civil e militar dos estados envolvidos, segundo [54]. Assim, possibilitando grande quantidade de informações para manuseio e direcionamento aos interessados no Sisbin.

2.7 COMPUTAÇÃO EM NUVEM PRIVADA

A Computação em Nuvem é um modelo que permite acesso ubíquo, conveniente e sob demanda, através da rede, a um conjunto compartilhado de recursos computacionais configuráveis (por exemplo: redes, servidores, armazenamento, aplicações e serviços), que podem ser rapidamente provisionados e disponibilizados com o mínimo de esforço de gerenciamento ou de interação com o provedor de serviços [43].

Seguem abaixo os tipos de serviços (de acordo com a arquitetura disponibilizadas pela nuvem):

1. Infrastructure as a service (IaaS): é o provisionamento pelo fornecedor de processamento, armazenamento, comunicação de rede e outros recursos fundamentais de computação, nos quais o cliente pode instalar e executar *softwares* em geral, incluindo sistemas operacionais (que podem vir instalados) e aplicativos. O cliente não gerencia nem controla a infraestrutura subjacente da nuvem, mas tem controle sobre o espaço de armazenamento e aplicativos instalados.

2. Plataform as a service (PaaS): Os recursos fornecidos são linguagens de programação, bibliotecas, serviços e ferramentas de suporte ao desenvolvimento de aplicações, para que o cliente possa implantar, na infraestrutura da nuvem, aplicativos criados ou adquiridos por ele. O cliente não gerencia nem controla a infraestrutura subjacente da nuvem que são fornecidos como IaaS (rede, servidores e armazenamento), mas tem controle sobre as aplicações implantadas e possivelmente sobre as configurações do ambiente que as hospeda.

3. Software as a service (SaaS): Neste modelo, o cliente tem a possibilidade de utilizar aplicações do provedor de serviços na infraestrutura de nuvem, que são acessíveis de forma transparente independente de dispositivo (desktops, tablets, smartphones, etc.). Essencialmente, trata-se de uma forma de trabalho cuja aplicação é oferecida como serviço, eliminando-se a necessidade de se adquirir licenças de uso e infraestrutura de TI (fornecida como IaaS) para utilizá-la. O cliente gerencia apenas as configurações dos aplicativos, específicas do usuário.

Nesse sentido, após a apreciação das normatizações de gerenciamento de riscos de SI, observa-se que preservados os requisitos mínimos de SI a computação em nuvem proporciona, por suas características essenciais, tais como acesso amplo pela rede, rápida elasticidade, serviços medidos por utilização, auto provisionamento sob demanda, compartilhamento através de pool de recursos [64].

Além das vantagens expostas, segundo [64] os modelos de implantação em nuvem possibilitam ampla flexibilidade na sua utilização, dividindo-se em nuvem privada, como a infraestrutura que está disponível para uso exclusivo de uma única organização; nuvem comunitária: como uma infraestrutura que está disponível para uso exclusivo de uma comunidade específica, formada por organizações que possuem interesses e preocupações comuns; nuvem pública, como uma infraestrutura disponível para uso aberto do público em geral; e nuvem híbrida: como uma infraestrutura de nuvem composta de duas ou mais infraestruturas de nuvem (privada, comunitária ou pública).

Segundo [65] as atualizações de normativas recentes sobre o uso de nuvem foram um reflexo da necessidade do uso da nuvem frente a pandemia do coronavírus, onde ocorreu a migração de centenas de órgãos públicos e privados para o modelo *home office*, aumentando a demanda por serviços em nuvem de forma exponencial. A transformação digital foi acelerada em meses o que aconteceria ao longo dos anos, e dentre as mudanças está a alta adesão à nuvem.

Diante disso, a normatização recente da instrução normativa n° 5/2021 do GSI/PR [43], dispôs sobre os requisitos mínimos de segurança de informação para utilização de soluções de computação em nuvem, visando uma adequação na sua utilização em organismos públicos e privados.

Em meio a alta adesão de serviços de nuvem, [64] sugere a necessidade de enfrentar riscos de transposição complexa, fato que funciona como incentivo para o tratamento das vulnerabilidades da computação em nuvem por entidades governamentais brasileiras, principalmente quando se refere a questionamentos acerca dos riscos que estão atrelados ao seu uso, com atenção ao tratamento de dados sensíveis.

Assim, preservados os requisitos mínimos de SI, a computação em nuvem, proporciona por suas características essenciais, as vantagens descritas a seguir [64]:

> - Acesso amplo pela rede: os recursos de nuvem estão disponíveis para acesso pela rede por diferentes dispositivos (estações de trabalho, smartphones, tablets, etc.) através de mecanismos padrões.
> - Rápida elasticidade: os recursos computacionais podem ser elasticamente provisionados e liberados, em alguns casos, de maneira automática adaptando-se à demanda.
> - Serviços medidos por utilização: os serviços de computação em nuvem automaticamente controlam e otimizam a utilização de recursos através de mecanismos de medição utilizados em nível de abstração associado ao tipo de serviço utilizado, como armazenamento, processamento, largura de banda e contas de usuário ativas.
> - Auto provisionamento sob demanda: o consumidor pode ter a iniciativa de provisionar recursos na nuvem e ajustá-los de acordo com as suas necessidades ao decorrer do tempo, de maneira automática, sem necessidade de interação com cada provedor de serviços.
> - Compartilhamento através de pool de recursos: os recursos computacionais do provedor são agrupados para servir a múltiplos consumidores (modelo multitenant) com recursos físicos e virtuais, sendo alocados e realocados dinamicamente de acordo com as demandas dos seus consumidores.

2.8 REQUISITOS VOLTADOS A SEGURANÇA EM NUVEM PRIVADA

Os tipos de serviços devem considerar o emprego de diversos níveis de abstração, visando aumentar a segurança na computação em nuvem e a eficiência na sua utilização, segundo os autores [45] e [66].

De forma similar o trabalho [67] indica um nível de segurança maior, assim como [66], mas também acrescenta que uma avaliação de desempenho de três servidores privados em nuvem devem ser considerados, diante de diferentes cenários de teste para avaliar o desempenho de CPU, memória e disco, possibilitando ilustrar a aplicabilidade destes *softwares* numa nuvem privada de baixo custo, com fácil gestão e alta

capacidade de desempenho, facilitando a compreensão e comparação do *software* NextCloud com outros softwares, dando ampla vantagem de utilização nessa ferramenta de código aberto se comparada aos outros servidores [68].

Nesse contexto, os autores [64] demonstram uma aplicação de um modelo de requisitos de segurança de computação em nuvem que de forma conceitual trata de quatro componentes – segurança de dados; avaliação de risco; requisitos técnicos, legais e de negócios e de conformidade, com um escopo mais amplo e complexo, baseado na participação de 480 funcionários de tecnologia de informação do governo australiano, promovendo uma percepção mais abrangente sobre o uso da segurança em nuvem.

Dessa maneira, a **Instrução Normativa n° 5/2021 do GSI/PR [43], dispôs sobre os requisitos mínimos de segurança de informação para utilização de soluções de computação em nuvem [69], regulamentando órgãos e entidades da administração pública federal, com prazo de readequação de contratos de até 12 meses, determinando que os interessados na adoção da tecnologia em nuvem elaborassem um ato normativo sobre seu uso seguro, contemplando no mínimo: uma política de segurança da informação do órgão ou entidade, ser homologado pela alta administração e divulgado a todas as partes interessadas, relacionar metas a serem alcançadas e os objetivos que regem o serviço de computação em nuvem, definir as funções e responsabilidades dos agentes consignados para o gerenciamento dos serviços em nuvem; e estabelecer a periodicidade para sua revisão, a qual não pode exceder a dois anos.**

Vale destacar que esse Normativo também dispõe sobre as competências do Gestor de Segurança e do Comitê de Segurança, além do procedimento para transferência de serviços e tratamento das informações, conforme a LGPD e estabelece as cláusulas contratuais mínimas, como termo de confidencialidade, garantia de exclusividade de direitos, proibição do uso de informações do órgão pelo provedor de serviço de nuvem para propaganda ou mecanismos afins, dentre outras orientações.

Considerando os avanços tecnológicos, a computação em nuvem se tornou uma realidade plenamente acessível às organizações, sendo mundialmente adotada por empresas e órgãos de governo. Dentre os benefícios da adoção deste modelo, destacam-se: redução de custos, elasticidade, redução da ociosidade dos recursos, agilidade na implantação de novos serviços, foco nas atividades finalísticas do negócio e uso mais inteligente da equipe de TI.

Em comparação aos proveitos da computação em nuvem, o uso de salas-cofre e salas seguras torna-se dispendioso, com perda de escala e eficiência, além de apresentar maior complexidade de operação e manutenção de equipamentos. Compete à autoridade máxima do órgão, com apoio do Comitê de Governança Digital, do Comitê de Segurança da Informação e Comunicações e do Comitê Estratégico de Tecnologia da Informação, a definição dos serviços de TIC, no todo ou em parte, que possam comprometer a segurança nacional, conforme os requisitos de confidencialidade, integridade, disponibilidade e autenticidade das informações envolvidas, em conformidade com a IN Nº 01 GSI/PR/2008 e suas Normas Complementares, e considerando os princípios de acesso à informação e sua imprescindibilidade à segurança do Estado e da sociedade, dispostos pela Lei nº Lei n° 12.527.

Este documento de Boas práticas, Orientações e Vedações tem força normativa legal, estando vinculado à Portaria MP/STI nº 20, de 14 de junho de 2016, na forma de anexo, tendo sido assinado, em sua última versão, pelo Secretário de Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão em 13/05/2016 e publicado na mesma data.

Além disso, os casos de serviços de TIC que possam comprometer a segurança nacional, os órgãos devem contratar serviços de computação em nuvem com os órgãos ou entidades da APF ou podem realizar diretamente Serviços de TIC Próprios. Nesse caso, os Serviços de TIC Próprios, quando comprometer a segurança nacional, sua operação não poderá ser compartilhada ou contratada de terceiros. Para tanto, a contratação de serviços em nuvem deverá respeitar a seguinte ordem de prioridade, quanto a capacidade de serviços que possa atender as necessidades do contratante: SaaS; PaaS e IaaS.

Vale ressaltar que os órgãos que não possuem infraestrutura de TIC própria ou que necessitem renová-la ou ampliá-la devem contratar IaaS, devendo a contratação direta de equipamentos de infraestrutura de TIC, como por exemplo, servidores e armazenamentos, somente poderá ser feita mediante justificativa aprovada previamente pela autoridade máxima do órgão ou pelo Comitê de Governança Digital, ou equivalente, caso esse tenha delegação para tal.

Assim, os órgãos deverão exigir, por meio de cláusulas contratuais, em conformidade com o disposto na NC 14/IN01/DSIC/GSIPR, que os dados e informações do contratante residam exclusivamente em território nacional, incluindo replicação e cópias de segurança (backups), de modo que o contratante disponha de todas as garantias da legislação brasileira enquanto tomador do serviço e responsável pela guarda das informações armazenadas em nuvem.

2.9 PREVISÕES LEGAIS E AUDITORIA

O STF, baseado no entendimento de Tércio Sampaio Ferraz Júnior, interpreta que a inviolabilidade do sigilo de dados refere-se apenas aos dados em trânsito durante os instantes da comunicação telefônica e telemática propriamente dita, não se aplicando aos dados já armazenados anteriormente. “Para o STF o sigilo garantido pelo art. 5º, XII, da CF refere-se apenas à comunicação de dados, e não aos dados em si mesmos” [14].

Esta visão, no entanto, é questionada por alguns acadêmicos quanto a sua validade para os dias atuais, levando em consideração “a crescente quantidade de informações íntimas armazenadas em servidores de e-mails e aplicações de troca de mensagens”. O inciso X, art. 5º da Constituição, contudo, é capaz de resguardar os dados armazenados em servidores de e-mail e aplicativos de mensagens, a depender do grau de privacidade das informações [70]. A jurisprudência da Suprema Corte, por hora, não alterou seu entendimento, mas inovou no tema de proteção de dados pessoais [71], ao também utilizá-lo, direta ou indiretamente, para fins de AI.

Em 2018, ministro do STF atendeu mandado de segurança do INEP contra Acórdão do TCU, que de-

terminava a este Instituto a entrega de dados individualizados do Censo Escolar e do Enem para auditoria do Programa Bolsa Família – por parte do TCU. O INEP alegou que a disponibilização dos dados comprometeria a médio e a longo prazos os objetivos públicos da sua pesquisa estatística, vulnerabilizando a privacidade dos indivíduos que prestaram as informações e alegando mudança de finalidade no tratamento dos dados [14].

Os incisos X, XIV e XXXIII do art. 5º da Constituição e a LAI asseguram o sigilo de dados pessoais. A divergência quanto ao dever de sigilo do INEP sobre os dados requisitados pelo TCU é matéria sujeita à reserva de jurisdição, não cabendo ao órgão de controle externo decidir sobre a caracterização de ofensa à garantia constitucional.

Nas palavras do ministro [14], apesar de o sigilo estatístico não ter caráter absoluto:

> [...] a transmissão a outro órgão do Estado dessas informações e para uma finalidade diversa daquela inicialmente declarada subverte a autorização daqueles que forneceram seus dados pessoais, em aparente violação do dever de sigilo e da garantia de inviolabilidade da intimidade.

No início de 2020, foi firmado Termo de Autorização entre o Serpro e a Abin, prevendo a disponibilização de informações como nome, filiação, endereço, telefone, dados dos veículos e foto dos portadores de carteira de motorista, com base no Decreto nº 10.046, de 2019, que dispõe sobre o compartilhamento de dados no âmbito da APF.

Ao cabo, o Termo foi revogado e a respectiva revogação publicada no Diário Oficial, por iniciativa do Serpro. Nota-se, mais uma vez, a consagração do princípio da finalidade, diretriz que ao longo do tempo vem sendo reforçada pela Suprema Corte.

Em outra questão, em de maio de 2020, o STF suspendeu a eficácia da MP nº 954/2020, que previa o compartilhamento de dados de usuários dos serviços de telefonia fixa e móvel com o IBGE, sem autorização dos titulares, para a produção de estatística oficial durante a pandemia do novo coronavírus, declarando-a inconstitucional.

A alegação da maioria dos ministros foi de que a Medida não definiu apropriadamente como e para que os dados coletados seriam utilizados, contrariando o princípio da finalidade. A incompletude do texto em relação à possibilidade de anonimização dos dados também foi citada [71]. Ademais, a citada MP violaria o direito constitucional à intimidade, à vida privada e ao sigilo de dados. Ao mesmo tempo, o Supremo reconheceu a existência de direito autônomo à proteção de dados pessoais (ADI nº 6387, 6388, 6389, 6390 e 6393).

Em matéria diversa, envolvendo diretamente o Sisbin, ainda em 2020, dois partidos políticos ajuizaram a ADI nº 6529 perante o STF, com pedido de medida cautelar em face do parágrafo único do art. 4º e do caput do art. 9º-A da Lei nº 9.883, de 7 de dezembro 1999, que institui o Sisbin e criou a Abin. Uma das argumentações para o pedido foi de que a Abin teria tido seu "poder requisitório de informações" no Sisbin demasiadamente aumentado em face de sua recente reestruturação regimental, fragilizando, assim, direitos

fundamentais mínimos dos cidadãos como sigilo, privacidade e intimidade.

Argumentaram ainda que em razão da capilaridade do Sisbin, a Abin teria o poder de requisitar dados de quaisquer investigações, sigilo fiscal, dados do COAF, dentre outras informações sigilosas, inclusive aquelas resguardadas por reserva de jurisdição. Em complemento, pediram ao STF balizas mínimas ao compartilhamento de dados de inteligência.

O STF, [14] confirmando a decisão prévia da liminar, assim decidiu:

> **[...] a) os órgãos componentes do Sisbin somente podem fornecer dados e conhecimentos específicos à Abin quando comprovado o interesse público da medida, afastada qualquer possibilidade desses dados atenderem interesses pessoais ou privados;**
> **b) toda e qualquer decisão pela qual se solicitarem os dados deverá ser devidamente motivada para eventual controle de legalidade pelo Poder Judiciário;**
> **c) mesmo quando presente o interesse público, os dados referentes às comunicações telefônicas ou dados sujeitos à reserva de jurisdição não podem ser compartilhados na forma do dispositivo, em razão daquela limitação, decorrente do respeito aos direitos fundamentais;**
> **d) nas hipóteses cabíveis de fornecimento de informações e dados à Abin é imprescindível procedimento formalmente instaurado e a existência de sistemas eletrônicos de segurança e registro de acesso, inclusive para efeito de responsabilização, em caso de eventual omissão desvio ou abuso.**

Esta decisão tem importância histórica para o Sisbin, uma vez que impôs diretrizes objetivas ao ato de compartilhamento de dados no âmbito do Sistema. Ainda que não expressa em legislação adequada, esta decisão pode ser considerada positiva para o Sisbin.

Dessa forma, a auditoria e registro de solicitação de dados por autoridade constituída possibilitada pela nuvem privada atenderia requisitos fundamentais para o exercício da democracia, como o controle e a gestão da informação, trilhas de auditoria e registro de solicitações, podendo ser escalonados os níveis de acesso diretamente proporcionais a hierarquização de usuários.

Em síntese, o referencial teórico e os trabalhos correlatados possibilitaram a identificação do Sisbin, a importância da avaliação de processos e negócios, a relevância da segurança da informação com a mitigação de riscos na privacidade de dados pessoais, aspectos relevantes da segurança da informação, a exemplificação e expansão do uso de compartilhamento de informações, a compreensão da computação em nuvem e seus requisitos voltados a segurança. E também as previsões legais e a auditoria como condicionantes fundamentais ao pleno desenvolvimento do sistema.

3 METODOLOGIA

3.1 OBJETIVO DA PESQUISA

O objeto desta pesquisa consistiu em diagnosticar e propor uma otimização no fluxo de informações sigilosas não classificadas no âmbito do Sisbin.

Para tanto, no primeiro passo foi realizado um diagnóstico sobre o assunto por meio de um Canvas e no segundo momento foi aplicada uma pesquisa para integrantes do Sisbin.

3.2 *LÓCUS* DA PESQUISA

A pesquisa está ancorada no Sisbin. A área de segurança de informações deste sistema foi escolhida para diagnosticar e otimizar o fluxo de informações e conhecimentos, buscando como escopo as informações sigilosas não classificadas.

A equipe total participante da pesquisa do Canvas foi composta por 17 docentes delimitados na área de ensino e 137 funcionários com perfis e cargos diferentes do Sisbin em geral.

3.3 CLASSIFICAÇÃO DA PESQUISA

Trata-se de uma pesquisa de natureza aplicada, com objetivos exploratórios e descritivos. Ela é descritiva pois "tem como principal objetivo descrever características de determinada população, fenômeno ou estabelecimento de relações entre variáveis" [72]. Ela é exploratória pois tem a intenção de se ter maior familiaridade com o problema estudado, compreendendo os desafios e oportunidades em se utilizar a computação em nuvem privada no processo de comunicação sigilosa não classificada entre os órgãos do Sisbin. Dessa forma, "torna-se possível construir hipóteses, que são características de uma pesquisa exploratória" [73].

A pesquisa foi qualitativa pois trabalhou com "universos de significados, motivos, aspirações, crenças, valores, atitudes, o que corresponde a um espaço mais profundo de relações, dos processos e dos fenômenos que não podem ser reduzidos à operacionalização de variáveis" [74].

Utilizou-se do Canvas para compreensão da problemática e um questionário como forma de coleta de dados [75]. Ele foi construído utilizando as informações da literatura de SI e computação em nuvem [76] e, também, de legislações específicas sobre a LAI e de inteligência. Essa metodologia [77] é tecnicamente conhecido por BPVM sendo empregada para identificação, análise e solução de problemas visando com-

preender e melhorar o modelo de gestão das comunicações sigilosas, tendo como propósito compreender as dimensões do processo de troca de informações de inteligência e seus pilares de sustentação da organização [74].

Autores recentes como [29] e [30] utilizam e ressaltam a importância do uso do Canvas para composição visual de uma estrutura analítica de modelo de processos, visando explorar o potencial de resposta da demanda com base na proposta de valor, criação e entrega de valor e captura de valor. Desta forma, o canvas foi preenchido dentro da contextualização da organização, de forma visual, facilitando o mapeamento da concepção do processo e identificando suas partes críticas, sendo apresentado na seção de resultados.

No desenvolvimento do modelo buscou-se criar um ambiente de discussão onde foram coletadas informações com servidores de seis órgãos federais, conforme figura 2.1, para levantamento dos problemas vivenciados na comunicação entre órgãos de forma eficiente. Para tanto, foram realizadas treze reuniões com servidores que lidam com informações de inteligência nos níveis tático-operacional e estratégico em seus escritórios de trabalho, os meses de julho a setembro do ano de 2021, visando facilitar a interação e aproveitamento em ambiente profissional. Esses questionamentos foram inseridos no modelo de negócio de valor que buscou descrever a maneira como um projeto pode criar, entregar e desenvolver valores em seu empreendimento.

A elaboração do Canvas possibilitou a formação de desenho explicativo constituído com os principais itens de um negócio, sendo uma forma prática e ágil de visualizar todo o processo em apenas um quadro analítico. Além disso, proporciona uma capacidade de decomposição do todo em partes, facilitando o desenvolvimento de trabalho em conjunto quando desenvolvido em grupo que envolve a mesma área temática.

Nesse contexto, também se utilizou o questionário com o objetivo abranger maior público do Sisbin, que não seria possível com outra forma de coleta de dados. O questionário continha questões fechadas, que se utilizaram de uma escala do tipo-likert de 5 pontos, cujas opções foram: discordo totalmente, discordo, não concordo/não discordo, concordo e concordo totalmente, segundo [78]. Também foi facultada a opção para o respondente informar o desconhecimento sobre o assunto, com a opção: não sei/não quero responder. Aproveitou-se também para realizar algumas perguntas abertas no final do questionário, com o objetivo de entender melhor necessidades específicas e o entendimento dos respondentes sobre a temática do levantamento de dados.

A análise dos dados do questionário foi realizada utilizando estatística descritiva para as questões fechadas, somando-se as marcações de discordo totalmente e discordo, onde essas duas opções compuseram a “discordância” com o item questionado; e concordo e concordo totalmente, sintetizaram a concordância com o assunto abordado. Os respondentes que não opinaram ou não concordaram/ não discordaram, foram descartados do percentual que concordou ou discordou. O questionário contou com a participação de 137 servidores de 13 órgãos do Sisbin e foi aplicado de 18 de outubro a 18 de dezembro de 2021 . A amostra foi não probabilística por conveniência direcionada a servidores que lidam com informações sigilosas no seu dia-a-dia. A metodologia adotada neste trabalho teve como objetivo propor procedimentos

e uma arquitetura para a otimização do processo de comunicação sigilosa entre os órgãos do Sisbin com a implementação da computação em nuvem privada.

3.3.1 Considerações sobre a elaboração da pesquisa aplicada

As informações obtidas no Canvas respaldaram a construção de um questionário, conforme Apêndice "A". Por meio de perguntas fechadas e abertas, ou seja, tendo um roteiro prévio, mas com espaço para o respondente apresentar suas opiniões nas formas objetiva e discursiva. Esse questionário teve como objetivo abranger um volume maior de pessoas e avaliar a tendência de aceitação de uma solução de modernização do processo de troca de informações utilizando solução de nuvem privada, com requisitos de segurança da informação, incluindo o uso de criptografia de estado.

As questões foram construídas segundo as informações obtidas sobre a segurança da informação, computação em nuvem e legislações específicas sobre a LAI e de inteligência. O uso do questionário teve como objetivo abranger maior público do Sisbin, que não seria possível com outra forma de coleta de dados.

3.3.2 Questões sobre o Canvas - Negócio de Valor

A criação do Modelo de Negócio de Valor, também conhecido como canvas, teve o objetivo de proporcionar uma melhor experiência visual e compreensão do todo. Assim como, a teoria das cores no canvas, baseado no círculo cromático também permitiu destacar aspectos de maior importância. Esta teoria, resumidamente, busca o entendimento da ligação entre a luz e a natureza das cores, alcançando diferentes campos do estudo. No contexto de compreensão sobre o que são as cores, sua formação e como o cérebro humano as interpreta, além, é claro, das melhores formas de sua utilização [79].

Dentro desse estudo e, com o foco na apresentação do Canvas, foi utilizado o conceito da harmonia complementar, cuja essência, baseia-se no círculo cromático, apresentado na Figura 3.1, com o uso de cores que estão em pontos opostos do círculo, criando, assim, uma combinação contrastante entre as cores, o que proporciona uma melhor percepção do conteúdo apresentado [80].

Figura 3.1: Círculo Cromático
Fonte:Adaptado pelo autor

A 1ª parte do questionário foi direcionada para o levantamento das Organizações federais dos entrevistados, onde usamos o recurso da abstração para preservar os autores, somente relacionando os órgãos participantes do Sisbin.

Enquanto que, a 2ª parte abordou os critérios pertinentes a SI, sobre a situação da comunicação atual entre os órgãos federais e a computação em nuvem privada, ressaltando a importância da produção de documentos com tecnologias que permitam edição conjunta. Também foram questionadas a importância do controle e da auditoria, o assessoramento ao chefe do executivo, a automatização de registros, o suporte centralizado e o baixo custo como fatores de impacto para a tecnologia apresentada, conforme Quadro 3.1.

Quadro 3.1: Questões baseadas na validação dos aspectos do processo de comunicação

Critérios	**Afirmativas**
Disponibilidade Integridade Confidencialidade Autenticidade	2.1) A troca de informações entre os órgãos vinculados ao Sisbin ocorre com rapidez, atendendo aos critérios de “Disponibilidade, Integridade, Confidencialidade e Autenticidade".
Consciência Situacional	2.2) A criação de uma nuvem privada destinada ao Sisbin para a comunicação de conhecimentos sensíveis, atenderia aos critérios de disponibilidade, confidencialidade e integridade e autenticidade atendendo ao fluxo informacional necessário a troca de informações. 2.3) Em uma nuvem privada temos a capacidade integrar atividades laborativas de vários órgãos de interesse no Sisbin, proporcionando modelagem em casos de trabalhos conjuntos. Essa ferramenta agilizaria a produção de forma cooperativa com vários órgãos no Sisbin. 2.4) Os órgãos do sistema de inteligência necessitam compartilhar conhecimentos, analisando conjuntamente cenários internos e externos de interesse do Estado para fins de assessoramento e decisão, com o estabelecimento de pontos focais para troca de informações para a produção de relatórios, a facilidade de acesso a nuvem privada e segura acarretaria uma vantagem para a comunicação entre os órgãos.
Oportunidade Imparcialidade	2.5) A plataforma atual utilizada para troca de conhecimentos e dados atende aos critérios de Oportunidade e Imparcialidade para a comunicação de conhecimentos e dados entre os órgãos.
Segurança e Gestão	2.6) A possibilidade de controlar o fluxo de comunicação (segurança e gestão) dos conhecimentos e dados são fundamentais para a comunicação entre os órgãos.
Auditoria	2.7) A plataforma atual atende os critérios de possível auditoria para a comunicação de conhecimentos e dados entre os órgãos. 2.8) A oportunidade de criar na nuvem privada trilhas de auditoria na comunicação de conhecimentos e dados são fundamentais no processo de controle na troca de informações entre os órgãos.

Fonte: Autor (2022, p. 12)

3.3.3 Questões baseadas na LAI

Em seguida, na 2ª parte da pesquisa [74] foram abordadas no Quadro 3.2 perguntas baseadas na LAI criptografia de estado e a importância dos postos de controle para tratamento das informações sigilosas.

Quadro 3.2: Questões baseadas na LAI

Tema de Interesse	**afirmativas**
Informações e conhecimentos não classificados	3.1) É importante a proteção no fluxo das informações sigilosas não classificadas, mesmo sem possuírem amparo legal previsto na LAI.
	3.2) As ferramentas utilizadas para a troca de conhecimentos sigilosos não classificados atendem as necessidades de agilidade no fluxo informacional atual.
Informações classificadas	3.3) O uso de criptografia de estado utilizado somente para informações classificadas conforme a atende aos critérios de segurança para o fluxo de informações entre os órgãos do Sisbin.
Consciência Situacional	3,4) O aumento da sensibilização, habilitação e criação de postos de controle para o tratamento das informações sigilosas potencializarão a utilização da comunicação por nuvem privada gerando agilidade, segurança e oportunidade.

Fonte: Autor (2022, p.13)

3.3.4 Questões inter-relacionadas

Na 3ª parte foram abordadas no Quadro 3.3 perguntas inter-relacionadas sobre a nuvem privada, LAI e Norma Complementar Nr 14 - R01 - Segurança da Informação em Nuvem.

Quadro 3.3: Questões inter-relacionadas

Tema de Interesse	afirmativas
Consciência Situacional	4.1) A manutenção do fluxo de troca de conhecimentos e dados entre os órgãos do sistema são fundamentais ao assessoramento baseado em inteligência. 4.2) A alta administração de cada órgão ou entidade da Administração Pública Federal deve considerar a Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) para definir a utilização ou não das tecnologias de computação em nuvem.
Suporte tecnológico	4.3) A Abin, como órgão central do Sisbin deve ser a provedora dos recursos tecnológicos para acessar a nuvem privada, também baseando o servidor em área sob sua responsabilidade?

Fonte: Autor (2022, p.13)

3.3.5 Questões abertas sobre o diagnóstico da comunicação sigilosa

Quadro 3.4: Questões abertas sobre o diagnóstico

Tema de Interesse	Questões
Nuvem Privada	4.4) Caso queira apresentar sugestões sobre o trabalho de pesquisa especificamente na utilização do modelo no que tange a tecnologia empregada utilize o campo abaixo.
Integração Sisbin	4.5) Caso tenha alguma sugestão que fortaleça a interação e troca de conhecimentos utilize o campo abaixo.
Indicação para envio de pesquisa	4.6) Indique pessoas que podem participar na coleta da pesquisa?

Fonte: Autor (2022, p.13)

As questões abertas, conforme o Quadro 3.4 permitiram maior flexibilidade e participação dos respondentes. E para atingir os objetivos propostos nesse estudo, não foi necessário identificação, optando-se por segmentar as respostas de maneira anônima, utilizando-se uma numeração de 1 a 137 para fazer remissão a cada respondente, quando necessário, incluindo siglas como, por exemplo, R01, R02 em diante.

3.3.6 Metodologia da Governança e Gerenciamento de Riscos de Segurança com a proposta da aplicação da Nuvem Privada no Sisbin

A forma de conduzir um grupo está diretamente ligada a sua liderança e ao acompanhamento na condução dos processos firmados no negócio. Assim, a metodologia de análise das questões fundamentais de governança na adesão dos serviços da nuvem dizem respeito à identificação e implementação de estruturas organizacionais adequadas, processos e controles para manter a gestão das pessoas com eficácia, primando pela segurança da informação e seu fiel cumprimento. Ressaltando-se que cabe ao Sisbin garantir a segurança da informação, de forma razoável, em toda a cadeia de fornecimento do conhecimento.

Ademais, a Gestão de Riscos dos ativos na Nuvem permite alinhar a exposição ao risco e a capacidade de gerenciar a tolerância ao risco do proprietário dos dados. Desta forma, caracteriza-se como principal meio de decisão e suporte para os recursos de TIC para proteger a confidencialidade, integridade, e disponibilidade dos ativos de informação na Nuvem tão necessária ao compartilhamento de informações sensíveis do Sisbin.

No entanto, para garantir a eficácia da Gestão de Riscos na Nuvem é preciso estabelecer requisitos

contratuais adequados entre os órgãos e adotar tecnologias capazes de coletar os dados necessários para informar as decisões de informação de risco (por exemplo, o uso da informação, acesso, controles de segurança, localização, etc), se fazendo fundamental a troca de experiências e opiniões entre os membros dos sistemas durante o desnrolar do processo.

Nesse intuito, o prestador de serviço de Nuvem deve incluir métricas e controles para auxiliar os orgãos (clientes) na implementação dos seus requisitos de informação de Gestão de Risco. Atualmente entidades como o Open Cloud Manifesto, Computing Use Cases Group e o Cloud Security Alliance trabalham no desenvolvimento de padrões de segurança para computação em nuvem, levando essas pesquisas para um grande número de áreas, incluindo auditoria, aplicativos, criptografia, governança, segurança de rede, gerenciamento de risco, armazenamento e virtualização. Segundo especialistas o primeiro passo é identificar as diferenças entre a segurança local e a segurança na nuvem e examinar quais padrões existentes combinam com as operações em nuvem [81].

Em síntese, a adoção do sistema de computação em nuvem pretende adotar padrões que permitam que os orgãos do Sisbin possam se integrar, seguramente, disponibilizando serviços de computação em nuvem de diferentes fornecedores e ter a garantia de que seus dados ficarão seguros na nuvem.

4 ANÁLISE DOS RESULTADOS

Nesta seção serão apresentados as análises dos resultados da pesquisa. Primeiramente, apresenta-se o canvas com as suas principais informações, na Seção 4.1 e as discussões entorno da elaboração dessa ferramenta de análise.

Em seguida são apresentados os resultados obtidos pela aplicação do questionário, com questões sobre o Canvas na Seção 4.2, a LAI (Seção 4.3); na sequência, estarão a análise das perguntas inter-relacionadas (nuvem privada, LAI e Normativo sobre Nuvem (Seção 4.4); por fim, apresentam-se a análise sobre as perguntas abertas (Seção 4.5).

Por fim, será analisado e proposto um modelo de comunicação de nuvem privada no âmbito do Sisbin (Seção 4.6).

4.1 O CANVAS DO MODELO DE VALOR DO NEGÓCIO

Um dos resultados da dissertação foi a elaboração do canvas do Modelo de Negócio de Valor, construído após 13 reuniões com 17 servidores do Sisbin, como apresentado na Figura 4.1. Dessa forma, foi consolidado em apenas uma página, as informações relevantes para a compreensão do processo de troca de informações sigilosas entre os órgãos do Sisbin. Ele proporciona diversos aspectos e permite o entendimento sobre o processo de troca de conhecimentos entre os órgãos do Sisbin.

Primeiramente, foi importante saber o que se pretende alcançar diante da problemática de otimizar o fluxo informacional no Sisbin, portanto após discussão em grupo o objetivo do processo foi estabelecido como: “propor um modelo de comunicação de conhecimentos e dados por meio de nuvem privada de fácil acesso entre os órgãos do Sisbin de forma confiável, disponível e segura”. Vale destacar que esse processo foi elaborado a partir de sugestões dos servidores do próprio Sisbin.

O conceito sobre as partes interessadas corresponde a todos os elementos (pessoas, instituições, grupos, órgãos governamentais, etc.) que de alguma forma afetam ou são afetados pela sua organização. Desta maneira, foram identificadas as seguintes partes interessadas para o processo: o Presidente da República; a Secretaria de Controle Interno da Presidência da República; a Comissão Mista de Controle da Atividade de Inteligência; o DSI; e outros Órgãos da APF que serão diretamente beneficiados com o fluxo de informações sensíveis.

A razão de existir desse processo, ou seja, o que ele deve entregar de valor para seus clientes e partes interessadas foram elegidas em: antecipar fatos ao decisor, possibilitando maior capacidade de decidir baseada em inteligência, automatização do registro da informação, gestão de conhecimentos e dados e garantir a comunicação mesmo com a interrupção do sistema por meios alternativos.

A visão de futuro consiste em antecipar ameaças e oportunidades de uma determinada situação, seja por meio da inteligência contextual ou por meio de análises sistêmicas de um setor. Vale destacar que pessoas dotadas dessa competência, geralmente, possuem significativa vantagem perante seus concorrentes. Dessa forma, o resultado desse processo foi buscar ser reconhecido como um sistema de comunicação de conhecimentos e dados do Sisbin, sendo um sistema eficiente para acessar conhecimentos sensíveis, operacionalizar equipes dotadas de capacidade para desenvolver processos normatizados e consolidar uma cultura de comunicação de conhecimentos entre os órgãos.

Para definição de risco foi entedido como "o efeito da incerteza nos objetivos". Entende-se como efeito, "um desvio em relação ao esperado, que pode ser positivo, negativo ou ambos, e pode criar ou resultar em oportunidades e ameaças". Partindo-se dessa definição, o conceito de Gestão de Riscos, de acordo com a norma, envolve atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos, cujo propósito é a criação e proteção de valor apoiando o alcance de objetivos. Assim, foram identificados como incertezas: a possibilidade de erro de uso do sistema por parte do usuário; falta de apoio dos membros do Sisbin; indisponibilidade do sistema; ataque cibernético ao sistema; vazamento de informações; manutenção da cifragem externa pelo usuário; informação difundida errada; e falta de infraestrutura tecnológica para suporte aos usuários.

Enquanto, que para as organizações foram caracterizadas como instituições de todos os tipos e tamanhos que enfrentam influências e fatores de ordem interna e externa, o que lhes tira a certeza do alcance de seus objetivos; a norma assegura ainda que gerenciar riscos auxilia as organizações no estabelecimento de estratégias, no alcance de objetivos e na tomada de decisões fundamentadas.

Nesse aspecto, relacionado a fatores internos e externos, a norma fundamenta que gerir riscos seja um processo integrante da governança e liderança das organizações, sendo de fundamental importância que ele permeie os demais níveis – como forma de contribuir para a melhoria dos sistemas de gestão como um todo. Isso revela a visão integrada pela qual a Gestão de Riscos deve ser encarada, não sendo preocupação apenas da alta gestão das entidades, mas de todos os seus níveis. De acordo com [42], a Gestão de Riscos possibilita criar e proteger valor nas organizações.

Também foram analisadas as atividades críticas, possibilitando que os riscos possam ser evitados, eliminados ou mitigados, sendo reduzidos para níveis aceitáveis para o sucesso do processo. Nesse sentido, tem-se como pontos de atenção contínua durante todo o processo: a infraestrutura de tecnologia de suporte, a manutenção da cifragem externa pelo usuário e garantir a troca de informações mesmo com interrupção do sistema.

Outro fator importante para o processo são as informações de controle que possuem a função de averiguar as atividades efetivas e se estão de acordo com o previsto no processo na forma que foi planejado, permitindo o monitoramento do processo e se o processo cumpre o seu objetivo, entregando o valor proposto, alinhado com a sua visão de futuro, controlando os riscos identificados. Nesse sentido, após ampla discussão se definiu que os principais indicadores a serem monitorados deveriam ser: o número de usuários do sistema, o número de relatórios em conjunto em desenvolvimento, a quantidade de mensagens trocadas e a quantidade de pessoas capacitadas para uso da ferramenta.

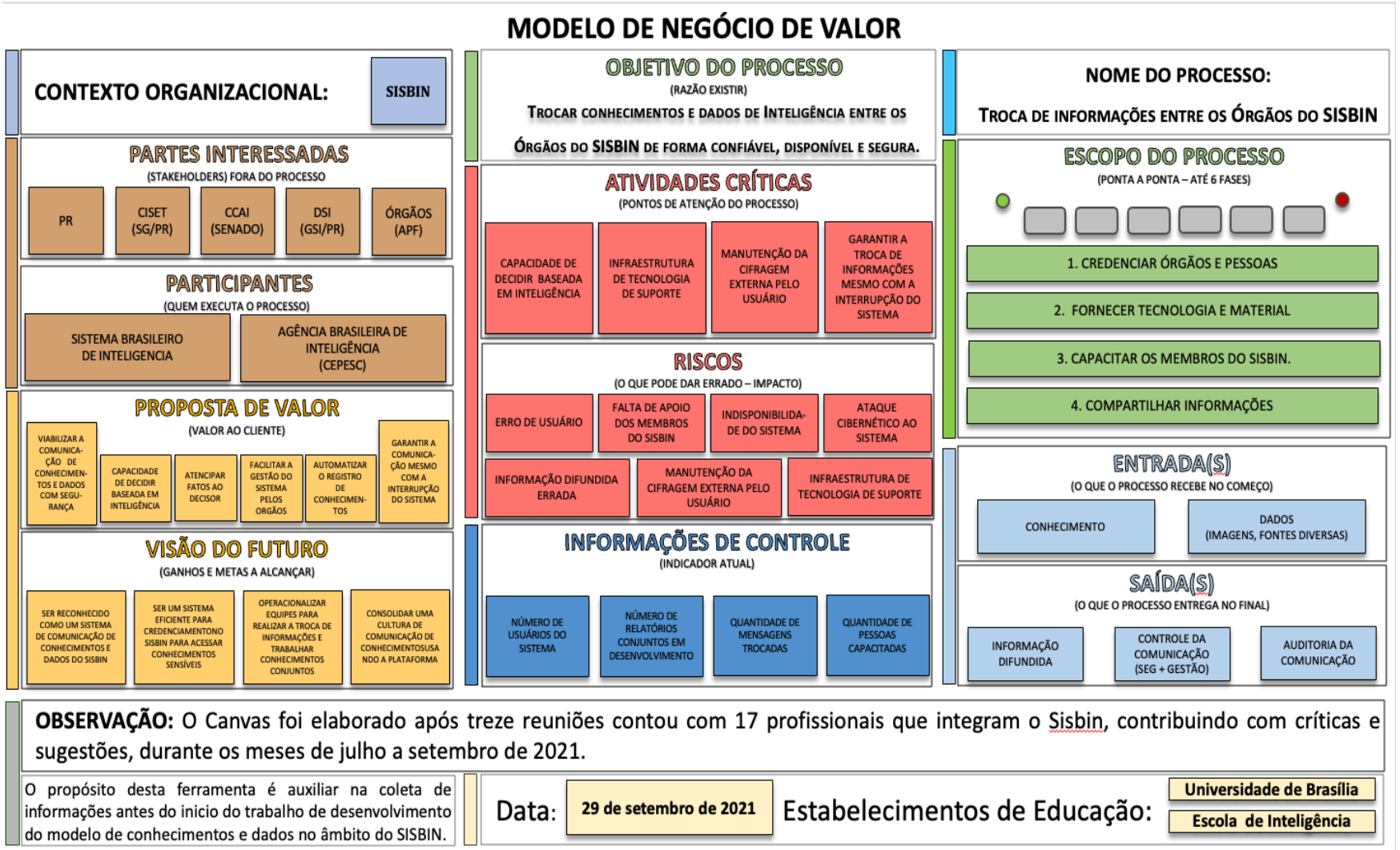

Figura 4.1: Modelo de negócio de valor
Fonte:O Autor

O escopo desse processo após as discussões entre os participantes abrangeu: o credenciamento de órgãos e pessoas; suporte tecnológico e empréstimo sob cautela de material; capacitação dos membros no uso do modelo proposto e a sistematização no compartilhamento de informações. Ressalta-se que inicialmente, na entrada, o processo receberá conhecimentos e dados, e em encerramento, na saída o processo proverá informação difundida, controle das comunicações e auditoria na comunicação, proporcionando segurança efetiva no trâmite de informações.

Após análise do modelo de negócio de valor passamos a elaborar uma pesquisa a ser aplicada nos utilizadores do sistema, com intuito de coletar opiniões e dados sobre o tema, porém integralmente restrita ao Sisbin.

Os resultados da pesquisa ratificaram o canvas sobre a necessidade de uma ferramenta atualizada para troca de conhecimentos e dados nos sinalizando que se faz necessária uma modernização tecnológica e que atualmente os critérios de disponibilidade e confiabilidade são os que foram mais relevantes sob o ponto de vista dos pesquisados.

Em seguida, foram elaboradas perguntas sobre a possibilidade de se produzir documentos conjuntamente na nuvem, onde a maioria dos respondentes reforçaram essa importância e que se faz fundamental a necessidade de produzir trabalhos conjuntos, em virtude das operações ocorrerem de forma integrada.

Também foram coletadas opiniões sobre a importância do controle e auditoria na atividade de inteligência, sendo destacado na pesquisa que a maioria ratifica o valor dessa temática e que menos da metade dos respondentes acreditam que a plataforma atual atende a essa necessidade, reforçando a premência de possibilitar aos órgãos de controle uma ferramenta de auditória no fluxo de mensagens.

Em continuidade, foram mensuradas a melhoria do assessoramento ao Chefe do executivo e automatização de registros, onde o resultado demonstra que quase a totalidade dos pesquisados concordam que a utilização da nuvem privada pode antecipar fatos ao decisor (Presidente da República), perfazendo uma proposta de valor para o Chefe do Executivo.

Ademais, o suporte centralizado e o baixo custo foram quantificados como fatores de impacto no estabelecimento de nuvem privada, onde concluiu-se que a maioria dos participantes concorda na centralização do suporte na Abin e na economicidade no uso da ferramenta.

Conclui-se parcialmente que foi primordial o desenvolvimento do Canvas, pois permitiu a compreensão do problema e eleger pontos críticos para o desenvolvimento de todo o processo, reforçando tópicos fundamentais no fluxo informacional, como assessoramento ao Chefe do Poder Executivo por meio de ferramentas que permitam a manutenção dos critérios de disponibilidade, integridade, confidencialidade e autenticidade. Além de reforçar pontos críticos que perpassam governos e se solidificam como ferramenta de estado, como a auditoria, controle dos meios utilizados, segurança e gestão da comunicação desde o início do processo até o encerramento, permitindo os órgãos judiciários e fiscalizadores atuar efetivamente no trânsito informacional, caso necessário.

4.2 ASPECTOS DO PROCESSO DE TROCA DE INFORMAÇÕES NO SISBIN

Os resultados sobre o processo de troca de informações de inteligência estão dispostos na Tabela 4.1. É praticamente unânime a concordância dos respondentes da necessidade de controle da segurança e da gestão do conhecimento, nesse processo (Questão 2.6). Também é possível verificar que a maioria dos respondentes relatam que a solução atual atende aos critérios de integridade, confidencialidade e autenticidade exigidos para troca de informações de inteligência (Questões 2.1 a, b e c). Contudo, aproximadamente metade dos respondentes mencionam que a solução atual não atende aos critérios de disponibilidade (Questão 2.1a).

Ademais, observa-se que a maioria relata que a solução atual não atende ao critério de oportunidade (Questão 2.5), o que permite concluir que há uma percepção de que a solução atual não é efetiva para compartilhamento de informações, apesar de que quando ela consegue estabelecer o fluxo informacional, faça atendendo a critérios de sigilo.

Ao questionar sobre possível solução utilizando nuvem privada, 74% responderam que concordam que essa solução atenderia à confidencialidade, integridade, autenticidade e disponibilidade. Isso reforça a importância do uso dessa ferramenta, porém também demonstra a indicação dos discordantes com a segurança dos conhecimentos e dados na nuvem, fortalecendo o gerenciamento de riscos e a adequação a normatização de requisitos mínimos para implementação da nuvem estabelecida pelo DSIC.

Importante destacar que o uso dessa solução viabilizaria a produção de trabalhos conjuntos inter órgãos e a edição conjunta de relatórios. Esses dois pontos tiveram concordância de mais de 90% dos respondentes (Questões 2.3 e 2.4).

O processo de troca atual de informações do Sisbin fortaleceram a ideia de que é necessário trabalhar em conjunto e em ambiente inter agências. Tal fato favorece o emprego de uma tecnologia que viabilize a elaboração e edição de relatórios conjuntos, confirmados nas questões constante na Tabela 4.1.

Em relação ao uso da computação em nuvem merece destaque a implementação de um meio seguro para trânsito de informações. Ainda foram reforçados aspectos de transposição complexa e o aumento exponencial da transformação digital, respaldando o emprego de *softwares* que garantam a segurança no fluxo informacional tanto no armazenamento como no transporte de dados.

Ainda de acordo com os respondentes, uma solução de nuvem privada fortalece o Sisbin (questões 2.9 e 2.11), permitindo gerar valor ao Presidente da República (questão 2.10) e ainda, eles reconhecem a percepção de liderança da Abin como importante na condução desse processo (questão 2.12).

Tabela 4.1: Respostas sobre os aspectos do processo de troca de informações

Afirmativas avaliadas sobre a comunicação sigilosa	**Concordam**	**Discordam**	**Não opinaram**	**Não concordo - Não discordo**
2.1 a) A troca de informações entre os órgãos vinculados ao Sisbin ocorre com rapidez, atendendo aos critérios de Disponibilidade.	51% (51)	49% (49)	10% (14)	17% (23)
2.1b) A troca de informações entre os órgãos vinculados ao Sisbin ocorre com rapidez, atendendo aos critérios de Integridade	85% (92)	15% (16)	12% (17)	9% (12)
2.1c) A troca de informações entre os órgãos vinculados ao Sisbin ocorre com rapidez, atendendo aos critérios de Confidencialidade	81% (88)	19% (21)	8% (11)	12% (17)
2.1d) A troca de informações entre os órgãos vinculados ao Sisbin ocorre com rapidez, atendendo aos critérios de Autenticidade.	87% (92)	13% (14)	11% (15)	12% (16)
2.2) A criação de uma nuvem privada no Sisbin atenderia à disponibilidade, a integridade, à confidencialidade, e a autenticidade.	74% (80)	26% (28)	4% (6)	17% (23)
2.3) A capacidade de produzir trabalhos conjuntos agilizaria a produção de documentos	91% (118)	9% (12)	1% (1)	4% (6)
2.4) A troca de informações com edição conjunta de relatórios traz vantagens ao Sisbin.	92% (117)	8% (10)	2% (3)	5% (7)
2.5 a) A plataforma atual atende ao critério de oportunidade.	38% (33)	63% (55)	24% (33)	12% (16)
2.5 b) A plataforma atual atende ao critério de imparcialidade.	76% (63)	24% (20)	28% (38)	12% (16)
2.6 O controle da segurança e a gestão dos conhecimentos são fundamentais para a comunicação.	98% (131)	2% (2)	0% (0)	3% (4)
2.7 A plataforma atual atende aos critérios de possível auditoria.	65% (35)	35% (19)	42% (57)	19% (26)
2.8 A nuvem privada produz trilhas de auditoria na comunicação de conhecimentos e dados.	93% (113)	7% (8)	6% (8)	6% (8)
2.9 A adoção de nuvem privada de fácil acesso fomentaria o aumento da integração no Sisbin.	91% (116)	9% (12)	1% (2)	5% (7)
2.10 A antecipação de fatos ao Presidente da República por meio da nuvem privada condiz um valor.	88% (105)	12% (14)	2% (3)	11% (15)
2.11 A nuvem privada capaz de automatizar o registro de conhecimentos fortalece o Sisbin.	93% (112)	7% (9)	2% (3)	2% (3)
2.12 O suporte tecnológico centralizado pela Abin no Sisbin gera continuidade na comunicação.	89% (91)	11% (11)	11% (3)	15% (13)

4.3 RESPOSTAS DA PESQUISA SOBRE A LEI DE ACESSO À INFORMAÇÃO

A Tabela 4.2 apresenta o resultado das questões relacionadas à LAI, tais como a informações sigilosas não classificadas, o uso da criptografia de estado e a importância dos postos de controle para tratamento das informações sigilosas.

Tabela 4.2: Respostas relacionadas sobre a Lei de Acesso à Informação

Afirmativas avaliadas sobre a LAI	**Concordam**	**Discordam**	**Não opinaram**	**Não concordo - Não discordo**
3.1 A proteção no fluxo das informações sigilosas não classificadas, mesmo sem possuírem amparo legal previsto na LAI, são fundamentais.	98% (130)	2% (2)	2% (1)	3% (4)
3.2 As ferramentas utilizadas para a troca de conhecimentos sigilosos não classificados atendem as necessidades de agilidade atual.	47% (36)	53% (40)	25% (34)	20% (27)
3.3 O uso de criptografia de estado somente para informações classificadas conforme a LAI atende aos critérios de segurança no Sisbin.	51% (49)	49% (47)	9% (28)	20% (13)
3.4. a) A criação de postos de controle no tratamento das informações sigilosas potencializa o uso da nuvem privada, gerando agilidade.	85% (99)	15% (17)	5% (7)	10% (14)
3.4 b) A criação de postos de controle no tratamento das informações sigilosas potencializa o uso da nuvem privada, gerando segurança.	83% (88)	17% (18)	6% (23)	17% (8)
3.4 c) A criação de postos de controle no tratamento das informações sigilosas potencializa o uso da nuvem privada, gerando oportunidade.	89% (104)	11% (13)	7% (7)	8% (15)

Mesmo sem possuírem amparo legal previsto na LAI, a proteção no fluxo das informações sigilosas, não classificadas, se materializa como fundamental para a maioria dos entrevistados no processo de segurança no fluxo de informações (Questão 3.1). Importante ressaltar que as informações sigilosas, que não possuírem hipótese de sigilo fundamentada em lei, tem sua confidencialidade baseada no princípio da razoabilidade, gerando grande vulnerabilidade na divulgação da informação sensível, conforme o Art. 31 da LAI.

Merecendo igual destaque, a informação sobre as ferramentas utilizadas para a troca de conhecimentos sigilosos não classificados, onde em grande parte dos respondentes mostrou um equilíbrio de opiniões (Questões 3.2 e 3.3), fortalecendo a ideia da falta de sensibilização de usuários e formação de opinião. De forma semelhante, a questão sobre o aumento da sensibilização, habilitação e criação de postos de controle no tratamento das informações sigilosas foi apreciada como meio de potencializar o uso da nuvem privada, ratificando a importância desse modelo.

Também foi mensurada a importância da criação de postos de controle no tratamento de informações sigilosas, onde os resultados (Questões 3.4 a, b e c) mostraram que a maioria dos respondentes concordam que as fiscalizações do fluxo de informações promovem agilidade, segurança e oportunidade.

Os principais aspectos a serem discutidos relacionados a LAI neste trabalho, permitem avaliar como fundamental a previsão de amparo legal para proteger as informações sigilosas, conforme a Tabela 4.2

apresenta, e a adoção de tecnologias que garantam a segurança e a proteção dos dados trafegados e armazenados, atualmente possibilitados por softwares de código aberto que podem ser implementados em testes como uma solução disponível no mercado.

Conclui-se parcialmente que, a proteção no fluxo das informações sigilosas não classificadas, mesmo sem possuírem amparo legal previsto na LAI se materializa como fundamental para a maioria dos entrevistados no processo de segurança no fluxo de informações. Importante ressaltar que as informações sigilosas que não possuírem hipótese de sigilo fundamentada em lei, tem sua confidencialidade baseada no princípio da razoabilidade, gerando grande vulnerabilidade na divulgação da informação sensível. Merecendo igual destaque a informação sobre as ferramentas utilizadas para a troca de conhecimentos sigilosos não classificados, onde visualiza-se em grande parte um equilíbrio de opiniões, pois as amostras foram bem equânimes, fortalecendo a ideia da falta de sensibilização de usuários e formação de opinião dos usuários.

4.4 RESPOSTAS DA PESQUISA SOBRE ASSUNTOS INTER-RELACIONADOS

A Tabela 4.3 apresenta perguntas inter-relacionadas sobre a nuvem privada, LAI e Norma Complementar Nr 14 - R01 - Segurança da Informação em Nuvem (Brasil, 2018). Os resultados confirmam que a manutenção do fluxo de troca de conhecimentos e dados entre os órgãos do sistema são fundamentais ao assessoramento baseado em inteligência, (Questão 4.1), e a liderança da Abin na condução do processo (questão 4.3). Também há concordância de que é necessário que a alta administração dos órgãos do Sisbin se aproprie da Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) para definir o emprego da tecnologia da nuvem (Questão 4.2).

Tabela 4.3: Respostas sobre assuntos inter-relacionados

Afirmativas avaliadas sobre questões interrelacionadas	**Concordam**	**Discordam**	**Não opinaram**	**Não concordo - Não discordo**
4.1) O fluxo de troca de conhecimentos e dados entre os órgãos do sistema são fundamentais ao assessoramento baseado em inteligência.	97% (131)	3% (2)	0% (0)	3% (4)
4.2) A alta administração deve considerar a GRSIC para usar a nuvem.	98% (129)	2% (2)	1% (1)	4% (5)
3.3 4.3) A Abin, como órgão central do Sisbin, deve ser a provedora da nuvem privada, baseando o servidor em área sob sua responsabilidade.	90% (104)	10% (11)	5% (15)	11% (17)

Esses pontos permitem uma análise em conjunto dos normativos já disponíveis e suas adequações necessárias no âmbito legal, assim como no campo tecnológico, favorecendo o assessoramento em alto nível por meio de uma ferramenta adequada.

Conclui-se, parcialmente, que a manutenção do fluxo de troca de conhecimentos e dados entre os órgãos do sistema é fundamental ao assessoramento baseado em inteligência, resultando na contabilização da maioria dos pesquisados confirmando a importância do fluxo de dados em meio eficiente e oportuno.

Assim, nesse escopo, a maioria dos pesquisados avalia que o uso de criptografia de estado somente para informações classificadas conforme a LAI atende aos critérios de segurança para o fluxo de informações no Sisbin. De forma semelhante, a questão sobre o aumento da sensibilização, habilitação e criação de postos de controle no tratamento das informações sigilosas foi apreciada como meio de potencializar o uso da nuvem privada ratificando a importância desse modelo.

Por fim, a pergunta foi direcionada para a alta administração dos órgãos, visando checar a efetividade da GRSIC como capaz de definir o emprego da tecnologia da nuvem, resultando na maioria dos consultados concordando com o normativo sobre segurança da informação em nuvem, elaborado pelo DSIC. Também foi apreciada a situação da Abin, como órgão central do Sisbin, sendo a responsável pelo provimento do acesso à nuvem e pela guarda dos servidores, o que levou a maioria dos respondentes a concordarem com a afirmação.

4.5 RESPOSTAS DA PESQUISA SOBRE AS PERGUNTAS ABERTAS

Os respondentes tiveram a possibilidade de opinar em duas questões abertas: na primeira, foi perguntado se os respondentes teriam sugestões quanto ao modelo de uso de nuvem privada na troca de informações de inteligência; e a segunda, com relação às sugestões que pudessem fortalecer o processo, a interação e a troca conhecimentos entre os órgãos do Sisbin. Foram recebidas 33 respostas para a primeira questão, e 23 para a segunda.

As ideias apresentadas potencializam a adoção de uma ferramenta que possibilite trabalhos coordenados, criando embasamento para argumentos já estudados durante o desenvolvimento do trabalho, desde que a implementação da ferramenta tecnológica seja segura e possibilite a impulsão do processo de comunicação sigilosa não classificada de forma eficaz entre órgãos.

As perguntas estão citadas no Quadro 3.4 e suas respostas estão contidas nos Quadros 4.1 e 4.2, que seguem abaixo, sendo designadas conforme o número do respondente da pesquisa, como já citado nas considerações sobre os respondentes na Seção 3.2 deste trabalho.

De uma forma geral, as ideias apresentadas reforçam argumentos já estudados durante o desenvolvimento do trabalho, dando maior credibilidade para uma efetiva integração, potencializada por intermédio de uma ferramenta tecnológica que facilite o processo de comunicação sigilosa entre órgãos. Além de trazer novas ideias para desenvolvimento em artigos futuros com maior nível de profundidade teórica.

4.6 PROPOSTA DE NUVEM PRIVADA

A proposta da nuvem privada pode ser implementada por uma solução baseada em compartilhamento de dados que permitem aos usuários acessar remotamente os arquivos armazenados em nuvem privada

Quadro 4.1: Principais respostas abertas sobre otimização do modelo atual

Respondente	**Principais ideias**
R05	Observar os princípios relacionados com o modelo de *cloud* proposto pela VMWare.
R07	Sugiro o estudo da ferramenta NextCloud.
R35	O caminho natural da troca de informações entre Órgão do Sisbin seja a adoção das tecnologias de ponta, como por exemplo a nuvem privada, com protocolo de segurança.
R36	A adoção de criptografia de estado para informação não classificada é cabível, desde que ocorra a compartimentação/disciplina entre os canais de transmissão.
R37	Aumentar estudos sobre o controle de acessos secundários e como são registrados.
R48	Tal solução seria viável em rede isolada da Internet (VPN).
R66	A nuvem privada oferece riscos para informação sigilosa. Centralizar informações a torna alvo compensador. Isso pode ser feito, mas todos os riscos devem ser tomados em conta.
R73	A ideia é ótima, desde que garantida a segurança e o sigilo da informação, seja ela classificada ou não, bem como critérios rigorosos de acesso ao conhecimento e auditoria.
R89	Sugiro que olhe o art. 17 da nova IN do GSI/PR que trata de nuvem, IN nº 5 GSI/PR, de 31/08/2021, disponível em: www.gov.br/GSI/pt-br/assuntos/DSI/legislação.
R95	A implementação de um serviço dessa natureza deve ser precedida de estudos, desenvolvimento de mentalidade de contra-inteligência dos gestores de rede e nos usuários finais.
R97	A mobilidade dos recursos humanos de TI também é um desafio a se considerar. Existe a real e urgente necessidade de integração entre os órgãos do Sisbin.
R100	A tecnologia de nuvem requer um desenvolvimento elástico, o que significa a permanente possibilidade de agregar inovações tecnológicas e adequar-se a novas condições impostas.
R103	A governança aplicada às novas tecnologias e doutrinas permite aprimorar sistemas baseados em tecnologias de nuvem, tornando-o ágil, eficiente e capaz de sustentar ações.
R 105	O acesso à nuvem deverá conter mecanismos de rastreio de atividades assim como níveis diferentes de acesso. Há que se medir impactos de um possível vazamento de dados.
R108	O armazenamento de dados sigilosos em sistemas computacionais suscita elevada necessidade de controle nas fases de produção e de difusão das informações.
R 121	Um órgão faz um convênio bilateral com outro, e ambos disponibilizam seu banco de dados, porém nenhum dos órgãos tem acesso ao que o outro está consultando.
R 137	A auditoria, é estabelecida de forma conjunta com representantes de ambos os órgãos e apenas para a finalidade que a ensejou.

Fonte: Autor (2022, p. 13)

alocada em órgão a ser designado, atendendo aos critérios de segurança, disponibilidade e fácil acesso, por meio da proposta de implantação sugerida preliminarmente por [65] um trabalho relacionado.

4.6.1 Processo de acreditação de pessoa ou órgão no Sisbin

O processo de troca de mensagens sigilosas se inicia pelo cadastramento de pessoa ou órgão pela entidade responsável pela acreditação. Após a emissão de *token* e pelo fornecimento de credencial pelo órgão responsável. Ao invés de dar um certificado de acesso à informação sensível, a proposta será emitir um *token* com certificado secreto para acessar as informações. O *token* para acesso ao sistema de informações em nuvem privada é concedido de acordo com a emissão de credenciais e uma chave de acesso, conforme o descrito na Figura 4.2.

A informação no banco de dados estará privada sendo cifrada e decifrada somente para quem tem direito. Só o sistema que gerencia os arquivos permaneceria aberto.

Quadro 4.2: Consolidação das respostas sobre integração no Sisbin

Respondente	Respostas
R05	Identificar outros trabalhos no sistema de inteligência que eventualmente demonstrem o bom funcionamento de iniciativas de cloud.
R07	Faltam legislação, normativos que regulem o compartilhamento de dados no Sisbin. O STF por meio da ADI 6529 deu uma regulada nisso, mas o cenário é ainda mais complexo.
R35	Para análise de dados é importantíssimo a união de várias fontes que respaldem o informe até que vire informação.
R37	Essas trocas de informações, se padronizadas e confiáveis, afastando vaidades juvenis aumentariam sobremaneira a eficácia e eficiência dos nossos trabalhos de inteligência.
R48	Em que pese a tecnologia seja fundamental para dar maior oportunidade para os conhecimentos, a relação pessoal de confiança é que pode fomentar o compartilhamento de dados.
R54	Uso de wikis restritas aos analistas de cada projeto de produção conjunta.
R66	Acho importante expandir o conhecimento por meio de palestras aos parceiros do Sisbin sobre a interação de assuntos sensíveis na nuvem.
R73	Seria interessante agregar outros elementos procedimentais e tecnológicos para aumentar a segurança. A exemplo do uso de VPN para o acesso e uso em dispositivo móvel.
R89	O SIEx utiliza uma ferramenta bastante eficiente para a troca de mensagens e arquivos sigilosos não classificados (UNA). Também o Sistema SCADI Hermes, centralizando informações.
R95	Primeiro, devemos nos certificar de quem irá ter acesso aos bancos de dados.
R96	A utilização da logomarca do Sisbin nos documentos de Inteligência, substituindo a logo dos órgãos, sedimentaria mais rapidamente a ideia de colaboração.
R100	Realização de trabalho conjuntos.
R105	Treinamento e formação de equipe integrada de "pontos focais"nos vários órgãos também contribuiria para facilitar a adesão de todas as partes.
R108	Os órgãos que compõem o Sisbin devem ser nivelados nas questões relacionadas à área dedicada à Inteligência, tecnologia (hardware e software) modernos e confiáveis, e usuários capacitados em técnicas, atitudes e comportamentos adequados.
R111	Nos casos de políticas de natureza transversal, é essencial que haja mecanismos institucionalizados de coordenação, de forma a criar condições para a atuação conjunta e sinérgica, evitando ainda superposições ou esforços contraproducentes.
R123	Credenciamento de segurança de cada órgão integrante do Sisbin visando à proteção do conhecimento, capacitando os técnicos e os gestores.
R137	Necessidade de especialistas bastante capacitados para gerir incidentes e mitigar danos provocados por eventuais vazamentos ou acesso indevido nas bases de dados.

Fonte: Autor (2022, p. 13)

A seguir, partindo do pressuposto que as credenciais foram emitidas. Os integrantes do Sisbin se ligam a VPN [82], utilizando um fator duplo de autenticação, baseado em certificação digital e um *token* criptográfico, controlado pela Abin. Para tanto, o Duplo Fator de autenticação geralmente utilizado em *pen drive* contendo certificação digital, pode ser validado:

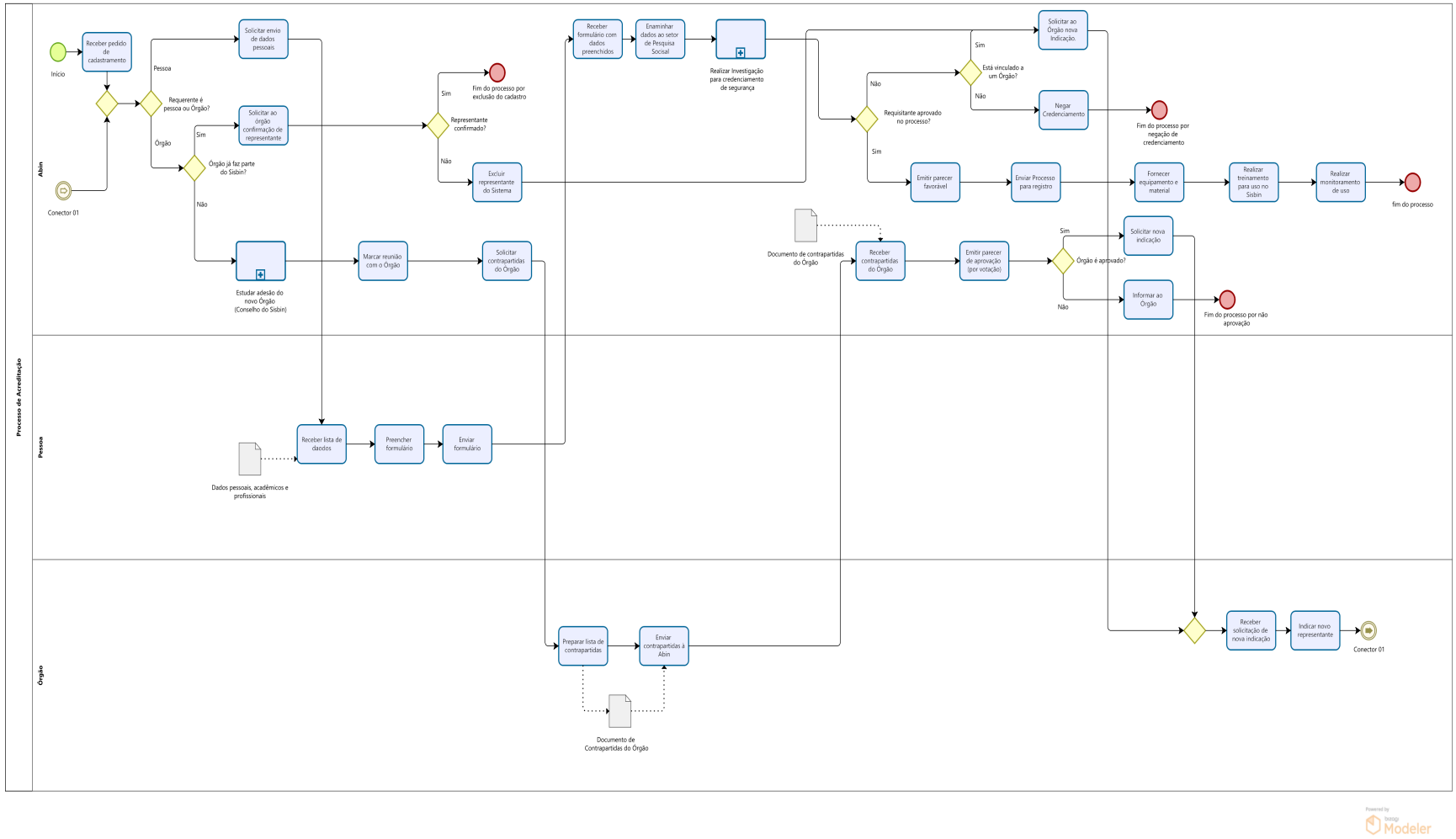

Figura 4.2: Acreditação de órgãos e pessoas no Sisbin
Fonte:O Autor

1. Via texto (chave): Ao realizar o login de acesso, chegará em seu número de telefone uma mensagem ou ligação, contendo o *token* de acesso. Assim, ao inserir este código, conseguirá login com segurança.

2. Confirmação por e-mail ou telefone, forma bastante conhecida. Assim, logo após o acesso, um e-mail será enviado a você. Como resultado deste e-mail, haverá um código ou um link para confirmação de acesso.

3. Pergunta secreta: Desta forma, assim que realizar acesso. Será necessário responder uma pergunta pré-estabelecida anteriormente, ao ser entregue uma chave. Assim, a resposta a está pergunta é a mesma que usou no momento da criação da autenticação dupla.

Após, encerrado o processo de acreditação e o *login* estar acessível, a informação sensível faz o *download* e só depois decifra para o acesso. Mesmo as informações sensíveis estarão cifradas com criptografia própria do nextcloud, padrão Advanced Encryption Standard (AES) e Rivest-Shamir-Adleman (RSA).

4.6.2 Topologia da Arquitetura Lógica de Referência

Diante disso, a partir da Figura 4.3, pode-se observar que os requisitos do sistema de segurança dos dados de fim-a-fim, com alta disponibilidade dos serviços e abstração de hardware, de maneira a possibilitar a implantação dessa solução em qualquer hardware padrão de data center, independente do fornecedor. Onde os data centers contêm servidores físicos ou virtuais conectados interna e externamente por meio de equipamentos de comunicação e sistema de rede para armazenar, transferir e acessar informações digitais. Cada servidor tem um processador, espaço de armazenamento e memória, assim como um computador pessoal, porém mais potente. Os data centers usam software para agrupar os servidores e distribuir a carga de trabalho entre eles.

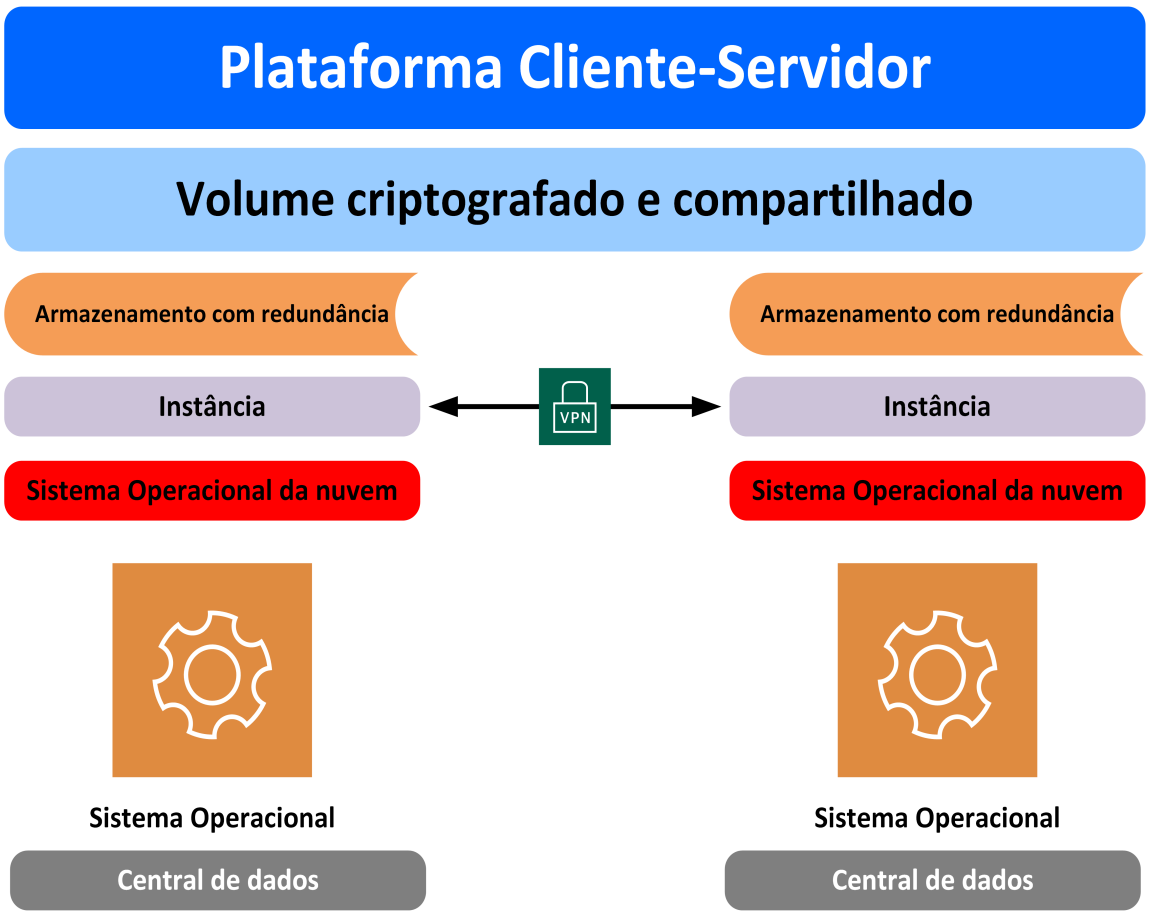

Figura 4.3: Topologia proposta lógica para o Sisbin
Fonte:O Autor

Assim, a proposta de implementação da nuvem privada desenvolvida preliminarmente por [65], propõe recursos de hardware alocados e uma solução de virtualização aberta instalada e customizada neste hardware [83]. Com essa estrutura, propõe-se uma infraestrutura virtual necessária para a solução de compartilhamento de arquivos. A infraestrutura virtual proposta foi uma solução de armazenamento distribuído a ser implementada, usando a melhor tecnologia disponível, preferencialmente de código aberto.

Com relação as condições de replicação de dados [84], as configurações particulares de armazenamento com redundância, foram definidas para disponibilidade. A segurança dos dados na transferência (VPN) e em repouso também foram garantidas por critérios de criptografia, tanto no transporte dos dados quanto em armazenamento. Um serviço de compartilhamento de arquivos foi, então, proposto. Com um portal *front-end* amigável, onde se desenvolve a aplicação na qual o usuário irá interagir diretamente, seja em softwares, sites e aplicativos, estando disponível na Internet para uso dos colaboradores que tenham acesso. Os passos para implementação de tal infraestrutura são discutidos mais adiante nesta seção. A Figura 4.3 apresenta a arquitetura lógica no âmbito do Sisbin.

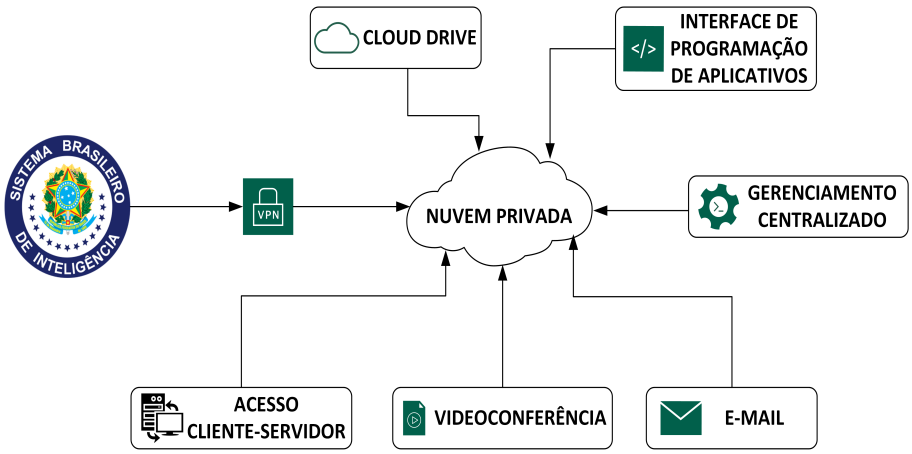

Figura 4.4: Arquitetura lógica proposta no Sisbin
Fonte:O Autor

4.6.3 Arquitetura Física de Referência Proposta

A Arquitetura Física de Referência proposta baseia-se no ambiente sugerido preliminarmente em [65] foi desenvolvido um ambiente de centro de dados distribuído e seguro, garantindo que os dados serão armazenados e transmitidos com criptografia, garantindo o sigilo e autenticidade das informações fim-a-fim. Os dados dos usuários serão transmitidos entre as instâncias utilizando tuneis VPN [85] e a alta disponibilidade é garantida pela possibilidade de replicação de DC conforme a disponibilidade de ambientes.

A proposta sugere na realização de futuros testes a utilização de apenas dois centros de dados, porém este sistema pode ser escalado para até centenas de servidores. A capacidade de garantir o sigilo nos dados transmitidos e armazenados e a alta disponibilidade facilita o trabalho remoto, pois os usuários poderão acessar os dados em qualquer lugar com Internet. Os componentes utilizados para permitir o funcionamento do modelo proposto são apresentados na Figura 4.5.

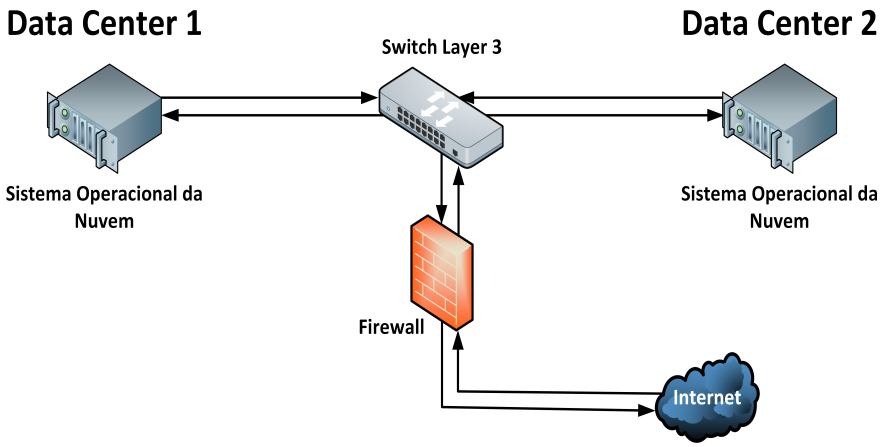

Figura 4.5: Topologia física proposta
Fonte:O Autor

A solução proposta para o armazenamento de arquivos altamente disponível, prevê uma infraestrutura física de base. Para isso, dois servidores físicos, interconectados por um switch 1GbE de camada 3 foram observados em trabalhos correlatos como ilustra a Figura 4.5

A comunicação entre servidores pelo switch simula satisfatoriamente a comunicação entre dois centros de dados dispersos geograficamente, já que o problema é reduzido a roteamento e banda disponível. Assim, nesta estrutura, cada servidor físico será logicamente referenciado como Data Center 1 (DC1) e Data Center 2 (DC2).

4.6.4 O emprego do Sistema Operacional da Nuvem

O Sistema Operacional da Nuvem é uma plataforma que controla recursos de computação, armazenamento e emulação de redes em um ou vários data centers, controlados por meio de um painel com interface administrativa, que permite o controle administrativo dos recursos e dos usuários, permitindo, assim, o provisionamento de recursos em um modelo de IaaS. Também é o responsável por virtualizar o hardware e abstrair os componentes físicos, permitindo a implementação de um SDDC [86], e roda sobre um sistema operacional, agindo, por definição, como um hypervisor tipo 2 (também conhecido como hypervisor convidado).

Após a instalação do Sistema Operacional da Nuvem, obtém-se uma agregação de recursos virtualizados dos dois servidores físicos em uma única console (conhecido como *Horizon dashboard*). Nesse ponto, o administrador do SDDC pode provisionar rede virtual, máquinas de computação virtual (conhecidas no mundo VMware como *Virtual Machines* e, neste contexto, como instâncias) e recursos de armazenamento no DC1 ou DC2.

Vale ressaltar que foram referenciadas propostas de trabalhos correlatos, porém não foram mencionadas as suas implementações, pois estas podem variar com o aparecimento de novas tecnologias. Duas das instâncias foram alocadas ao DC1 e a terceira instância ao DC2, caracterizando distribuição na CC.

4.6.5 Infraestrutura de armazenamento distribuído

A solução de armazenamento distribuído proposta possibilitará armazenamento redundante e escalonável de dados por meio de clusters ou instâncias de servidor [87]. Além de funcionar como um serviço em cima de instâncias de computação.

Outra questão é a proteção dos dados no volume compartilhado. Primeiro, políticas são criadas para que apenas IP permitidos possam ingressar no pool do cluster e apenas o serviço desejável tenha permissão para montar e fazer uso do volume compartilhado. Além disso, o armazenamento distribuído deve ser implementado com a opção de criptografia de dados.

4.6.6 Túnel seguro com VPN

A interface virtual de túnel [88], baseia-se em um princípio fundamental proposto de túneis seguros, uma associação entre o par chave pública e o endereço IP de origem do túnel. Usa-se uma única troca de chaves de ida e volta, e lida com toda criação de sessões de forma transparente para o usuário.

Propõe se que, ao enviar pacotes encapsulados criptografados, um *handshake* de troca de chaves deve ocorrer primeiro. Após essa troca de comunicação entre as máquinas do emissor e do destinatário, o emissor pode encaminhar mensagens criptografadas usando um par compartilhado de chaves simétricas, uma para enviar e outra para receber. Seguidamente a primeira mensagem criptografa do emissor para o destinatário, o destinatário pode começar a enviar mensagens criptografadas para o emissor.

Nesse contexto, um túnel VPN foi configurado entre as três instancias criadas pelo Sistema Operacional da nuvem e utilizadas pelo armazenamento distribuído. Como a VPN foi implementada nas instâncias virtuais, os pacotes saem das instâncias pela interface virtual criada pelo túnel da VPN já cifrados, não ficando disponíveis para leitura nem pelo sistema operacional da nuvem, nem pelo sistema operacional da máquina física onde está instalado, impossibilitando a leitura pelo administrador da nuvem.

4.6.7 A nuvem do usuário final

Na fase final da proposta, um portal de Internet é necessário para a interação dos usuários com o *storage* para compartilhamento de arquivos [89]. Por ser uma plataforma cliente-servidor para compartilhamento de arquivos, sendo o lado do cliente do aplicativo cliente-servidor muito semelhante ao Dropbox ou Google Drive, onde usuários registrados podem enviar seus arquivos pessoais para a nuvem, através de um aplicativo móvel ou um navegador da web [83]. Do lado do servidor, a infraestrutura existente no ambiente onde o cliente-servidor está instalado é usada para o armazenamento que a ferramenta fornece.

O volume compartilhado é montado nos sistemas de arquivos da instância. O próximo passo é proteger a conexão entre o navegador da web do cliente e o servidor usando o protocolo HTTPS.

Diante disso, qualquer usuário que acessar via cliente-servidor e armazenar seus dados “na nuvem” se beneficiará da infraestrutura segura e distribuída.

4.6.8 Referência para Garantia de Segurança

A segurança de dados é um tema importante e sensível em toda a ambiente corporativo. Os governos em todo o mundo estão legislando severamente sobre isso, por exemplo, a Regulamento Geral sobre a Proteção de Dados, na Europa, e a própria Lei Geral de Proteção dos Dados, no Brasil.

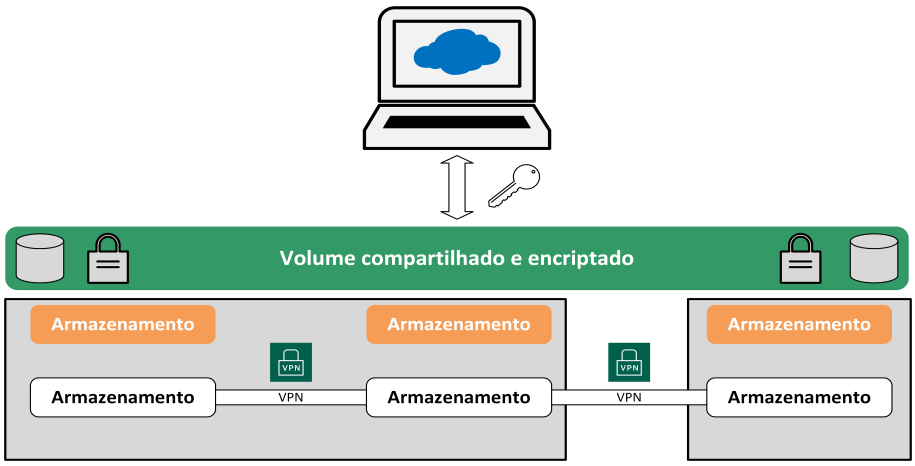

Figura 4.6: Topologia de segurança lógica para o ambiente distribuído.
Fonte:o Autor

A solução implementada e descrita neste artigo trata, fim-a-fim, da segurança de dados no ambiente virtualizado e distribuído proposto. A figura 4.6 ilustra o detalhe da proposta e os tópicos a seguir resumem os aspectos de segurança envolvidos, conforme [65]:

> • Segurança do dado em transporte: Como a solução proposta sugere replicação de dados entre data centers geograficamente distribuídos, foi necessário cuidado com a confidencialidade desses dados cruzando redes públicas e até mesmo a Internet. Para isso, foi criado um túnel VPN, com o software WireGuard, entre todas as instâncias GlusterFS que servem ao gluster volume compartilhado. Este túnel VPN garante que apenas o destinatário possa interpretar os bits de forma inteligível, salvaguardando assim o conteúdo da mensagem na transmissão entre servidores.
> • Proteção de dados em repouso: O conceito fundamental de segurança está altamente relacionado à maneira como os dados são armazenados. O armazenamento criptografado é a garantia de que os dados ficarão ilegíveis para um usuário que não possui as permissões necessárias (um possível invasor). Em particular, a encriptação dos dados é garantida pela encriptação que o GlusterFS oferece aos dados dos seus volumes, só sendo possível utilizar o volume compartilhado endpoints na faixa de IP permitidos e se em posse da chave atribuída na encriptação.
> • Conexão segura cliente-servidor: Uma vez garantida a segurança dos dados na transferência (através do túnel VPN com WireGuard) e em repouso (através de volumes criptografados com GlusterFS), a próxima e última falha de segurança a ser tratada foi a garantia de uma conexão segura entre os usuários e o serviço NextCloud. Como o NextCloud é implementado por meio de uma interface da web, foi usada uma camada adicional de segurança com SSL/TLS sobre protocolo HTTP. Essa camada permite que os dados sejam transmitidos, por meio de uma conexão criptografada, para o servidor web e, a partir daí, para os volumes criptografados compartilhados.

Assim, conforme a Figura 4.7 Exemplificação da garantia de segurança, a proposta apresentada atende aos requisitos de disponibilidade, segurança e fácil acesso e necessita de testes com informações sensíveis não classificadas para validar o sistema e treinar os usuários.

Vale ressaltar que apesar da referência mencionar as aplicações utilizadas nos testes implementados, a intenção desse trabalho é reforçar os requisitos para serem adaptados à melhor tecnologia no momento em que a solução for operacionalizada.

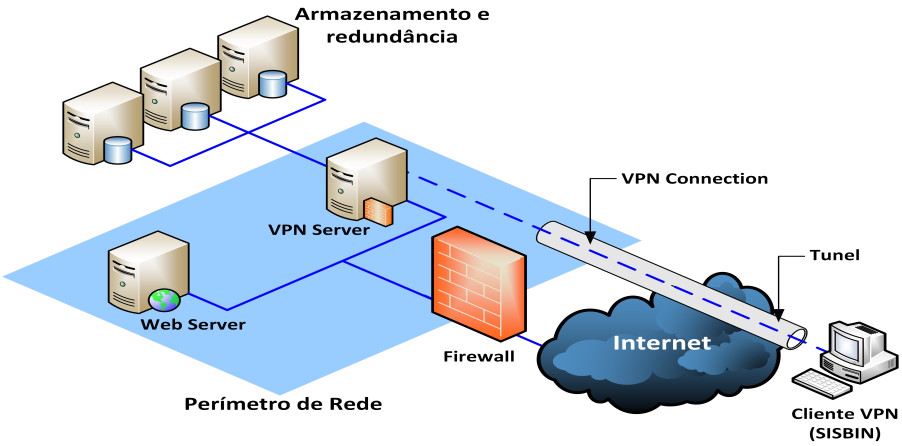

Figura 4.7: Exemplificação da garantia de segurança
Fonte:o Autor

4.7 SÍNTESE DOS RESULTADOS E DISCUSSÕES

Percebe-se que após análise dos dados obtidos, existe a necessidade de otimização da ferramenta atual utilizada na comunicação sigilosa entre os órgãos do Sisbin.

O modelo de negócio de valor – Canvas permitiu mapear o objetivo do processo fundamental para o funcionamento da comunicação sigilosa, bem como levantar indicadores, contexto inserido, partes interessadas, participantes, proposta de valor, visão de futuro, atividades críticas, riscos envolvidos, informações de controle e o desenvolvimento do processo como um todo, permitindo a manutenção do foco durante a pesquisa na cadeia de valor do processo.

Com relação ao uso da ferramenta atual para troca de informações foi observado que não atende de forma eficiente ao critério de disponibilidade. Ao ser posta a hipótese de uma nuvem privada para compartilhamento de dados foi levantado que atenderia aos critérios de disponibilidade, integridade, confidencialidade e autenticidade, possibilitando a necessidade de trabalhos conjuntos. Igualmente fortalecendo a ideia de atendimento a oportunidade e imparcialidade promovida pela integração de fontes e pela agilidade proporcionada pelo ambiente de nuvem.

Destaca-se a relevância do tratamento dos riscos associados, o controle, a gestão e auditoria da plataforma para assegurar a segurança da informação, sendo reforçadas durante toda a pesquisa.

Também foi evidenciada a relação ao baixo custo da computação em nuvem privada, reforçando aspectos de aumento de servidores e utilização de programas baseados em códigos abertos, fortalecendo a elasticidade, tendo como alicerce o suporte centralizado na Abin.

Outrossim, a LAI também foi analisada como não contemplando a comunicação sigilosa no que tange a assuntos sensíveis não classificados, a fundamentação baseada na razoabilidade sem hipótese de sigilo que

garanta seu secretismo trouxe questionamentos para a necessidade de revisão ou normatização específica para assegurar interesses do Estado Brasileiro. Também ficou caracterizada na pesquisa a importância da sensibilização, credenciamento e aumento de postos de classificação de documentos sigilosos.

Ainda foi fortalecida a governança devendo permear todo o processo de comunicação sigilosa, precisando avaliar nas organizações federais sob sua responsabilidade a GRSIC e sendo reforçada para a maioria dos respondentes que na hipótese de da utilização da nuvem privada está deve estar alocada na Abin.

Em síntese, os resultados demonstraram a necessidade de otimização da ferramenta usada na troca de conhecimentos sigilosos.

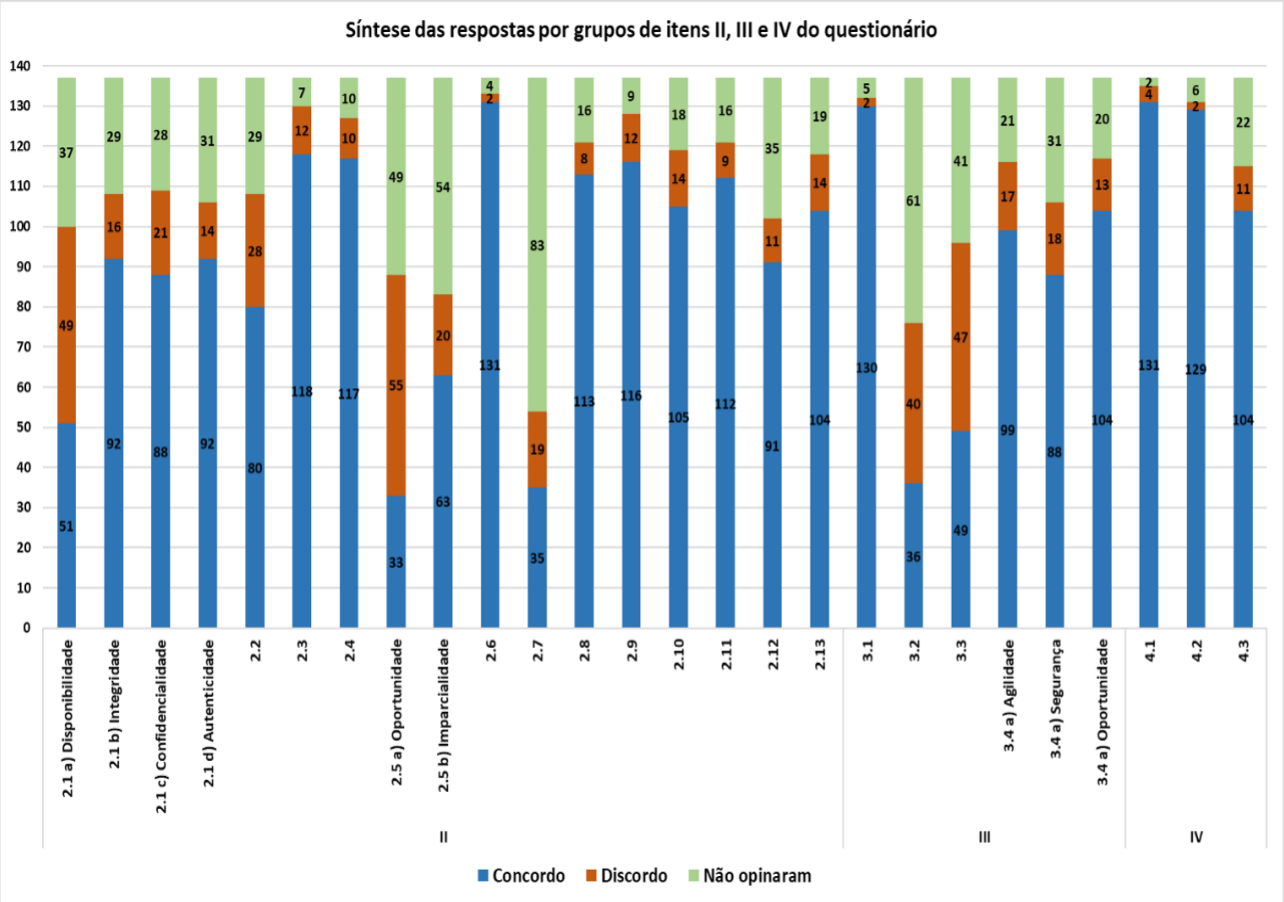

Figura 4.8: Síntese da tabulação da pesquisa aplicada no Sisbin
Fonte:Autores (2022, p. 23)

5 CONSIDERAÇÕES FINAIS

Essa dissertação teve por objetivo propor procedimentos e uma arquitetura de referência para a otimização do processo de comunicação sigilosa entre os órgãos do Sistema Brasileiro de Inteligência (Sisbin) com a indicação da computação em nuvem privada, inicialmente direcionada a mensagens não classificadas entre os órgãos do sistema, visando agilizar, garantir e assegurar a troca de informações.

A adoção da nuvem privada é favorecida por reforçar parâmetros como: ser de baixo custo, fácil acesso, disponível e segura. Porém, foram bem argumentadas opiniões nas respostas abertas que ressaltaram ao mantenedor e ao fornecedor da nuvem critérios de segurança da informação, como a disponibilidade, integridade, autenticidade e confiabilidade, garantindo seu funcionamento, além de cláusulas contratuais específicas que assegurem essa integração entre órgãos e serviços, atualmente já parcialmente estabelecidas no conselho consultivo do Sisbin e já bem delineadas no recente normativo sobre nuvem.

Em síntese, esse trabalho indicou a necessidade de atualização de uma ferramenta para troca de informações entre os órgãos, com a possibilidade de realizar documentos, apreciações e estimativas de forma conjunta. Também trouxe a computação em nuvem privada como uma solução, fortalecendo critérios fundamentais de segurança cibernética, como os servidores estarem sob a guarda do órgão central do sistema, assim como o suporte tecnológico também ser fornecido pela Abin, como fatores de risco de grande impacto na segurança dos dados no ambiente da computação em nuvem.

A criação de uma fundamentação legal para tratar a informação sensível de inteligência foi observada como um desafio, pois atualmente não há previsões jurídicas objetivas na LAI que abordem essa questão.

O desenvolvimento de protocolos para fluxo de informações sigilosas não classificadas, o treinamento e formação de equipes integradas, com pontos focais dos órgãos integrados ao Departamento de Segurança da Informação também foram fortalecidos como oportunidades significativas no processo.

O compartilhamento de dados para fins de AI no Sisbin tem previsão legal – ainda que genérica – na lei que o criou e na ENINT, sendo imprescindível para a efetivação do interesse público. A atuação do Sistema também está sujeita a distintos controles, destacando-se o da Secretaria de Controle Interno da Presidência da República – CISET/SG/PR, para controle financeiro e patrimonial, e o da CCAI, para controle congressual da Atividade de Inteligência.

O Brasil e o mundo sofrem de constante déficit institucional no campo da proteção de dados em decorrência da permanente evolução das TIC. Historicamente, no Brasil, o deficit é ainda maior no tocante a AI. Se, por um lado, é necessário garantir a defesa dos direitos e garantias fundamentais, evitando a qualquer custo uma sociedade de vigilância e de controle social; por outro, vale reconhecer a urgência de racionalizar despesas em prol da modernização na administração, por meio de um "governo digital" que trate os dados pessoais de forma a garantir a livre cidadania, bem com permita o pleno funcionamento da

inteligência de Estado, visando a preservação e salvaguarda dos interesses da sociedade brasileira.

A comunidade da inteligência aguarda, há bastante tempo, a constitucionalização da Atividade de Inteligência (AI) e a elaboração de normas que permitam ao profissional da área atuar com a noção exata de seus limites. Uma rede integrada de troca de conhecimentos em Inteligência, como o Sisbin, só adquirirá maior legitimidade e imagem positiva junto à sociedade quando regras e procedimentos claros de compartilhamento de dados forem estipulados pelo Legislativo.

Por fim, a dissertação permitiu a consolidação de procedimentos e uma arquitetura de referência para otimização do processo de comunicação sigilosa, demonstrando que a computação em nuvem privada aparece como uma solução a ser implementada no âmbito do Sisbin.

5.1 TRABALHOS FUTUROS

Em relação aos trabalhos futuros, uma série de soluções de SaaS e PaaS podem ser estruturados e implementados em órgãos do Sisbin que participem de uma mesma configuração ministerial, possibilitando experimentações com testes e validações.

A constitucionalização da AI, a elaboração de normas que permitam ao profissional de inteligência atuar com a noção exata de seus limites e outras tecnologias que possibilitem auditar o fluxo de informações sigilosas também são estudos fundamentais para a segurança do Estado brasileiro e para preservação das pessoas e orgãos envolvidos.

Finalmente, a implementação de estudos que envolvam o uso de criptografia de Estado por meio de tecnologias disruptivas com rápida troca de informações, alicerçadas na garantia de alto nível de confiabilidade potencializariam ainda mais o fluxo informacional atual.

REFERÊNCIAS BIBLIOGRÁFICAS

1 BRASIL. Decreto nº 8.793, de 29 de junho de 2016. *Diário Oficial [da] República Federativa do Brasil*, 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8793.htm>.

2 BRASIL. Decreto nº 4.376, de 13 de setembro de 2002. *Diário Oficial [da] República Federativa do Brasil*, 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2002/d4376.htm>.

3 FERREIRA, G. Perspectivas e desafios para o trabalho integrado em centros de inteligência. *Revista Brasileira de Inteligência*, v. 2, n. 16, p. 79–100, 2021.

4 BRASIL. Atividade de inteligência no brasil - coletânea de legislações - volume 5 (2012-2018). *Agência Brasileira de Inteligência*, 2023. Disponível em: <https://www.gov.br/abin/pt-br/centrais-de-conteudo/publicacoes/files_64131dd8816af.pdf>.

5 BRASIL. Lei nº 9.883 de 07 de dezembro de 1999. institui o sistema brasileiro de inteligência, cria a agência brasileira de inteligência - abin. *Diário Oficial [da] República Federativa do Brasil*, 1999. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9883.htm>.

6 BRASIL. Doutrina nacional da atividade de inteligência: fundamentos doutrinários. *Agência Brasileira de Inteligência*, 2016.

7 RIBEIRO, C. D. M.; NUNES, R. R.; OLIVEIRA, R. D. Um diagnóstico sobre o processo de comunicação sigilosa entre os órgãos do sistema brasileiro de inteligência. *Revista Ibérica de Sistemas e Tecnologias de Informação*, Associação Ibérica de Sistemas e Tecnologias de Informação, p. 169–183, 2022.

8 LU, C.-W.; HSIEH, C.-M.; CHANG, C.-H.; YANG, C.-T. An improvement to data service in cloud computing with content sensitive transaction analysis and adaptation. In: IEEE. *2013 IEEE 37th Annual Computer Software and Applications Conference Workshops*. [S.l.], 2013. p. 463–468.

9 BRASIL. Lei no 12.527 de 18 de novembro de 2011. lei de acesso a informação (lai). *Diário Oficial [da] República Federativa do Brasil*, 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>.

10 NOERTJAHYANA, A.; PALIT, H. N.; ANDJARWIRAWAN, J.; RENO, J. *Private cloud storage implementation using OpenStack Swift*. Tese (Doutorado) — Petra Christian University, 2019.

11 FERREIRA, J. R.; PINCOVSCY, J. A.; RIBEIRO, C. de M.; CANEDO, E. D.; MENDONçA, F. L. L. de. Mitigação dos riscos à privacidade através da anonimização de dados. *Revista Ibérica de Sistemas e Tecnologias de Informação*, Associação Ibérica de Sistemas e Tecnologias de Informação, 2022.

12 NASCIMENTO, F. P. d.; SOUSA, F. Classificação da pesquisa. natureza, método ou abordagem metodológica, objetivos e procedimentos. *Metodologia da Pesquisa Científica: teoria e prática–como elaborar TCC. Brasília: Thesaurus*, 2016.

13 MIDIA, C. . I. *Abin anuncia sistema de criptografia de dados para proteger Petrobras*. 2008. Urlhttps://itforum.com.br/noticias/abin-anuncia-sistema-de-criptografia-de-dados-para-proteger-petrobras/.

14 MENDES, G. F. Curso de direito constitucional/gilmar ferreira mendes, paulo gustavo gonete branco. *9ª Edição. São Paulo: Saraiva*, 2014.

15 ROCHA, W. L. industrial, econômico e financeiro, são paulo: Malheiros, v. 41, n. 125, jan./mar. 2002. *Revista Brasileira de Direito Societário e Registro Empresarial*, p. 192, 2020.

16 CRUZ, A. Aprimoramento da capacidade analítica e avanço na atividade de inteligência. *Revista Brasileira de Inteligência*, v. 1, n. 15, p. 25–40, 2020.

17 CLARK, R. M. *Intelligence analysis: a target-centric approach*. [S.l.]: CQ press, 2019.

18 HERMAN, M. *Intelligence power in peace and war*. [S.l.]: Cambridge University Press, 1996.

19 FRANCO, C. R. da R. Um catálogo de boas práticas, erros sintáticos e semânticos em modelos bpmn. *Universidade Federal de Pernambuco*, 2017.

20 DUMAS, M.; ROSA, M. L.; MENDLING, J.; REIJERS, H. A. *Fundamentals of business process management*. [S.l.]: Springer, 2013.

21 CAMPOS, A. L. *Modelagem de Processos com BPMN 2ª edição*. [S.l.]: Brasport, 2014.

22 RIOS, I. R. et al. Análise de fluxos informacionais do processo de aquisição por pregão eletrônico da pró-reitoria administrativa da universidade federal da paraíba. *Universidade Federal da Paraíba*, 2019.

23 LACHTERMACHER, G. *Pesquisa operacional na tomada de decisões* . [S.l.]: Grupo Gen-LTC, 2016.

24 ARAúJO, W. J. d.; GOMES, T. A. Avaliação de sistemas de gerenciamento de processos de negócios (bpms): análise multicritério dos softwares bizagi e bonita. *RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação*, SciELO Brasil, v. 20, 2023.

25 SCHEER, A.; BRABäNDER, E. O processo de gest!ao de processos de negócio. *Manual de BPM: Gestão de processos de negócio, Bookman, Porto Alegre*, 2013.

26 VALLE, R.; OLIVEIRA, S. B. d. Análise e modelagem de processos de negócios: foco na notação bpmn (business process modeling notation). In: *Análise e modelagem de processos de negócios: Foco na notação BPMN (Business Process Modeling Notation)*. [S.l.]: Editora Atlas, 2011. p. 207–207.

27 PAIM, R.; CARDOSO, V.; CAULLIRAUX, H.; CLEMENTE, R. *Gestão de processos: pensar, agir e aprender*. [S.l.]: Bookman Editora, 2009.

28 FILHO, J. R. de F.; MARCHISOTTI, G. G.; MAGGESSI, K. M. F.; JUNIOR, H. L. D. M. Método de pesquisa misto para identificação do problema de pesquisa. *Conhecimento & Diversidade*, Centro Universitário LaSalle-RJ, v. 10, n. 22, p. 88–102, 2018.

29 FILHO, A. M. S.; SILVA, R. R. da; SILVA, D. C. da; MEDEIROS, M. F. M. de. O processo empreendedor: associando o business model canvas (bmc) ao life cycle canvas (lcc). *Exacta*, Universidade Nove de Julho, v. 16, n. 4, p. 35–44, 2018.

30 HAMWI, M.; LIZARRALDE, I.; LEGARDEUR, J. Demand response business model canvas: A tool for flexibility creation in the electricity markets. *Journal of Cleaner Production*, Elsevier, v. 282, p. 124539, 2021.

31 MAHLE, A. C. O. A autodeterminação informativa como fundamento da lei geral de proteção de dados brasileira: uma análise a partir da lgpd. *Universidade Federal de São Carlos*, 2021.

32 RIBEIRO, R. C.; CANEDO, E. D. Using mcda for selecting criteria of lgpd compliant personal data security. In: *The 21st Annual International Conference on Digital Government Research*. [S.l.: s.n.], 2020. p. 175–184.

33 ZHENG, J.; SHEN, X. Pattern mining and detection of malicious sql queries on anonymization mechanism. *IEEE Access*, IEEE, v. 9, p. 15015–15027, 2021.

34 ŠTARCHOŇ, P.; PIKULÍK, T. Gdpr principles in data protection encourage pseudonymization through most popular and full-personalized devices-mobile phones. *Procedia Computer Science*, Elsevier, v. 151, p. 303–312, 2019.

35 BRASIL. Lei nº 13.709 de 14 de agosto de 2018. lei geral de proteção de dados pessoais (lgpd). *Diário Oficial [da] República Federativa do Brasil*, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>.

36 DIAS, S. P. Autonomia heteronoma e discriminação algorítmica: análise do piso normativo para admissão do tratamento discriminatório de dados pessoais do titular. *Universidade Federal de Ouro Preto*, 2022.

37 XUE, M.; KARRAS, P.; RAÏSSI, C.; PUNG, H. K. Utility-driven anonymization in data publishing. In: *Proceedings of the 20th ACM international conference on Information and knowledge management*. [S.l.: s.n.], 2011. p. 2277–2280.

38 SPADA, E. S.; FORTE, S. H. A. C. Cenários prospectivos das universidades corporativas no brasil-2030. *Future Studies Research Journal: Trends and Strategies*, v. 10, n. 2, p. 188–213, 2018.

39 GUNAWAN, D. A data anonymization method to mitigate identity attack in transactional database publishing. In: IEEE. *2020 8th International Conference on Information and Communication Technology (ICoICT)*. [S.l.], 2020. p. 1–6.

40 GUNAWAN, D.; NUGROHO, Y. S.; IRSYADI, F. Y. A. et al. Anonymizing prescription data against individual privacy breach in healthcare database. In: IEEE. *2021 9th International Conference on Information and Communication Technology (ICoICT)*. [S.l.], 2021. p. 138–143.

41 AREAL, B. M. d. M. G. *Building Anonymised Database Samples*. Tese (Doutorado) — Universidade NOVA de Lisboa (Portugal), 2011.

42 ABNT, N. Iso 31000 gestão de riscos: Princípios e diretrizes. *Committee Draft of ISO*, v. 31000, 2009.

43 INSTITUCIONAL, P. da República/Gabinete de S. Instrução normativa 5 de 30 de agosto de 2021 - dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal. *Diário Oficial da União*, https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684, 2021.

44 ABNT, N. Informação e documentação - artigo em publicação periódica técnica e/ou científica - apresentação. *Committee Draft of ISO*, v. 6022, 2018.

45 SEN, A. K.; TIWARI, P. K. Security issues and solutions in cloud computing. *IOSR Journal of Computer Engineering*, v. 19, n. 2, p. 67–72, 2017.

46 RANGEL, A. S. Transparência versus segurança da informação: uma análise dos fatores de risco expostos na comunicação entre o governo e a sociedade. 2015.

47 CAVIGGIOLI, F.; COLOMBELLI, A.; MARCO, A. D.; SCELLATO, G.; UGHETTO, E. Co-evolution patterns of university patenting and technological specialization in european regions. *The Journal of Technology Transfer*, Springer, v. 48, n. 1, p. 216–239, 2023.

48 INSTITUCIONAL, P. da República/Gabinete de S. Portaria gsi/pr nº 93, de 18 de outubro de 2021. *Diário Oficial da União*, Diário Oficial da União, Seção 1, p. 36, 2021.

49 KOZHUHAROVA, D.; KIROV, A.; AL-SHARGABI, Z. Ethics in cybersecurity. what are the challenges we need to be aware of and how to handle them? In: *Cybersecurity of Digital Service Chains: Challenges, Methodologies, and Tools*. [S.l.]: Springer International Publishing Cham, 2022. p. 202–221.

50 SOUZA, A. d. F. N. d. As capacidades geradas pela implantação do projeto piloto do sistema integrado de monitoramento de fronteiras (sisfron) na fronteira oeste brasileira. 2020.

51 FERREIRA, É. d. S. O programa estratégico do exército brasileiro"sistema integrado de monitoramento de fronteiras"e a aquisição de novas tecnologias. Escola Superior de Guerra (Campus Brasília), 2020.

52 EPEX, E. d. P. d. E. Escritório de projetos do exército - epex 2020. Exército Brasileiro, 2020.

53 RODRIGUEZ, P. A. L. As relações interorganizacionais em programas públicos: um estudo de caso no programa sistema integrado de monitoramento de fronteiras–sisfron. IDP/EAB, 2020.

54 BUFOLO, R. O sisfron e o papel do exército nas operações em ambiente interagências. *Rio de Janeiro: Escola de Comando e Estado-Maior do Exército*, 2014.

55 RAZA, S. Proposição de um sistema de segurança de fronteiras brasileiras: um esforço para transformar o desenho de força. *A América do Sul vive um momento bastante especial. Com o encerramento de um longo ciclo de regimes autoritários e a superação das principais hipóteses de conflito entre os países da região, o subcontinente tem avançado decisivamente rumo à consolidação democrática, ao progresso socioeconômico e à estabilidade institucional. Ainda que tal processo enfrente obstáculos e, por vezes, aparentes recuos, não se vislumbra a possibilidade de inversão de tal tendência.*, p. 59, 2014.

56 LEITE, A. P. et al. O projeto piloto do sistema integrado de monitoramento de fronteiras (2012-2016). 2018.

57 TANG, W.; QIANG, M.; DUFFIELD, C. F.; YOUNG, D. M.; LU, Y. Incentives in the chinese construction industry. *Journal of Construction Engineering and Management*, American Society of Civil Engineers, v. 134, n. 7, p. 457–467, 2008.

58 PEREIRA, A. C. A. A implantação da 3ª bateria de artilharia antiaérea na 4ª brigada de cavalaria mecanizada e sua integração ao projeto piloto do sistema integrado de monitoramento de fronteiras: uma proposta de emprego nas operações de busca aérea na faixa de fronteira. 2018.

59 NASCIMENTO, J. C. P. O impacto das novas tecnologias no programa sistema integrado de monitoramento de fronteiras (sisfron). 2020.

60 ANDRADE, I. de O.; CORTINHAS, J. da S.; SOARES, M. A.; FRANCO, L. G. A. *Sistema integrado de monitoramento de fronteiras em perspectiva*. [S.l.]: Instituto de Pesquisa Econômica Aplicada, 2019.

61 LOPES, L. D. O. A atuação brasileira contra o narcotráfico transnacional no arco central da fronteira: uma análise do sistema integrado de monitoramento de fronteiras (sisfron). Universidade Federal do Tocantins, 2022.

62 OLIVEIRA, R. C. F. de; NZE, G. D. A.; DIAS, U. S. Emprego dual-civil e militar-do 5g na defesa brasileira: uma proposta para o sisfron, sob domínio do exército. *Revista Ibérica de Sistemas e Tecnologias de Informação*, Associação Ibérica de Sistemas e Tecnologias de Informação, n. E49, p. 599–615, 2022.

63 COSTA, M. K. B. d. Políticas de segurança e defesa da fronteira brasileira no contexto de integração regional: os casos das fronteiras brasil-paraguai e brasil-uruguai. 2017.

64 ALVES, A. de A.; ALVES, C. A. de M.; TABOSA, F. G. F.; NUNES, R. R. Riscos da computação em nuvem: estudo na ótica dos gestores de órgãos públicos federais no brasil. *Navus: Revista de Gestão e Tecnologia*, Serviço Nacional de Aprendizagem Comercial (Senac), v. 1, n. 11, p. 1–18, 2021.

65 MOREIRA, C. V.; MONTEIRO, R. M.; FILHO, F. L. de C.; LUCAS, M.; ALBUQUERQUE, R. de O.; JúNIOR, R. T. de S. et al. Compartilhamento de arquivos em home office: uma solução de armazenamento de arquivos segura e altamente disponível em um ambiente de nuvem privada. *Revista Ibérica de Sistemas e Tecnologias de Informação*, Associação Ibérica de Sistemas e Tecnologias de Informação, v. 1, n. E42, p. 409–424, 2021.

66 AHMED, I. A brief review: security issues in cloud computing and their solutions. *Telkomnika (Telecommunication Computing Electronics and Control)*, v. 17, n. 6, p. 2812–2817, 2019.

67 SANTOS, D. M. L. dos; VALE, K. M. A. C.; ALENCAR, F. M. R. de. Avaliação de desempenho de nuvens privadas: um comparativo entre owncloud, nextcloud e pydio. *Brazilian Journal of Development*, v. 6, n. 6, p. 40549–40566, 2020.

68 FERNÁNDEZ, O. J. M. et al. *Carrera de Ingeniería en Informática frente a las innovaciones: Pertinencia de los planes curriculares académicos universitarios en ingeniería en informática en relación a la demanda del mercado laboral paraguayo.* Dissertação (Mestrado) — FCJPC-UAA, 2017.

69 YOU, P.; PENG, Y.; LIU, W.; XUE, S. Security issues and solutions in cloud computing. In: IEEE. *2012 32nd International Conference on Distributed Computing Systems Workshops*. [S.l.], 2012. p. 573–577.

70 MENDES, L. S. *Privacidade, proteção de dados e defesa do consumidor-Linhas gerais de um novo direito fundamental*. [S.l.]: Saraiva Educação SA, 2017.

71 BOENISCH, F.; MUNZ, R.; TIEPELT, M.; HANISCH, S.; KUHN, C.; FRANCIS, P. Side-channel attacks on query-based data anonymization. In: *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. [S.l.: s.n.], 2021. p. 1254–1265.

72 GIL, A. *Como classificar as pesquisas. Como elaborar projetos de pesquisa, 4 (1), 44-45*. 2002.

73 BARDIN, L.; CAVIGNAC, J.; LINS, C.; MAUX, A.; LIMA, I. B. de; SOUZA, G. I. R. de; DANTAS, M. G. da S.; VIRGINIO, D. F. Gil, ac métodos e técnicas de pesquisa social . são paulo: Atlas, 2010. *Programação Geral*, p. 69, 2010.

74 MINAYO, M. C. de S.; DESLANDES, S. F.; GOMES, R. *Pesquisa social: teoria, método e criatividade*. [S.l.]: Editora Vozes Limitada, 2011.

75 GIL, A. C. *Métodos e técnicas de pesquisa social*. [S.l.]: 6. ed. Ediitora Atlas SA, 2008.

76 KUMAR, P. R.; RAJ, P. H.; JELCIANA, P. Exploring data security issues and solutions in cloud computing. *Procedia Computer Science*, Elsevier, v. 125, p. 691–697, 2018.

77 GONÇALVES, C. Notas de aula de metodologia científica. *Universidade Federal de Minas Gerais*, 2013.

78 FEIJó, A. M.; VICENTE, E. F. R.; PETRI, S. M. O uso das escalas likert nas pesquisas de contabilidade. *Revista Gestão Organizacional*, v. 13, n. 1, p. 27–41, 2020.

79 CALANDRINI, L. C. L. As cores na arte: uma experiência cromática. *Trabalho de Conclusão de Curso (Graduação em Comunicação Visual Design)-Escola de Belas Artes, Universidade Federal do Rio de Janeiro. Rio de Janeiro*, 2018.

80 ARTES, G. *Teoria das cores - Estudo e Harmonia das cores*. 2020. Disponível em: <https://gdartes.com.br/teoria-das-cores-estudo-e-harmonia-das-cores/>.

81 CASTRO, R. d. C. de; SOUSA, V. L. P. de. Segurança em cloud computing: Governança e gerenciamento de riscos de segurança. 2010.

82 BARROSO, R. d. O. et al. Pfsense: teletrabalho durante a pandemia do covid-19. Instituto Federal do Amapá, 2021.

83 DOCUMENTATION, O. *OpenStack's Documentation - Manage IP addresses*. 2019. Disponível em: <https://docs.openstack.org/ocata/user-guide/cli-manage-ip-addresses.html>.

84 HASHEM, I. A. T.; YAQOOB, I.; ANUAR, N. B.; MOKHTAR, S.; GANI, A.; KHAN, S. U. The rise of "big data" on cloud computing: Review and open research issues. *Information systems*, Elsevier, v. 47, p. 98–115, 2015.

85 ANDRADE, A. L. L.; OLIVEIRA, P. B. de; FILHO, F. L. de C.; DIAS, U. S.; JúNIOR, R. T. de S.; ALBUQUERQUE, R. de O. Estudo de soluções vpn site-to-site segundo as técnicas criptográficas empregadas. *WWW/INTERNET*, p. 171, 2019.

86 DARABSEH, A.; AL-AYYOUB, M.; JARARWEH, Y.; BENKHELIFA, E.; VOUK, M.; RINDOS, A. Sddc: A software defined datacenter experimental framework. In: IEEE. *2015 3rd international conference on future internet of things and cloud*. [S.l.], 2015. p. 189–194.

87 DAVIDSON, S. B.; GARCIA-MOLINA, H.; SKEEN, D. Consistency in a partitioned network: a survey. *ACM Computing Surveys (CSUR)*, ACM New York, NY, USA, v. 17, n. 3, p. 341–370, 1985.

88 DONENFELD, J. A. Wireguard: next generation kernel network tunnel (2018). *URL: https://www. wireguard. com/papers/wireguard. pdf*, 2017.

89 VENKATESH, A.; EASTAFF, M. S. A study of data storage security issues in cloud computing. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, v. 3, n. 1, p. 1741–1745, 2018.

APÊNDICES

Apêndice A - Questionário de Identificação para o Sisbin

Seção 1 de 4

IDENTIFICAÇÃO DA APLICABILIDADE DE UM MODELO DE COMUNICAÇÃO PARA TROCA DE CONHECIMENTOS E DADOS SENSÍVEIS ENTRE OS ÓRGÃOS DO SISTEMA BRASILEIRO DE INTELIGÊNCIA (SISBIN) DE FORMA CONFIÁVEL, DISPONÍVEL E SEGURA POR MEIO DE NUVEM PRIVADA DE FÁCIL ACESSO.

Bem-vindo ao formulário Identificação da aplicabilidade de um modelo de comunicação de conhecimentos e dados entre os órgãos do SISBIN de forma confiável, disponível e segura por meio de nuvem privada de fácil acesso. Abaixo, serão relacionados alguns modelos e atividades identificados em publicações acadêmicas. Será solicitada sua opinião quanto ao conhecimento destes modelos e a contribuição efetiva deles à troca de conhecimentos entre os órgãos do SISBIN. Não se preocupe se alguns dos modelos forem desconhecidos ou não tiver opinião formada sobre sua aplicabilidade, basta marcar o item identificado com essa opção (Não concordo nem discordo) ou deixá-lo em branco. A estimativa de tempo para preencher o questionário é de 15 minutos. Muito Obrigado!

Esta pesquisa é parte de um trabalho de mestrado do Programa de Pós-Graduação Profissional em Engenharia Elétrica da Universidade de Brasília - PPEE/UnB.

Contatos do pesquisador: cilenomag@gmail.com

DECLARAÇÃO DE CONSENTIMENTO INFORMADO
Ao responder a esta pesquisa, você permite que os pesquisadores obtenham, usem e divulguem as informações anônimas fornecidas conforme descrito abaixo.

CONDIÇÕES E ESTIPULAÇÕES
1. Eu entendo que todas as informações são confidenciais. Não serei identificado pessoalmente. Concordo em preencher o questionário para fins de pesquisa e que os dados derivados desta pesquisa anônima podem ser publicados em periódicos, conferências e postagens em blog.
2. Eu entendo que minha participação nesta pesquisa é totalmente voluntária e que a recusa em participar não implicará em nenhuma penalidade ou perda de benefícios. Se eu quiser, posso cancelar minha participação a qualquer momento. Também entendo que, se decidir participar, posso recusar-me a responder a qualquer pergunta para a qual não me sinta confortável em responder.
3. Entendo que posso entrar em contato com os pesquisadores se tiver alguma dúvida sobre a pesquisa. Estou ciente de que meu consentimento não me beneficiará diretamente. Também estou ciente de que o autor manterá os dados coletados em perpetuidade e poderá utilizar os dados para trabalhos acadêmicos futuros.
4. Ao clicar no botão abaixo, eu livremente dou consentimento e reconheço meus direitos como um participante voluntário de pesquisa conforme descrito acima e dou consentimento aos pesquisadores para usarem minhas respostas na condução de pesquisas nas áreas mencionadas acima.

Após a seção 1 Continuar para a próxima seção

acima.

* Indica uma pergunta obrigatória

Tema: Um modelo de comunicação de conhecimentos e dados entre os órgãos do SISBIN de forma confiável, disponível e segura por meio de nuvem privada de fácil acesso.

1. 1. Qual o órgão o Sr/a pertence no SISBIN? *

Marcar apenas uma oval.

- ◯ EB
- ◯ FAB
- ◯ GSIPR
- ◯ ABIN
- ◯ AGU
- ◯ CGU
- ◯ PF
- ◯ PFR
- ◯ STJ
- ◯ PR
- ◯ VPR
- ◯ MB
- ◯ MAPA
- ◯ PGR
- ◯ Outro: _____

2. PERGUNTAS BASEADAS NO MODELO DE NEGÓCIO DE VALOR

Essas perguntas foram baseadas no Modelo de Negócio de Valor discutida com integrantes da Escola de Inteligência e com integrantes do Departamento de Segurança da Informação e Comunicações do GSIPR.

2. 2.1) Na sua opinião, a troca de informações entre os órgãos vinculados ao SISBIN ocorre com rapidez, atentendendo aos critérios de “Disponibilidade, Integridade, Confidencialidade e Autenticidade"? Marque a seleção abaixo conforme a sua precepção atual: *

Marcar apenas uma oval por linha.

	Discordo plenamente	Discordo	Não concordo / Não discordo	Concordo	Concordo plenamente	Não sei responder ou não quero responder
Disponibilidade	◯	◯	◯	◯	◯	◯
Integridade	◯	◯	◯	◯	◯	◯
Confidencialidade	◯	◯	◯	◯	◯	◯
Autenticidade	◯	◯	◯	◯	◯	◯

3. 2.2) Caso ocorra a criação de uma nuvem privada destinada ao SISBIN para a comunicação de conhecimentos sensíveis, isso atenderia aos critérios de disponibilidade, confidencialidade e integridade e autenticidade atendendo ao fluxo informacional necessário a troca de informações? *

Marcar apenas uma oval.

- ◯ Discordo plenamente
- ◯ Discordo
- ◯ Não concordo / Não discordo
- ◯ Concordo
- ◯ Concordo plenamente
- ◯ Não sei ou não quero responder

4. 2.3) Em uma nuvem privada temos a capacidade integrar atividades laborativas de vários orgãos de interesse no SISBIN, proporcionando modelagem em casos de trabalhos conjuntos. Essa ferramenta agilizaria a produção de forma cooperativa com vários órgãos no SISBIN? *

Marcar apenas uma oval.

- Discordo plenamente
- Discordo
- Não concordo / Não discordo
- Concordo
- Concordo plenamente
- Não sei ou não quero responder

5. 2.4) Os órgãos do sistema de inteligência necessitam compartilhar conhecimentos, analisando conjuntamente cenários internos e externos de interesse do Estado para fins de assessoramento e decisão, com o estabelecimento de pontos focais para troca de informações para a produção de relatórios, a facilidade de acesso a nuvem privada e segura acarretaria uma vantagem para a comunicação entre os órgãos? *

Marcar apenas uma oval.

- Discordo plenamente
- Discordo
- Não concordo / Não discordo
- Concordo
- Concordo plenamente
- Não sei ou não quero responder

6. 2.5) A plataforma atual utilizada para troca de conhecimentos e dados atende os critérios de Oportunidade e Imparcialidade para a comunicação de conhecimentos e dados entre os órgãos? *

Marcar apenas uma oval por linha.

	Discordo plenamente	Discordo	Concordo	Não concordo / Não discordo	Concordo plenamente	Não sei ou não quero responder
Oportunidade	◯	◯	◯	◯	◯	◯
Imparcialidade	◯	◯	◯	◯	◯	◯

7. 2.6) Na sua opinião a possibilidade de controlar o fluxo de comunicação (segurança e gestão) dos conhecimentos e dados são fundamentais para a comunicação entre os órgãos? *

Marcar apenas uma oval.

- ◯ Discordo plenamente
- ◯ Discordo
- ◯ Não concordo / Não discordo
- ◯ Concordo
- ◯ Concordo plenamente
- ◯ Não sei ou não quero responder

8. 2.7) A plataforma atual atende os critérios de possível auditoria para a comunicação de conhecimentos e dados entre os órgãos? * *

Marcar apenas uma oval.

- ◯ Discordo plenamente
- ◯ Discordo
- ◯ Não concordo / Não discordo
- ◯ Concordo
- ◯ Concordo plenamente
- ◯ Não sei ou não quero responder

9. 2.8) A oportunidade de criar na nuvem privada trilhas de auditoria na comunicação de conhecimentos e dados são fundamentais no processo de controle na troca de informações entre os órgãos? *

Marcar apenas uma oval.

- ◯ Discordo plenamente
- ◯ Discordo
- ◯ Não concordo / Não discordo
- ◯ Concordo
- ◯ Concordo plenamente
- ◯ Não sei ou não quero responder

10. 2.9) A adoção de um modelo de comunicação de conhecimentos e dados entre os órgãos do SISBIN de forma confiável, disponível e segura por meio de nuvem privada de fácil acesso fomentaria o aumento da integração entre os órgãos do SIBIN? *

Marcar apenas uma oval.

- ◯ Discordo plenamente
- ◯ Discordo
- ◯ Não concordo / Não discordo
- ◯ Concordo
- ◯ Concordo plenamente
- ◯ Não sei ou não quero responder

11. 2.10) A possibilidade de antecipar fatos ao decisor (Presidente da República) por meio da utilização da nuvem privada e segura condiz uma proposta de valor como subsídio para o Chefe do Executivo? *

Marcar apenas uma oval.

- ◯ Discordo plenamente
- ◯ Discordo
- ◯ Não concordo / Não discordo
- ◯ Concordo
- ◯ Concordo plenamente
- ◯ Não sei ou não quero responder

12. 2.11) A implantação de uma ferramenta baseda em nuvem privada capaz de automatizar o registro de conhecimentos acarretaria um fortalecimento nas comunicações de conhecimentos e dados entre os órgãos? *

Marcar apenas uma oval.

- Discordo plenamente
- Discordo
- Não concordo / Não discordo
- Concordo
- Concordo plenamente
- Não sei ou não quero responder

13. 2.12) O suporte tecnológico centralizado pela ABIN para os órgãos do SISBIN, visando dar continuidade na troca de conhecimentos e dados por meio da nuvem privada facilitaria a manutenção da continuidade no uso da plataforma na nuvem privada e segura? *

Marcar apenas uma oval.

- Discordo plenamente
- Discordo
- Não concordo / Não discordo
- Concordo
- Concordo plenamente
- Não sei ou não quero responder

14. 2.13) Em caso da implantação de uma nuvem privada para troca de conhecimentos e dados entre os órgãos, o baixo custo envolvido na utilização da ferramenta favoreceria a utilização desse modelo por todos os órgãos? *

Marcar apenas uma oval.

- Discordo plenamente
- Discordo
- Não concordo / Não discordo
- Concordo
- Concordo plenamente
- Não sei ou não quero responder

3. PERGUNTAS BASEADAS NA LEI DE ACESSO A INFORMACÃO

Essas perguntas se basearam no Art 25 da Lei de Acesso a Informacao, Lei nº 12.527, de 18 de novembro de 2011 – Brasil.

15. 3.1) Na sua opinião é importante a proteção no fluxo das informações sigilosas não classificadas, mesmo sem possuírem amparo legal previsto na LAI? *

Marcar apenas uma oval.

- ◯ Discordo plenamente
- ◯ Discordo
- ◯ Não concordo / Não discordo
- ◯ Concordo
- ◯ Concordo plenamente
- ◯ Não sei ou não quero responder
- ◯ Outro: _____

16. 3.2) As ferramentas utilizadas para a troca de conhecimentos sigilosos não classificados atendem as necessidades de agilidade no fluxo informacional atual? *

Marcar apenas uma oval.

- ◯ Discordo plenamente
- ◯ Discordo
- ◯ Não concordo / Não discordo
- ◯ Concordo
- ◯ Concordo plenamente
- ◯ Não sei ou não quero responder

17. 3.3) Na sua opinião o uso de criptografia de estado utilizado somente para informações classificadas conforme a LAI atende aos critérios de segurança para o fluxo de informações entre os órgãos do SISBIN? *

Marcar apenas uma oval.

- ◯ Discordo plenamente
- ◯ Discordo
- ◯ Não concordo / Não discordo
- ◯ Concordo
- ◯ Concordo plenamente
- ◯ Não sei ou não quero responder

18. 3.4) O Sr concorda que o aumento da sensibilização, habilitação e criação de postos de controle para o tratamento das informações sigilosas potencializarão a utilização da comunicação por nuvem privada gerando agilidade, segurança e oportunidade? *

Marcar apenas uma oval por linha.

	Discordo plenamente	Discordo	Concordo	Não concordo / Não discordo	Concordo plenamente	Não sei ou não quero responder
Agilidade	◯	◯	◯	◯	◯	◯
Segurança	◯	◯	◯	◯	◯	◯
Oportunidade	◯	◯	◯	◯	◯	◯

4. PERGUNTAS INTER-RELACIONADAS

Essas perguntas inter-relacionaram as perguntas anteriores e a Norma Complementar Nr 14 - R01 - Seguranca da Informacao em Nuvem.

19. 4.1) Em sua opinião a manutenção do fluxo de troca de conhecimentos e dados entre os órgãos do sistema são fundamentais ao assessoramento baseado em inteligência? *

Marcar apenas uma oval.

- Discordo plenamente
- Discordo
- Não concordo / Não discordo
- Concordo
- Concordo plenamente
- Não sei ou não quero responder

20. 4.2) O Sr/a concorda que a alta administração de cada órgão ou entidade da Administração Pública Federal deve considerar a Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) para definir a utilização ou não das tecnologias de computação em nuvem? *

Marcar apenas uma oval.

- Discordo plenamente
- Discordo
- Não concordo / Não discordo
- Concordo
- Concordo plenamente
- Não sei ou não quero responder

21. 4.3) O Sr/a concorda que a Abin, como órgão central do SISBIN, deve ser a provedora dos recursos tecnológicos para acessar a nuvem privada, também baseando o servidor em área sob sua responsabilidade? *

Marcar apenas uma oval.

- Discordo plenamente
- Discordo
- Não concordo / Não discordo
- Concordo
- Concordo plenamente
- Não sei ou não quero responder

22. 4.4) Caso queira apresentar sugestões sobre o trabalho de pesquisa especificamente na utilização do modelo no que tange a tecnologia empregada utilize o campo abaixo:

23. 4.5) Caso tenha alguma sugestão que fortaleça a interação e troca de conhecimentos utilize o campo abaixo:

24. 4.6) Indique pessoas que podem participar na coleta da pesquisa?