UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS DA EDUCAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

Gislaine Parra Freund

COM.PRIVACY: Modelo para gerenciamento de evidências de proteção e privacidade de dados

Florianópolis
2022

Gislaine Parra Freund

COM.PRIVACY: Modelo para gerenciamento de evidências de proteção e privacidade de dados

Tese submetida ao Programa de Pós-Graduação em Ciência da Informação da Universidade Federal de Santa Catarina para a obtenção do título de doutora em Ciência da Informação.

Orientador: Prof. Douglas Dyllon Jeronimo de Macedo, Dr.

Florianópolis

2022

Ficha de identificação da obra

Freund, Gislaine Parra
COM.PRIVACY : Modelo para gerenciamento de evidência de proteção e privacidade de dados / Gislaine Parra Freund ; orientador, Douglas Dyllon Jeronimo de Macedo, 2022.
216 p.

Tese (doutorado) - Universidade Federal de Santa Catarina, Centro de Ciências da Educação, Programa de Pós Graduação em Ciência da Informação, Florianópolis, 2022.

Inclui referências.

1. Ciência da Informação. 2. Proteção e Privacidade de Dados. 3. Segurança da Informação. 4. Gerenciamento de Evidências . 5. Pesquisa em Ciência do Design. I. Dyllon Jeronimo de Macedo, Douglas. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Ciência da Informação. III. Título.

Gislaine Parra Freund

COM.PRIVACY: Modelo para gerenciamento de evidências de proteção e privacidade de dados

O presente trabalho em nível de doutorado foi avaliado e aprovado por banca examinadora composta pelos seguintes membros:

Prof. Guilherme de Ataíde Dias, Dr.
Universidade Federal da Paraíba (UFPB)

Prof. Mario Antonio Ribeiro Dantas, Dr.
Universidade Federal de Juiz de Fora (UFJF)

Prof. Marcelo Minghelli, Dr.
Universidade Federal de Santa Catarina (UFSC)

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para obtenção do título de doutora em Ciência da Informação.

Documento assinado digitalmente
Edgar Bisset Alvarez
Data: 14/12/2022 14:30:41-0300
CPF: ***.516.228-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Edgar Bisset Alvarez, Dr.
Coordenador do Programa

Documento assinado digitalmente
Douglas Dyllon Jeronimo de Macedo
Data: 12/12/2022 21:49:19-0300
CPF: ***.987.372-**
Verifique as assinaturas em https://v.ufsc.br

Prof. Douglas Dyllon Jeronimo de Macedo, Dr.
Orientador

Florianópolis, 2022.

Dedico este trabalho ao meu esposo Cassiano,
à minha filha Julia e aos meus pais.

AGRADECIMENTOS

Primeiramente gostaria de agradecer a Deus por ter me acompanhado em toda essa jornada, me dando sabedoria para enfrentar os momentos mais difíceis.

Ao meu marido Cassiano e à minha filha Julia por estarem junto de mim durante todos os momentos, me incentivando a caminhar em busca desse sonho.

Agradeço aos meus pais Osvaldo e Geni e ao meu irmão Leandro por todas as palavras encorajadoras e pela torcida para que eu chegasse até aqui.

Meus sinceros agradecimentos ao meu orientador Douglas Dyllon Jeronimo de Macedo pela compreensão, confiança e pelos ensinamentos para minha formação enquanto pesquisadora. Sou extremamente grata por isso.

Aos membros da banca, professores Dr. Guilherme de Ataíde Dias, Dr. Mario Antonio Ribeiro Dantas e Dr. Marcelo Minghelli pela participação e por todos os apontamentos de melhoria que foram apresentados para a pesquisa.

À direção, coordenação, a todos os professores e funcionários do PGCIN pela dedicação e apoio dispensado em todos os momentos de necessidade.

Aos colegas de turma pelos momentos de estudo e muita aprendizagem nas disciplinas que fizemos juntos.

Ao Fabio Ricardo Santana pela compreensão de minhas ausências no trabalho para me dedicar à pesquisa e pelo apoio que sempre me foi dado.

Ao Claudio Cesar Reiter, diretor da CASCARESC, por ter permitido que a experimentação dessa tese fosse realizada nessa instituição.

À minha amiga Priscila Basto Fagundes por todo o apoio desde o início dessa caminhada e por todos os “Vai dar tudo certo!” que foram ditos. Você foi muito importante nesse processo, acredite!

À minha amiga Carla Bergamo por acompanhar essa trajetória junto comigo e pelas palavras de incentivo ditas em todos os momentos em que precisei. Gratidão eterna!

Agradeço a todos que de alguma forma contribuíram para o desenvolvimento desta tese e para a conclusão do meu doutorado, muito obrigada!

RESUMO

O universo digital proporcionou às organizações, privadas e públicas, o uso massivo de dados pessoais e informações corporativas. Com isso, novos desafios surgiram no que se refere à proteção e privacidade de dados, e legislações para tratar o tema foram adotadas em âmbito mundial. As legislações, assim como as normativas sobre essa temática, apresentam os requisitos que as organizações, os processos, os produtos ou os ambientes precisam atender para serem considerados seguros. E para adequar-se a elas é necessária à implementação de práticas diversas tanto no contexto tecnológico quanto de processos. Dentre os requisitos preconizados nas normativas, destacam-se para esta pesquisa, os requisitos de "Responsabilização" e de "Conformidade com a Privacidade", os quais definem que as organizações devem ser responsáveis e capazes de demonstrar conformidade com as mesmas. Com isso, além do desafio de implementar os requisitos de proteção e privacidade de dados, é necessário adotar processos sistematizados que comprovem como e em quais evidências estes requisitos são validados. Para demonstrar conformidade com as normativas, evidências são adotadas para comprovar a adequação aos requisitos, e precisam ser suficientes e adequadas para serem apresentadas em auditorias de qualquer natureza, tanto para fins de certificações quanto para atendimento a órgãos reguladores. Diante do exposto, considerando a obrigatoriedade da proteção e privacidade de dados por força de lei e a importância de comprovar conformidade com normativas, esta pesquisa apresenta um modelo para gerenciar evidências de proteção e privacidade dos dados para demonstrar diligência e conformidade com normativas. Para alcançar os objetivos definidos para este trabalho, foi realizada uma pesquisa aplicada, exploratória e descritiva, com abordagem quantitativa e qualitativa. Quanto aos procedimentos técnicos, esta pesquisa é classificada como bibliográfica, experimental e com painel de especialistas. Como método de pesquisa este trabalho utilizou o *Design Science Research* (DSR). Para a validação do modelo proposto, o mesmo foi aplicado em uma organização que possibilitou a observação e identificação de melhorias durante sua utilização, além da submissão de um questionário a especialistas para avaliarem o modelo. Diante do realizado, conclui-se que o modelo apoia a validação e comprovação de conformidade com requisitos de proteção e privacidade de dados em todas as operações de tratamento dos dados, e pode ser adotado tanto na atividade de adequação e implementação das normativas, no processo de aferição e verificação de conformidade com as mesmas, assim como para promover a transparência do tratamento dos dados a seus titulares.

Palavras-chave: proteção e privacidade de dados; segurança da informação; evidências; gerenciamento de evidências; pesquisa em ciência do design.

ABSTRACT

The digital universe has provided private and public organizations with the massive usage of personal data and corporate information. As a result, new challenges have arisen with regard to data protection and privacy, and legislation to address this issue has been adopted worldwide. The legislation as well as the regulations on this subject present the requirements that organizations, processes, products or environments need to meet to be considered safe. To adapt to them, it is necessary to implement different technological and procedural practices. “Accountability” and “Privacy Compliance” stand out in the requirements recommended, which define that organizations must be responsible and able to demonstrate compliance with them. Thus, in addition of data protection and privacy requirements, it is necessary to adopt systematized processes to prove how and on which evidence these requirements are validated. Evidence is adopted in different contexts and in all of them, it needs to be sufficient and adequate to be presented in any audit, both for certification and compliance with regulatory agencies. Considering the law mandate and need of regulatory compliance, this research presents a model for managing evidence of data protection and privacy. To reach the objectives, an applied, exploratory and descriptive research was carried out, with a quantitative and qualitative approach. As for the technical procedures, this research is classified as bibliographic, experimental and with a panel of experts. As a research method, this work used Design Science Research (DSR). To validate the model, it was applied in an organization that allowed the observation and identification of improvements, in addition to the submission of a questionnaire to specialists to assess the adequacy of the model. It is concluded that the model supports the validation and compliance proof with data protection and privacy requirements in all data processing operations, and can be adopted both to adequacy and implementation of regulations, in the process of gauging and verifying compliance, as well as to promote transparency in the processing of data to their holders.

Keywords:. data protection and privacy; information security; evidence; evidence management; design science research.

RESUMEN

El universo digital ha proporcionado a las organizaciones, privadas y públicas, el uso masivo de datos personales e información corporativa. Como resultado, han surgido nuevos desafíos con respecto a la protección de datos y la privacidad, y se ha adoptado legislación para abordar el problema en todo el mundo. La legislación, así como la normativa en la materia, presenta los requisitos que deben cumplir las organizaciones, procesos, productos o ambientes para ser considerados seguros. Y para adaptarse a ellos es necesario implementar diferentes prácticas tanto en el contexto tecnológico como en los procesos. Entre los requisitos recomendados en la normativa, se destacan para esta investigación los requisitos de "Responsabilidad" y "Cumplimiento de la privacidad", que definen que las organizaciones deben ser responsables y capaces de demostrar el cumplimiento de los mismos. Por lo tanto, además del desafío de implementar los requisitos de protección de datos y privacidad, es necesario adoptar procesos sistematizados que demuestren cómo y con qué evidencia se validan estos requisitos. Para demostrar el cumplimiento de la normativa, se adoptan pruebas para acreditar el cumplimiento de los requisitos, las cuales deben ser suficientes y adecuadas para ser presentadas en auditorías de cualquier naturaleza, tanto para fines de certificación como para el cumplimiento de los organismos reguladores. Dado lo anterior, considerando la obligatoriedad de la protección y privacidad de los datos por ley y la importancia de acreditar el cumplimiento de la normativa, esta investigación presenta un modelo de gestión de pruebas de protección y privacidad de datos para demostrar la diligencia y el cumplimiento de la normativa. Para lograr los objetivos definidos para este trabajo, se realizó una investigación aplicada, exploratoria y descriptiva, con enfoque cuantitativo y cualitativo. En cuanto a los procedimientos técnicos, esta investigación se clasifica en bibliográfica, experimental y con panel de expertos. Como método de investigación, este trabajo utilizó Design Science Research (DSR). Para la validación del modelo propuesto, se aplicó en una organización que permitió observar e identificar mejoras durante su uso, además de enviar un cuestionario a especialistas para evaluar el modelo. En vista de lo realizado, se concluye que el modelo soporta la validación y prueba del cumplimiento de los requisitos de protección y privacidad de datos en todas las operaciones de tratamiento de datos, pudiendo ser adoptado tanto en la actividad de adecuación e implementación de normativas, en la proceso de medición y verificación del cumplimiento de los mismos, así como promover la transparencia en el tratamiento de los datos a sus titulares.

Palabras clave: protección de datos y privacidad; seguridad de la Información; evidencia; gestión de pruebas; investigación en ciencias del diseño.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

CAE	-	*Claim, Argument, Evidence*
CAPES	-	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CFTV	-	Circuito Fechado de Televisão
CLT	-	Consolidação das Leis Trabalhistas
DLP	-	*Data Loss Prevention*
DP	-	Dados Pessoais
DSR	-	*Design Science Research*
GDPR	-	*General Data Protection Regulation*
GMUD	-	Gestão de Mudanças
GPO	-	*Group Policy*
GSN	-	*Goal Structuring Notation*
IDS	-	*Intrusion Detection System*
IEEE	-	*Institute of Electrical and Electronic Engineers*
IoT	-	*Internet of Things*
IPS	-	*Intrusion Prevention System*
ISO	-	*International Organization for Standardization*
ISTA	-	*Information Science & Technology Abstracts*
LGPD	-	Lei Geral de Proteção de Dados
LISTA	-	*Library, Information Science & Technology Abstracts*
NDA	-	*Non-Disclosure Agreement*
PGCIN	-	Programa de Pós-Graduação em Ciência da Informação
RSL	-	Revisão Sistemática de Literatura
SIEM	-	*Security Information and Event Management*
SLA	-	*Service Level Agreement*
UFSC	-	Universidade Federal de Santa Catarina
WoS	-	*Web of Science*

SUMÁRIO

1 INTRODUÇÃO

Dados e informações são insumos essenciais para organizações de vários setores da economia. A necessidade informacional, o uso massivo de dados e o desenvolvimento das Tecnologias de Informação e Comunicação (TICs) vêm conduzindo a dinâmica mundial na era digital (FAGUNDES *et al*, 2017). As TICs, em constante evolução, têm continuamente aumentado a sua capacidade de armazenamento e processamento, viabilizando, assim, o crescimento da produção de dados e informações (FREUND *et al,* 2019). Independentemente do quesito propulsor, esse cenário estruturado a partir de dados remodela diferentes áreas de negócio, apresenta necessidades particulares e abre novas frentes de estudos relacionados à arquitetura, armazenamento, recuperação, segurança e proteção de dados.

Neste contexto, dados pessoais que de acordo com a ABNT NBR ISO/IEC 29100 (2020) são informações que identificam uma pessoal natural ou com seu uso pode tornar uma pessoa natural identificável — tais como nome, número de inscrição no Cadastro de Pessoas Físicas (CPF), endereço, número de telefone, entre outros — e informações corporativas — tais como planos de projetos, organogramas, segredos industriais, entre outras — são mantidos por organizações privadas e públicas de diferentes formas, para propósitos distintos. Além disso, seu tratamento acontece em sistemas de informação com diferentes arquiteturas para armazenamento, controle, segurança e privacidade. Para Isaak e Hanna (2018), os dados pessoais e informações corporativas coletados por essas organizações são submetidos a controles de segurança em níveis variados, de acordo com o ramo de atuação da organização e com as regulamentações aplicáveis a cada um deles. Mendes (2014, p. 33) complementa que a "utilização massiva de dados pessoais por organismos estatais e privados a partir de avançadas tecnologias da informação, apresenta novos desafios ao direito à privacidade".

Este tema também é discutido por Frazão, Tepedino e Oliva (2019), os quais entendem que "com o acelerado desenvolvimento tecnológico e a consolidação de espaços públicos virtuais, a gestão da informação sobre si próprio tornou-se expressão fundamental do indivíduo". Os autores complementam que existe um confronto dessa realidade com os interesses comerciais por esses dados pessoais por representarem um ativo fundamental para o aprimoramento de inúmeras atividades.

Diante da relevância e ampla utilização de dados pessoais em diferentes cenários, ascende a necessidade de fontes regulatórias específicas e normativas de referência para tratar o tema "privacidade de dados" também no âmbito digital. Dados pessoais, então, foram considerados dados críticos no âmbito da segurança da informação e receberam controles

robustos para assegurar o seu sigilo, porém, foram tratados no contexto mais amplo das informações confidenciais, não havendo definições estabelecidas especificamente para o tratamento desse tipo de dado. Com o consumo de dados pessoais, a temática da privacidade de dados passa a ser regulada por leis em um universo complementar ao da segurança da informação, com princípios específicos, e torna-se essencial, intensificando assim as obrigações de conformidade. A privacidade de dados pessoais passa a ocupar um espaço fundamental na vida do cidadão, regulamentada pela legislação.

A Lei propulsora de privacidade de dados foi a *General Data Protection Regulation* (GDPR), aplicável aos 27 países da União Europeia, sancionada em 2016 e com vigência desde maio de 2018. Esses países, por sua vez, exigem que outros países tenham leis equivalentes às suas para transacionar dados pessoais, o que fez com que a maioria daqueles que ainda não tinham leis para tratar o tema adotassem meios legais para proteger a privacidade de indivíduos. Tal é o caso do Brasil, que em 2018 sancionou a Lei Geral de Proteção de Dados Pessoais (LGPD), a qual entrou em vigor a partir de setembro de 2020. Já os países que possuíam leis para tratar a privacidade vêm atualizando-as para atender a esta modalidade de privacidade digital e equivalência à GDPR. (FACCHINI NETO; DEMOLINER, 2019).

Outro ponto a ser observado é o aspecto social envolvido nessa legislação, visto que o titular do dado é o sujeito protegido pela lei, afinal o objetivo da lei é proteger um direito do cidadão. Conforme Frazão (2018), "a Lei Geral de Proteção de Dados deixa claro que pretende proteger o usuário-cidadão plenamente, em todos os aspectos da sua autonomia pública e privada, valorizando e preservando sua autodeterminação informativa e sua capacidade decisória". Tal é a relevância da referida tutela que o direito à proteção e privacidade de dados pessoais foi inserido na Constituição Federal de 1988 como direito fundamental, pela Emenda Constitucional Nº 115, de 10 de fevereiro de 2022.

Dessa forma, se de um lado está o direito do cidadão à proteção e privacidade de seus dados, do outro a adequação às normativas e legislações demanda a implementação de boas práticas diversas em uma visão de ponta a ponta, que envolvem desde a cautela e autorização na coleta dos dados até a proteção e garantia de exclusão desses dados. Dentre essas práticas, destacam-se a provisão, organização e manutenção de evidências de conformidade concretas que possam ser utilizadas para comprovar a diligência e conformidade com normativas e fontes regulatórias. Essas práticas estão associadas aos requisitos de "Responsabilização" e "Conformidade com a Privacidade", também previstos nas legislações e normativas que são o foco de estudo desta pesquisa.

O tema “evidências de conformidade” existente nas normativas na maioria das vezes é intrínseco e não é apresentado de forma explícita com essa nomenclatura e nem como um requisito nas legislações ou normativas de referência sobre proteção e privacidade de dados. Contudo, observa-se nas legislações e nas normativas que os requisitos que trazem em seu conteúdo os verbos “demonstrar”, “provar” e “comprovar”, são atendidos com artefatos que podem ser utilizados como evidências na comprovação de conformidade.

A temática “evidências” é adotada em diversos contextos, tais como contábil, cibersegurança, qualidade, serviços em nuvem, entre outros, e em todos eles essas evidências, sejam físicas ou digitais, precisam ser suficientes e adequadas para serem apresentadas em auditoria de qualquer natureza, tanto para fins de certificações quanto para atendimento a órgãos reguladores ou clientes e fornecedores. Mohammed (2018) considera que as evidências digitais possuem a vantagem de estarem menos expostas a impactos que possam afetar sua proteção em comparação com outros tipos de evidências, além da imparcialidade e confiabilidade das mesmas.

No contexto de auditorias contábeis, Zuca (2015) salienta a importância da confiabilidade e completeza das evidências e complementa que a quantidade suficiente e a adequação das evidências de auditoria são aspectos inter-relacionados. Nesse sentido, não há um padrão de quantidade de evidências necessárias, mas que a quantidade diminui se a qualidade (adequação) das evidências obtidas aumenta. Ou seja, quanto maior a qualidade das evidências, menor será a quantidade necessária para uma comprovação.

Já no contexto de segurança em sistemas críticos, Nair *et al.* (2015) apresentam que evidências são utilizadas para justificar a segurança aceitável de um sistema, e complementam que fatores secundários — tais como as ferramentas utilizadas para gerar as evidências, as técnicas aplicadas e a experiência das pessoas que criam as evidências — podem afetar o desempenho de um avaliador e o resultado de uma análise.

No escopo dos serviços em nuvem, as evidências também são adotadas para comprovar a proteção adotada nos ambientes utilizados para a prestação de serviços. Para Freund *et al.* (2018), ao avaliar a norma ISO 27017:2016 que apresenta recomendações de boas práticas de segurança de informação para provedores de serviços em nuvem, traz que “o provedor deve evidenciar para o cliente que todos os controles de segurança acordados estão implementados e sendo praticados adequadamente”.

Assim como nos contextos apresentados, no campo da proteção e privacidade de dados também é necessário garantir o atendimento aos requisitos definidos nas normativas de referência e ser capaz de demonstrá-lo, ou seja, adotar processos sistematizados que

demonstrem como e em quais evidências esses requisitos são validados. Se por um lado as normativas definem os requisitos que um processo, produto ou ambiente precisa atender para ser considerado seguro, por outro lado estes devem estar preparados para demonstrar como esses requisitos são cumpridos com a obtenção e manutenção de evidências convincentes em todas as operações de tratamento dos dados. Diante disso, a quantidade de artefatos para evidências pode variar de acordo com os controles implementados. A complexidade está relacionada às características das organizações, que sofrem mudanças ao longo do tempo na medida em que os cenários que as originaram e as suportam são alterados.

Isto posto, observa-se que, para demonstrar conformidade, as evidências devem ser gerenciadas e estruturadas de modo a não comprometer a clareza em sua apresentação e os objetivos aos quais se propõem. Devem estar adequadas quanto à sua confiabilidade, quantidade, atualidade, rastreabilidade e ao que se espera para a comprovação de cada requisito requerido. Além disso, considerando que os cenários são dinâmicos — pois as condições, características e o ambiente tecnológico configurado inicialmente podem mudar —, gerenciar evidências passa a ser necessário, visto que elas precisam ser rastreáveis e acompanhar essas mudanças, estando coerentes também com a realidade do momento, ou seja, estando aptas e adequadas ao contexto para o qual são designadas.

Sendo assim, esta tese tem o objetivo de apresentar um modelo que contemple o gerenciamento de evidências de proteção e privacidade de dados de forma sistematizada para auxiliar na atividade de comprovação de conformidade.

Pretende-se, com esta pesquisa, que o modelo seja utilizado na tutela do direito à proteção e privacidade dos dados e que contribua com o processo de adequação de cenários às normativas de proteção e privacidade de dados, elevando assim a capacidade de comprovação sobre o tratamento de dados pessoais. Pretende-se também que o modelo possibilite que pesquisadores da comunidade acadêmica deem continuidade aos temas aqui expostos, aprimorando a problemática apresentada em estudos futuros.

1.1 MOTIVAÇÃO E JUSTIFICATIVA

A obrigatoriedade de proteção e privacidade de dados por força de lei aumenta a responsabilidade das instituições que tratam dados pessoais em adequarem seus produtos, processos, sistemas e infraestrutura, além de desenvolverem internamente a cultura de proteção e privacidade. Diversas áreas que, de alguma forma, manipulam dados pessoais precisam estar aptas a protegê-los, provendo a transparência a seus titulares, rastreabilidade dos dados e sendo

capazes de comprovar que estão em conformidade com normativas de referência e legislações. Aquelas que já utilizavam alguns controles de proteção precisam adicionalmente implementar requisitos de privacidade previstos na legislação e em normativas de referência para estarem preparadas, também, para esta obrigação legal.

Em vista disso, os pontos que reforçam a relevância do tema e motivam o desenvolvimento deste estudo são: a) leis específicas sobre privacidade foram sancionadas em âmbito mundial, tornando sua implementação obrigatória; b) além da institucionalização dessas leis, a compatibilidade entre elas tornou-se exigência para possibilitar transações envolvendo dados pessoais de diferentes países; e c) diante da obrigatoriedade de cumprimento dos requisitos de privacidade, além de garanti-los é necessário demonstrar conformidade com normativas. Dada a importância e obrigatoriedade da implementação dos requisitos de privacidade, é necessário examinar como e em que evidências eles são validados. Com isso, gerenciar evidências se torna um desafio, tendo em vista a diversidade de cenários dos quais elas são extraídas e o dinamismo desses cenários diante da necessidade de validar os requisitos e controles implementados em relação à proteção e privacidade de dados.

Em suma, a motivação desta pesquisa é desenvolver um modelo que, de forma sistemática, gerencie evidências de modo a demonstrar conformidade com normativas de referência de proteção e privacidade de dados. Pode-se, assim, considerar que o desenvolvimento desta pesquisa se justifica:

a) Pela obrigatoriedade da adequação de processos, sistemas e ambientes às leis específicas de privacidade e proteção de dados, sancionadas em âmbito mundial;
b) Por entender que o uso de evidências é o meio de comprovar conformidade com as alegações de proteção e privacidade de dados;
c) Pela necessidade de demonstrar conformidade com as normativas utilizando evidências que possam comprovar a adequação de cenários aos requisitos de proteção e privacidade de dados;
d) Pelo desafio de gerenciar evidências de proteção e privacidade de dados em cenários dinâmicos, mantendo-as coerentes e atualizadas com os mesmos;
e) Por não terem sido encontrados trabalhos relacionados que apresentassem modelos para implementar proteção e privacidade de dados e para a adoção de abordagens que apoiam no gerenciamento de evidências;
f) Por ampliar a visão da temática referente à privacidade de dados no âmbito da Ciência da Informação e em outras áreas;

g) Por contribuir com a interdisciplinaridade entre a Ciência da Informação e demais áreas, tais como: Ciência da Computação, Direito e Administração.

Além disso, a ampliação da visão da temática referente à privacidade de dados no âmbito da Ciência da Informação e em outras áreas permite que pesquisadores utilizem o modelo para a realização de testes e ajustes de suas pesquisas, bem como deem continuidade aos estudos aqui propostos.

1.2 PROBLEMA DE PESQUISA E HIPÓTESE

Mesmo antes da sanção da Lei Geral de Proteção de Dados, no cenário brasileiro, dados pessoais já eram classificados como confidenciais pela Constituição Brasileira de 1988; pela Lei n. 8.078/1990, que dispõe sobre a proteção do consumidor; pela Lei n. 12.737/2012, conhecida como "Lei Carolina Dieckmann", que dispõe sobre a tipificação criminal de delitos informáticos; e pela Lei n. 12.965/2014, conhecida como o Marco Civil da Internet, que estabelece princípios, direitos e deveres para o uso da Internet no Brasil. Em outros países, do mesmo modo, legislações diversas sustentam esse direito aos cidadãos, fato que fez com que a confidencialidade desses dados fosse tratada pelos programas de segurança informacional das organizações. Com a promulgação de leis específicas para tratar o assunto, a proteção de dados pessoais deixou de ser uma preocupação exclusiva dessa área de segurança da informação e com foco somente no sigilo dos dados, e passou a ser um direito do cidadão titular do dado com base em princípios que alteram o enfoque da temática, ampliando o escopo necessário para tratamento desses dados. Os controles e mecanismos de tratamento dos dados pessoais passam a ser pautados também pela transparência, finalidade da coleta e uso, autorização do titular e proteção da privacidade. Partindo do princípio de que a privacidade de dados se trata de um direito do indivíduo e considerando que organizações tratam dados pessoais com frequência em seus modelos de negócio, ignorá-la já não é mais uma opção possível.

Diversos requisitos de proteção e privacidade, tais como consentimento e escolha, legitimidade e especificação de objetivo, limitação de coleta, entre outros, devem ser implementados, e dentre eles, para o contexto desta pesquisa, destacam-se "Responsabilização" e "Conformidade com a Privacidade", os quais definem que as organizações devem ser responsáveis e capazes de demonstrar conformidade com fontes regulatórias e normativas de referência. Em atendimento a esses requisitos, é necessário identificar e gerenciar artefatos a serem utilizados como evidências probatórias de forma que possam ser recuperados ou obtidos sempre que necessário e válidos para o propósito da solicitação. Essa é uma tarefa intensa, visto

que todos os requisitos das leis, normativas ou padrões de proteção e privacidade de dados devem ser confirmados com evidências consistentes o suficiente para comprovar sua aderência.

Em concordância com Abdullah, Sadiq e Indulska (2010) e Sadiq e Governatori (2015), manter evidências de conformidade é um desafio no âmbito do gerenciamento de conformidade regulatória, e as organizações precisam de abordagens eficazes para planejar sistematicamente, documentar e demonstrar suas obrigações regulatórias. Apesar de existirem estudos já publicados em bases de periódicos e na Internet em geral para adequar e implementar requisitos de privacidade, eles não possuem o intuito de modelar as evidências e apoiar no seu gerenciamento com o propósito de utilizá-las na comprovação de conformidade com as normativas, desprovendo, assim, organizações de um modelo com abordagem integrada de referência para este fim. Devido à complexidade de implementação e adequação dos cenários organizacionais às legislações de proteção e privacidade de dados, observa-se que os esforços dos estudos publicados estão voltados a esses processos, ficando a comprovação dos requisitos de "Responsabilização" e "Conformidade com a Privacidade" das normativas de referência como uma preocupação secundária, até que se torne uma necessidade eminente, motivada pela necessidade de certificação ou por solicitações de órgãos reguladores.

A ausência de um modelo que apresente abordagens para o gerenciamento de evidências de forma sistemática faz com que profissionais tenham a missão de adequar seus ambientes ou desenvolver novos processos, produtos, sistemas e serviços, focando também nos requisitos da "Responsabilização" e "Conformidade com a Privacidade", e acabem por consultar e utilizar um arcabouço documental diversificado, preparando modelos próprios sem uma referência de conduta que contribua com essa atividade de forma eficaz.

Para o desenvolvimento desta pesquisa foram definidas hipóteses a serem validadas com a execução das atividades planejadas para este estudo. As hipóteses, segundo Deslandes (1994), são o diálogo entre o olhar do pesquisador e a realidade investigada, representado em um conjunto de afirmações provisórias a respeito de um determinado problema a serem verificadas na investigação, podendo elas serem formuladas a partir de fontes diversas, inclusive da intuição do pesquisador. Para este estudo foram definidas as seguintes hipóteses:

- H1: As abordagens utilizadas para o gerenciamento de evidência em casos de garantia de padrões de segurança aplicados em sistemas críticos podem ser ajustadas para o contexto de proteção e privacidade de dados e contribuir também com essa temática.

- H2: Considerando que além de implementar controle, mecanismos e processos de proteção e privacidade de dados orientados pelos requisitos das normativas de referência é necessário ser capaz de comprová-los, é possível afirmar que um modelo para gerenciar as

evidências de proteção e privacidade de dados contribui para demonstrar a conformidade com as normativas.

Considerando a obrigatoriedade de proteção e privacidade de dados por força de lei e a importância de estudos que apresentem abordagens para gerenciar evidências que validem os requisitos de proteção e privacidade de dados de acordo com as normativas, emerge a seguinte questão de pesquisa como elemento principal de investigação desta tese: **Como sistematizar o gerenciamento de evidências de conformidade de proteção e privacidade de dados em um modelo que apoie os requisitos de "Responsabilização" e "Conformidade com a Privacidade" previstos nas normativas?**

1.3 OBJETIVOS

Com o intuito de contribuir na comprovação de alegações de proteção e privacidade de dados com abordagens para o gerenciamento de evidências, e de responder à questão de pesquisa apresentada anteriormente, foram definidos para este estudo os objetivos descritos a seguir.

1.3.1 Objetivo Geral

Propor um modelo para o gerenciamento de evidências de proteção e privacidade dos dados para demonstrar conformidade com os requisitos previstos nas normativas de referência.

1.3.2 Objetivos Específicos

a) Identificar os componentes que constituirão o modelo, estabelecendo os elementos essenciais e a estrutura;

b) Elaborar o modelo para gerenciar evidências de proteção e privacidade de dados e o método de aplicação, empregando os componentes e a abordagem definida;

c) Aplicar o modelo identificando as melhorias a serem ajustadas;

d) Validar o modelo, submetendo à apreciação de especialistas.

1.4 INEDITISMO

Com intuito de comprovar a originalidade do modelo proposto e o ineditismo desta tese, em busca de trabalhos relacionados, foi elaborada uma Revisão Sistemática da Literatura (RSL) nas seguintes bases de dados: Catálogo de Teses e Dissertações da CAPES; Base de Dados Referenciais de Artigos de Periódicos em Ciência da Informação; *Library, Information Science & Technology Abstracts* (LISTA); *Information Science & Technology Abstracts* (ISTA); IEEE *Xplore Digital Library* (IEEE); *Web of Science* (WoS) e Scopus. A RSL na íntegra é apresentada na seção 3 deste documento.

As pesquisas realizadas com recorte de tempo entre 2010 e 2020 nas bases de periódicos foram realizadas por meio de palavras-chave constituindo dois conjuntos de termos por assunto, os quais foram adequados conforme as configurações fornecidas por cada base de dados. Após realizar os processos que integram a revisão sistemática de literatura, foi possível constatar a escassez de trabalhos relacionados à temática nos resultados encontrados: apenas sete trabalhos possuem alguma correspondência com esta pesquisa, conforme detalha-se na subseção 3.1 deste estudo. Vale ressaltar que foram realizadas buscas exploratórias nas bases apresentadas, as quais não esgotam totalmente as possibilidades de existirem outras soluções semelhantes para tratar a temática. Nas bases pesquisadas não foram encontrados estudos que propõem o gerenciamento de evidências no âmbito da proteção e privacidade de dados. Os sete trabalhos encontrados nas buscas, apresentados na subseção 3.1, não apresentam modelos para gerenciar evidências de proteção e privacidade de dados conforme esta pesquisa se propõe. Dentre os trabalhos encontrados que relacionam os assuntos de proteção e privacidade de dados com a abordagem de evidências, os mesmos aparecem aplicados no contexto de Internet das Coisas, computação em nuvem, processo de desenvolvimento de sistemas e infraestrutura de cibersegurança, não sendo encontrados trabalhos aplicados em contextos e cenários conforme este trabalho se propõe. Com isso, observa-se a originalidade e o ineditismo desta tese e percebe-se a oportunidade para novas pesquisas sobre o tema, unindo temáticas investigadas no âmbito da Ciência da Informação de forma complementar às outras áreas do conhecimento.

1.5 DELIMITAÇÃO DO ESCOPO

O modelo aqui proposto não tem a intenção de explorar questões jurisprudenciais em relação às leis selecionadas e abordadas no trabalho, nem aprofundar os estudos na área do direito referente às legislações que tratam sobre a temática de proteção e privacidade de dados

e nem em evidências probatórias, mas, sim, de contribuir na validação de requisitos e controles relacionados com a proteção e privacidade de dados em uma abordagem de gerenciamento de evidências de conformidade com normativas de referência de boas práticas.

A abordagem das Leis GDPR e LGPD no referencial teórico deve-se ao entendimento de que ao tratar de proteção e privacidade de dados é pertinente versar sobre essas legislações, visto que um dos itens motivacionais para o desenvolvimento desta pesquisa é o sancionamento das legislações de proteção e privacidade de dados em âmbito mundial.

Além disso, nesta pesquisa o modelo proposto utiliza instrumentos de apoio, um dos quais utiliza os requisitos da normativa de referência ABNT NBR ISO/IEC 29100:2020. Para essa escolha foi necessário avaliar a coerência dos conceitos desta normativa com a lei que rege a temática no Brasil (LGPD) e também com a lei de referência mundialmente (GDPR). Neste contexto, o que se espera é apresentar a relação conceitual entre a normativa de referência utilizada para o modelo e as legislações citadas para justificar sua escolha. Porém, o modelo não se limita ao uso da ISO 29100, outras normativas de referência podem ser adotadas para aplicação do modelo, desde que seu conteúdo seja transformado em requisitos e pré-requisitos, de acordo com o cenário de avaliação pretendido.

O modelo de gerenciamento de evidências de proteção e privacidade de dados apresentado nesta tese propõe-se a demonstrar conformidade com os requisitos de "Responsabilização" e "Conformidade com a Privacidade" previstos na normativa de referência, os quais relacionam-se com a comprovação de conformidade com as fontes regulatórias.

1.6 CONTRIBUIÇÕES DA PESQUISA

Em face das contribuições pretendidas com esta pesquisa, nesta subseção apresenta-se uma discussão acerca destas no âmbito científico, tecnológico e social.

A Ciência vive constantes transformações apoiadas em dados e informações que permeiam diferentes esferas do saber, permitindo diálogos entre elas. Conforme apontam Colombo e Fetz (2014, p. 47):

> Convivemos com informações recentes que protagonizam algumas transformações no campo científico, especialmente aquelas que visam à inter e multidisciplinaridade, saberes que visam atender — em partes — às necessidades da sociedade moderna, complexa em sua origem e que exige dos pesquisadores contemporâneos a exploração do conhecimento através de um senso crítico apurado.

Ao tratar o tema “proteção e privacidade de dados” no âmbito da Ciência da Informação, amplia-se a visão da temática nesta ciência, além de contribuir com sua interdisciplinaridade em relação a outras áreas, tais como Ciência da Computação, Direito e Administração. A comunidade acadêmica científica também pode se beneficiar com o estudo, visto que o trabalho apresentará a análise de abordagens de gerenciamento de evidências propostas na literatura, aplicada em diferentes contextos, e a proposição do modelo com base em pesquisas realizadas anteriormente, permitindo que pesquisadores o utilizem para a realização de testes e ajustes em suas pesquisas bem como deem continuidade aos estudos aqui propostos. Ao considerar que os resultados desta pesquisa são disponibilizados aos pesquisadores da Ciência da Informação, os mesmos também contribuem com as demais áreas supramencionadas, os quais com o viés da interdisciplinaridade existente evoluem no escopo desta pesquisa para as práticas informacionais em prol da proteção e privacidade de dados.

Já no âmbito tecnológico, ressalta-se que a globalização e o desenvolvimento de tecnologias vêm acompanhados de desafios no que se refere à segurança das informações corporativas e proteção à privacidade dos dados pessoais. Organizações públicas e privadas tratam dados pessoais em menor ou maior volume, os quais são processados, analisados e armazenados em infraestruturas tecnológicas que apoiam seu ciclo de vida. Isso posto, ao considerar que a proteção e privacidade de dados pessoais é um direito fundamental do cidadão, é evidente que a adaptabilidade da tecnologia às necessidades de proteção é essencial e vem sendo discutida e desenvolvida pela Ciência para proporcionar a proteção efetiva desses dados na amplitude e importância merecidas ao tema. Diante disso, é fundamental que organizações que tratam dados pessoais estejam munidas de tecnologia capaz de proteger esses dados satisfatoriamente e que sejam capazes de comprovar a aderência aos requisitos das normativas. Ao considerar que os artefatos a serem utilizados como evidências de conformidade com as normativas são produzidos pelo arcabouço tecnológico utilizado para proteger os dados e que o modelo a ser proposto sistematiza e organiza essas evidências com base em casos de garantia, o estudo proposto é relevante do ponto de vista tecnológico, visto que reunirá técnicas já consolidadas e utilizadas para assegurar os dados e abordagens aplicadas em outros contextos, com mais frequência no desenvolvimento de sistemas críticos (sistemas os quais uma falha pode acarretar em prejuízos, consequências catastróficas em ambientes ou até mesmo em perda de vidas humanas), em um modelo para gerenciamento das evidências de proteção e privacidade de dados.

Além do contexto tecno científico, no contexto social a Ciência tem impacto no cotidiano da humanidade, e são inúmeras as contribuições realizadas ao longo do tempo para o

estado atual. Rodríguez e Del Pino (2017, p. 2) ratificam a importância da Ciência no desenvolvimento das sociedades em diferentes campos de ação da humanidade, ao reforçarem que:

> [...] a atividade científica tem incrementado seu reconhecimento social, sendo idealizada como estratégia infalível para entender o mundo e nos aproximarmos à "verdade"; não é por acaso o uso da frase "comprovado cientificamente" cada vez que se quer confirmar que algo funciona realmente ou que de fato acontece.

Quanto às contribuições desta pesquisa no âmbito social, estas convergem em insumos para apoiar a gestão da proteção e privacidade de dados, beneficiando assim as partes que tratam dados pessoais e regulamentam as tratativas, assim como os titulares dos dados. No contexto das organizações, o modelo a ser proposto pretende apoiá-las na adequação e aderência às normativas de proteção e privacidade de dados e ser adotado como referência para o gerenciamento de evidências. Já os profissionais da área de proteção e privacidade de dados terão a oportunidade de adotar um modelo que objetiva garantir a qualidade e aceitação das evidências. No que se refere aos órgãos reguladores/certificadores e auditores, o modelo pretende proporcionar a padronização nas comprovações sobre o tratamento de dados pessoais. Quanto aos cidadãos, uma vez que a proteção e privacidade de dados pessoais é um direito do titular, pautado na transparência, o modelo propõe uma abordagem que pode ser utilizada na validação e comprovação de atendimento a esses direitos, que proporcionará a clareza e compreensão do tratamento em todas as operações de tratamento dos dados.

1.7 ADERÊNCIA DO TEMA DA PESQUISA AO PGCIN E À CIÊNCIA DA INFORMAÇÃO

Este estudo está sendo desenvolvido na linha de pesquisa "Informação, Gestão e Tecnologia" do Programa de Pós-Graduação em Ciência da Informação (PGCIN), da Universidade Federal de Santa Catarina, linha esta que se propõe a:

> Investigar os processos, ambientes, serviços, produtos e sistemas de gestão da informação e do conhecimento, por meio de abordagens interdisciplinares sobre o gerenciamento, produção, armazenamento, transmissão, acesso, segurança e avaliação de dados e informações existentes nos mais diversos meios, tendo em vista a sustentabilidade das organizações. Como suporte, aplica e desenvolve técnicas e tecnologias inteligentes e prospectivas. (UNIVERSIDADE FEDERAL DE SANTA CATARINA, 2019).

O tema deste trabalho de tese possui cunho interdisciplinar envolvendo predominantemente as áreas de Ciência da Computação e Direito. O tema "proteção e privacidade de dados" é abordado com frequência na área de Ciência da Computação no que se

refere a mecanismos, ferramentas e algoritmos seguros, que implementam requisitos do tema. Na área de Direito, o tema é abordado ao considerar as leis que regem a proteção e privacidade de dados.

Serão trazidos para este estudo cinco autores, os quais apresentam em suas definições acerca da Ciência da Informação as relações diretas com essa área e consequentemente com suas disciplinas. Para Borko (1968) a Ciência da Informação traz em seu cerne a interdisciplinaridade e está relacionada com a matemática, a linguística, a psicologia, a tecnologia de computação, a comunicação, a biblioteconomia, a administração, entre outras.

O autor complementa que:

> A Ciência da Informação é uma disciplina que investiga as propriedades e o comportamento informacional, as forças que governam os fluxos de informação, e os significados do processamento da informação, para uma acessibilidade e usabilidade ótima. Ela está preocupada com o corpo de conhecimento relacionado à origem, coleção, organização, armazenamento, recuperação, interpretação, transmissão, transformação, e utilização da informação. Isto inclui a investigação da representação da informação em ambos os sistemas, naturais e artificiais, o uso de códigos para a transmissão eficiente da mensagem, e o estudo do processamento de informações e de técnicas aplicadas aos computadores e seus sistemas de programação (BORKO, 1968, p. 3).

Queiroz e Moura (2015) ressaltam a relevância das definições de Borko para a Ciência da Informação, por ter abordado, no final de década de 1960, questões importantes que são estudadas pela Ciência da Informação até os dias atuais, como, por exemplo, o acesso à informação pelas pessoas e sua usabilidade. As autoras complementam que Borko, ao apontar a preocupação da Ciência da Informação com a origem, coleção, organização, armazenamento, recuperação, interpretação, transmissão, transformação e utilização da informação, declara o cunho interdisciplinar desta ciência e sua necessidade de usar teorias da Biblioteconomia, Comunicação, Informática, Psicologia, entre outras, e que há quase 50 anos o autor já visualizou o uso dos computadores e seus programas dentro da Ciência da Informação.

A percepção de Borko (1968) sobre a natureza interdisciplinar da Ciência da Informação se alinha à de Saracevic (1996), uma vez que para este último ela possui relação com: a Biblioteconomia, pois compartilha o seu papel social e sua preocupação com os problemas da efetiva utilização dos registros; a Ciência da Computação, uma vez que utiliza computadores e computação na recuperação e transformação da informação através de algoritmos, tratando da natureza da informação e da sua comunicação para ser utilizada pelos homens; a Ciência Cognitiva, pois é representada pela Inteligência Artificial, a qual contribui com inovações nos sistemas de informação, além de contribuir com modelos teóricos da cognição; e a Comunicação, pois compartilha interesse na comunicação humana, compreendendo a

informação como um fenômeno e a comunicação como um processo, ambas devendo ser estudadas em conjunto.

Apesar de não trazer explicitamente a questão da interdisciplinaridade, Capurro e Hjorland (2007) perpetuam a ideia de "[...] geração, coleta, organização, interpretação, armazenamento, recuperação, disseminação, transformação e uso da informação [...]" dentro da Ciência da Informação. Porém, por se tratar de um conceito mais recente, incorporam a ideia intrínseca da utilização de tecnologias modernas nessas atividades.

É possível encontrar na literatura diversos estudos dentro da área da Ciência da Computação que usufruem de conceitos originários da Ciência da Informação, assim como o contrário. Temas envolvendo Arquitetura da Informação, Web Semântica, Recuperação da Informação, Ontologias, Representação da Informação, Usabilidade, Segurança da Informação, entre outros, encontram na convergência entre as duas áreas soluções que cooperam com a ciência e com a sociedade como um todo. Cafezeiro, Costa e Kubrusly (2016) corroboram esse pensamento afirmando que a:

> [...] Ciência da Computação pode contribuir com a Ciência da Informação no sentido de oferecer mecanismos automatizados para o armazenamento, manuseio e recuperação da informação, e que inversamente, a Ciência da Informação pode contribuir com a computação no sentido de propor modelos de representação da informação que possibilitem um arranjo lógico mais elaborado sobre o qual os sistemas computacionais possam agir. [...] O que enfatiza a possibilidade de um modelo de coprodução, em que as ciências colaboram na conformação dos conceitos que as fundamentam. É um modelo de interdisciplinaridade porque confraterniza traduções provenientes de ambas as disciplinas sobre um objeto compartilhado por ambas, nesse caso, a informação [...]. (CAFEZEIRO; COSTA; KUBRUSLY, 2016, p. 130).

Para Alves *et al.* (2007), a Ciência da Computação fornece o meio, as ferramentas tecnológicas para o desenvolvimento de ambientes para acesso, transmissão, recuperação, armazenamento e transformação da informação, ao passo que a Ciência da Informação fornece os métodos, técnicas e ferramentas para o tratamento das informações nos documentos disponíveis e utiliza as aplicações tecnológicas em seu fazer.

Durante o percurso histórico, pode ser observado que, desde a origem da Ciência da Informação, muitos processos da Ciência da Computação foram incorporados por essa ciência em seus respectivos tempos. Direta ou indiretamente, as tecnologias de informação foram utilizadas para o desenvolvimento de pesquisas envolvendo todo o ciclo de vida dos dados, contribuindo, assim, para o desenvolvimento tanto da área de Ciência da Informação como da Ciência da Computação (FREUND; SEMBAY; MACEDO, 2019).

Tendo em vista que a segurança da informação e a proteção de dados sempre estiveram atreladas ao uso das tecnologias vigentes, bem como com as ferramentas e TICs da área de Ciência da Computação, propõe-se investigar sob o prisma pelo qual a Ciência da Informação percebe os problemas relacionados à proteção e privacidade dos dados, bem como as formas e métodos de trabalho realizados no tratamento da informação, para apoiar no desafio de comprovar conformidade com normativas de proteção à privacidade de dados.

Nessa visão, pode-se considerar que este projeto permeia essas ciências, uma vez que as abordagens a serem definidas farão com que métodos e ferramentas associados a elas atuem em conjunto com o objetivo de garantir proteção e privacidade dos dados e comprovar alegações sobre o tema nos mais variados tipos de ambientes informacionais. Esta pesquisa estabelece conexão também com a área do Direito, uma vez que pretende adotar abordagens para modelar evidências de forma que possam ser utilizadas para demonstrar conformidade com normativas de proteção e privacidade de dados alinhadas conceitualmente com leis dessa temática.

A citada interdisciplinaridade com a área de Direto não é abordada explicitamente pelos autores apresentados, porém, no entendimento de Braman (2009, p. 2), a prática da lei vem acompanhando as mudanças empíricas e se relacionando com diferentes temas dessa evolução. Para a autora, desde o século XVIII, "o ambiente jurídico da informação e da comunicação tem estado sob constante reconsideração desde que foi reconhecido como fundamental para as novas formas de governação democrática". Em relação a esse item destaca-se o resultado de uma pesquisa realizada por esta pesquisadora, na disciplina de Epistemologia da Ciência da Informação que compõe este programa de pós-graduação. Essa pesquisa envolveu uma análise das publicações na base *Web of Science*, buscando identificar as relações existentes entre a Segurança da Informação/Privacidade de Dados e a Ciência da Informação e compreender os temas precursores da temática no contexto epistemológico da Ciência da Informação, ou seja, os fundamentos epistemológicos que permitem abordar a Segurança da Informação/Privacidade de Dados no campo da Ciência da Informação, estabelecendo um diálogo entre elas, além de compreender o domínio dessa conexão. O estudo foi organizado por décadas, iniciando no ano de 1970, e para as buscas foram utilizadas as palavras "*information security*" e "*data protection*".

A partir dos resultados constatou-se que, apesar da diversidade de temas ter aumentado ao longo do tempo, a Ciência da Informação incorporou essas temáticas principalmente nos domínios gerenciais, culturais e legais, estabelecendo entre elas um diálogo que compartilha a informação como o principal objeto de estudo. Vale ressaltar que no domínio legal supracitado

identificou-se que o fator impulsionador foi a disponibilização e atualizações de leis de proteção de dados em âmbito mundial.

Diante do exposto, entende-se que são temáticas aderentes à Ciência da Informação e importantes de serem investigadas, pois contribuirão para o avanço desta ciência.

1.8 ESTRUTURA DO TRABALHO

O presente documento está dividido em sete seções. Nesta primeira seção foi apresentada a Introdução, a motivação e justificativa para a pesquisa, sua hipótese e a questão de pesquisa, os objetivos (geral e específicos), a delimitação do escopo da pesquisa, o ineditismo e a aderência do tema da pesquisa ao PGCIN e à Ciência da Informação.

Na segunda seção é contemplado o referencial teórico utilizado, em que são abordados: proteção e privacidade de dados; conceitos gerais, normativas de proteção e privacidade de dados, ABNT NBR ISO/IEC 29100:2020 – Tecnologia da informação – Técnicas de segurança – Estrutura de Privacidade; ISO/IEC 29101 – Information Technology – Security Techniques – Privacy Architecture Framework; ABNT NBR ISO/IEC 27701:2019 – Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes, detalhamento; ABNT NBR ISO/IEC 29100:2020 – Tecnologia da informação – Técnicas de segurança – Estrutura de privacidade, leis de proteção e privacidade de dados (*General Data Protection Regulation* – GDPR e Lei Geral de Proteção de Dados – LGPD); gerenciamento de evidências e casos de garantia.

Na terceira seção é apresentado o detalhamento da RSL realizada, o protocolo utilizado, seus resultados e uma síntese dos trabalhos considerados relacionados com a proposta em foco, evidenciando a sua originalidade, bem como o seu ineditismo.

Na quarta seção são abordados os aspectos metodológicos relacionados ao desenvolvimento da pesquisa, especificando sua caracterização e detalhando o percurso metodológico que se pretende implementar para o alcance dos objetivos.

Na quinta seção é apresentado o modelo para o gerenciamento de evidências de proteção e privacidade de dados, suas camadas, seus instrumentos de apoio, o cenário de aplicação da experimentação e o método utilizado para aplicação do modelo.

Na sexta seção é evidenciada a avaliação do modelo com a pesquisa com os especialistas e na sétima seção são apresentadas as conclusões. E, por fim, são listadas as referências utilizadas nesta tese, além dos apêndices.

2 REFERENCIAL TEÓRICO

Visando ampliar a compreensão sobre as temáticas abordadas nesta pesquisa, nesta seção serão tratados os seguintes assuntos: proteção e privacidade de dados – conceitos gerais, normativas de proteção e privacidade de dados, ABNT NBR ISO/IEC 29100:2020 – Tecnologia da informação – Técnicas de segurança – Estrutura de Privacidade, ISO/IEC 29101 – Information Technology – Security Techniques – Privacy Architecture Framework, ABNT NBR ISO/IEC 27701:2019 – Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes, Detalhamento ABNT NBR ISO/IEC 29100:2020 – Tecnologia da informação – Técnicas de segurança – Estrutura de privacidade, leis de proteção e privacidade de dados, *General Data Protection Regulation* (GDPR) e Lei Geral de Proteção de Dados (LGPD), *Privacy by Design*, Gerenciamento de evidências e Casos de garantia.

2.1 PROTEÇÃO E PRIVACIDADE DE DADOS – CONCEITOS GERAIS

Privacidade é um assunto que vem sendo discutido ao longo do tempo e tendo seu significado adaptado a cada época (BAASE, 2008). Atualmente, existe uma relação evidente entre a privacidade e o desenvolvimento da tecnologia, porém a temática teve suas origens nas sociedades antigas com sentidos distintos ao que se tem agora.

Dentre as publicações que discutem sobre o tema da privacidade, o artigo publicado em 1890, na Harvard Law Review, pelos advogados Samuel Warren e Louis Brandeis, com o título "O direto à privacidade", é citado como referência. No entendimento de Luckas (2017), esses autores foram os primeiros a reconhecer as ameaças à privacidade, causadas pela tecnologia e pelo desenvolvimento social. Essa obra refere-se à privacidade como o direito de ser deixado em paz. Os autores Warren e Brandeis abordam o tema considerando o rumo sensacionalista que os jornais estavam tomando na época, com a divulgação excessiva de escândalos e fofocas sobre a vida das pessoas e a nova tecnologia recém disponibilizada: as câmeras fotográficas, que possibilitaram que fotos espontâneas fossem tiradas de pessoas em locais públicos (WARREN; BRANDEIS, 1970).

O livro "Privacidade e Liberdade", publicado por Alan Westin, em 1967, também é um marco na trajetória das discussões sobre o tema. Essa obra define a privacidade em termos de autoafirmação, como uma reivindicação do indivíduo em determinar quando, como e quais informações sobre ele são comunicadas a outros (WESTIN, 2003).

Na compreensão de Holvats (2009), a proteção à privacidade é passiva, influenciada pelo governo por meio das leis e pela indústria com as leis e as autorregulamentações, as quais definem o caminho e o nível de proteção a ser adotado. Neste quesito é importante considerar que o governo, as leis e a indústria possuem um papel relevante, porém, dentre eles as leis influenciam nessa tratativa com maior vigor, interferindo nas questões culturais das localidades. Entende-se que países que possuem legislações de privacidade instituídas há mais tempo possuem uma cultura de privacidade mais desenvolvida.

Desde 1960, a relação entre a privacidade e o uso de dados vem se estreitando devido ao surgimento da Internet, à contemporaneidade da tecnologia da informação e, com isso, à troca de dados entre fronteiras, porém de forma distinta entre países com diferentes culturas. Nesse sentido, algumas iniciativas foram relevantes, as quais contribuíram com modelos, normativas e leis que tratam da proteção e privacidade dos dados atualmente. Dentre elas destacam-se as diretrizes desenvolvidas em 1980 pela Organização de Cooperação e Desenvolvimento Econômico (OCDE), que se basearam nas práticas adotadas pelo Departamento de Saúde, Educação e Bem-Estar (HEW) dos Estados Unidos, no relatório publicado em 1973 (ORGANIZAÇÃO DE COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO, 2013).

Solove (2006) destaca os oito princípios de privacidade definidos pela OCDE, sendo eles:

1 – Limitação da coleta: os dados devem ser coletados legalmente com o consentimento do indivíduo;

2 – Qualidade dos dados: os dados devem ser precisos e relevantes para uma finalidade específica;

3 – Especificação da finalidade: a finalidade da coleta de dados deve ser declarada no momento da coleta de dados e o uso dos dados deve ser limitado a esse objetivo;

4 – Limitação de uso: os dados não devem ser divulgados para diferentes fins sem o consentimento do indivíduo;

5 – Salvaguardas de segurança: os dados devem ser protegidos;

6 – Princípio da abertura: os indivíduos devem ser informados sobre as práticas e políticas daqueles que lidam com seus dados;

7 – Participação individual: as pessoas devem ter conhecimento sobre os dados que uma entidade possui sobre elas e poder corrigir erros ou problemas nesses dados;

8 – Responsabilidade: as entidades que controlam as informações pessoais devem ser responsabilizadas pela execução desses princípios.

Outra iniciativa importante nessa temática foi a Diretiva 95/46, de 1995. Esta Diretiva define os papéis envolvidos no processamento dos dados e apresenta princípios de privacidade relacionados a: Qualidade dos dados; Legitimidade do processamento dos dados; Garantias básicas ao titular dos dados (tais como de ser informado, de acesso e correção dos dados, de objeção, de optar por não ser submetido a processos de decisão automatizados); Segurança e confidencialidade dos dados. A Diretiva apresenta também as sanções a serem aplicadas no caso de descumprimento, entre outros itens que foram incorporados pelas leis vigentes atualmente em diversos países (DIRECTIVE 95/46/EC, 1995).

Por sua vez, as normativas referentes à segurança da informação, proteção e privacidade de dados estabelecem diretrizes para a implementação dos princípios e são instrumentos importantes a serem considerados no contexto dessas temáticas, sendo este o conteúdo abordado na próxima subseção.

2.2 NORMATIVAS DE PROTEÇÃO E PRIVACIDADE DE DADOS

O tema da proteção e privacidade de dados é regulamentado por leis que demandam implementação de medidas e controles e demais adequações para serem cumpridas. Normativas podem ser adotadas para apoiar nesta tarefa, visto que, enquanto as leis apresentam descrições generalistas dos princípios a serem adotados e demais definições, as normativas apresentam diretrizes de implementação e seus controles, de maneira detalhada e de fácil compreensão. Além disso, elas estabelecem os requisitos para o processo de certificação de produtos, serviços ou ambientes, caso seja requerido posteriormente.

Na próxima subseção são apresentadas as normas ISO 29100, ISO 29101 e ISO 27701 e seu escopo de aplicabilidade.

2.2.1 ABNT NBR ISO/IEC 29100:2020 – Tecnologia da informação – Técnicas de segurança – Estrutura de Privacidade

A ABNT NBR ISO/IEC 29100 é uma adoção idêntica, em conteúdo técnico, estrutura e redação, à ISO/IEC 29100:2011 + Amd.1:2018, elaborada pelo Technical Committee Information Technology (ISO/IEC JTC 1). Essa norma destina-se a aprimorar normas de segurança já existentes, porém com foco no tratamento de dados pessoais. Sua estrutura visa apoiar organizações a estabelecerem requisitos de salvaguarda de dados pessoais em ambientes de TIC e tem como objetivos: a) especificar uma terminologia comum de privacidade; b)

caracterizar atores e os seus papéis no tratamento de Dados Pessoais (DP); c) descrever os requisitos de salvaguarda da privacidade; e d) referenciar princípios conhecidos de privacidade. Devido às diferentes tecnologias existentes que processam dados pessoais, a ISO 29100 fornece uma base de entendimento comum para a proteção de dados pessoais, além de prover uma estrutura de alto nível para a proteção desses dados dentro de sistemas de tecnologia da informação e de comunicação (TIC) (ABNT NBR ISO/IEC 29100, 2011). Com isso, a norma se propõe a: ajudar no desenho, implementação, operação e manutenção de sistemas de TIC que tratem e protejam DP; incentivar soluções inovadoras que possibilitem a proteção de DP dentro dos sistemas de TIC; e melhorar os programas de privacidade nas organizações por meio do uso das melhores práticas. Esta norma é detalhada na subseção 2.2.4 por ser a normativa de referência para o desenvolvimento desta pesquisa.

2.2.2 ISO/IEC 29101 – Information technology – Security techniques – Privacy Architecture Framework

Trata-se de um padrão internacional, elaborado com base na ISO/IEC 29100, que apresenta uma arquitetura e boas práticas para a implementação dos requisitos de privacidade em sistemas de TIC que tratam dados pessoais. É aplicável a entidades envolvidas na especificação, aquisição, arquitetura, *design*, teste, manutenção, administração e operação de sistemas de TIC que processam dados pessoais. Essa norma apresenta uma estrutura que: a) especifica as preocupações com os sistemas de TIC que processam dados pessoais; b) lista componentes para a implementação de tais sistemas; e c) fornece visualizações de arquitetura contextualizando esses componentes (ISO/IEC 29101, 2013).

2.2.3 ABNT NBR ISO/IEC 27701:2019 – Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes

A ABNT NBR ISO/IEC 27701 é uma adoção idêntica, em conteúdo técnico, estrutura e redação, à ISO/IEC 27701:2019, que foi elaborada pelo Technical Committee Information Technology (ISO/IEC JTC 1), Subcommittee Information Security, Cybersecurity and Privacy Protection (SC 27). Essa norma especifica os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação (SGPI), na forma de uma extensão da ABNT NBR ISO/IEC 27001

e da ABNT NBR ISO/IEC 27002, para a gestão da privacidade dentro do contexto de uma organização. Especifica os requisitos relacionados a um sistema de gestão de privacidade de dados e fornece orientações para controladores e operadores responsáveis pelo tratamento de dados pessoais. A norma é aplicável a todos os tipos e tamanhos de organizações, sendo elas públicas e privadas, entidades governamentais e organizações sem fins lucrativos que sejam controladoras ou operadoras de dados pessoais (ISO/IEC 27701, 2019).

2.2.4 Detalhamento ABNT NBR ISO/IEC 29100 – 2020 – Tecnologia da informação – Técnicas de segurança – Estrutura de Privacidade

Conforme abordado anteriormente, na medida em que as discussões sobre privacidade de dados evoluíram e a manipulação dos dados se pluralizou movida pelo avanço tecnológico, diversas iniciativas ao redor do mundo foram encaminhadas para tratar sobre o tema. Para este trabalho buscou-se identificar uma referência normativa que apresentasse uma estrutura para a proteção de dados com base em conceitos alinhados mundialmente, que pudessem ser aplicados em conjunto com diferentes legislações, e que não determinasse características referentes às soluções tecnológicas utilizadas. A ISO 29100 traz essas características e reforça que, devido ao crescente número de tecnologias que processam dados pessoais, é importante ter normas de segurança da informação que forneçam uma base de entendimento comum para a proteção dos dados pessoais. A norma acrescenta que, devido à complexidade dos sistemas de TIC e às diferentes jurisdições legais existentes, assegurar a privacidade e estar conforme com as diversas leis pode ser uma tarefa difícil para as organizações. Sendo assim, a ISO 29100 é a normativa de referência adotada para esta pesquisa, e nesta subseção é apresentado seu detalhamento, sendo ele extraído diretamente da norma, em sua totalidade. O conteúdo apresentado a seguir traz partes da norma em uma tentativa de apresentar um resumo dos pontos mais relevantes a serem abordados e ser fiel ao que ela prescreve.

Dentre seus objetivos, a ISO 29100 se propõe a apoiar o desenho, implementação, operação e manutenção de sistemas de TIC no tratamento e proteção de dados pessoais e incentivar soluções inovadoras para proteger dados pessoais nos sistemas de TIC, padronizando a privacidade e fornecendo base para: a) uma arquitetura técnica de referência; b) implementação e uso de tecnologias específicas de privacidade; e c) a gestão geral de privacidade e especificações de engenharias específicas.

A norma ISO 29100 está organizada nos seguintes itens: i) Escopo; ii) Termos e definições; iii) Símbolos e termos abreviados; iv) Elementos básicos da estrutura de

privacidade; v) Os princípios de privacidade; vi) Anexo A – Correspondência entre os conceitos da ABNT NBR ISO/IEC 29100 e os conceitos da ISO/IEC 27000.

No que se refere ao seu escopo, a ISO 29100 é aplicável às pessoas naturais e organizações envolvidas na especificação, aquisição, arquitetura, concepção, desenvolvimento, teste, manutenção, administração e operação de sistemas de tecnologia da informação e comunicação ou serviços em que controles de privacidade são necessários para o tratamento de DP (ABNT NBR ISO/IEC 29100, 2020, p. 1).

A ISO 29100 aborda em seu conteúdo componentes como: a) Atores e seus papéis; b) Interações; c) Reconhecimento de DP; d) Requisitos de salvaguarda de privacidade; e) Políticas de privacidade; e f) Controles de privacidade, os quais são abordados a seguir.

a) Atores e seus papéis

Os atores envolvidos no tratamento de DP, segundo a ISO 29100, são: titulares, controladores, operadores e terceiros. Os titulares são os atores que fornecem os seus DP para tratamento pelos controladores e operadores e que determinam suas preferências para o tratamento de seus dados. Os controladores dos DP são os atores que determinam os propósitos e os meios pelos quais o tratamento dos DP ocorrerá. Os operadores dos DP realizam o tratamento dos DP (em nome do controlador ou conforme suas instruções). Os operadores observam os requisitos de privacidade estipulados pelo controlador e implementam os controles correspondentes para seu atendimento. Já os terceiros podem receber DP de um controlador ou de um operador e se tornar controladores de DP ao recebê-los.

b) Interações

As interações referem-se aos possíveis fluxos dos DP que podem existir entre os atores apresentados anteriormente em diferentes cenários. A ISO 29100 apresenta oito cenários possíveis, conforme listados a seguir:

> Cenário A - o titular de DP fornece DP para um controlador de DP (por exemplo, ao se registrar em um serviço prestado pelo controlador de DP).
>
> Cenário B - o controlador de DP fornece DP para um operador de DP, que realiza o tratamento de DP em nome do controlador de DP (por exemplo, como parte de um contrato de terceirização).

Cenário C - o titular de DP fornece DP para um operador de DP, que realiza o tratamento de DP em nome do controlador de DP.

Cenário D - o controlador de DP fornece ao titular de DP os DP que são relacionados ao titular de DP (por exemplo, respondendo a uma requisição feita pelo titular de DP).

Cenário E - o operador de DP fornece DP ao titular de DP (por exemplo, conforme indicado pelo controlador de DP).

Cenário F - o operador de DP fornece DP para o controlador de DP (por exemplo, depois de ter realizado o serviço para o qual foi designado).

Cenário G - o controlador de DP fornece DP para um terceiro (por exemplo, no contexto de um acordo comercial).

Cenário H - o operador de DP fornece DP para um terceiro (por exemplo, conforme indicado pelo controlador de DP).

O Quadro 1 apresenta os fluxos de DP possíveis entre o titular, o controlador, o operador e terceiros conforme a norma.

Quadro 1 - Fluxo de Dados Pessoais (DP)

	Titular do DP	**Controlador de DP**	**Operador de DP**	**Terceiro**
Cenário a)	Provedor de DP	Receptor de DP	-	-
Cenário b)	-	Provedor de DP	Receptor de DP	-
Cenário c)	Provedor de DP	-	Receptor de DP	-
Cenário d)	Receptor de DP	Provedor de DP	-	-
Cenário e)	Receptor de DP	-	Provedor de DP	-
Cenário f)	-	Receptor de DP	Provedor de DP	-
Cenário g)	-	Provedor de DP	-	Receptor de DP
Cenário h)	-	-	Provedor de DP	Receptor de DP

Fonte: NBR ISO/IEC 29100 (2011).

c) Reconhecimento de DP

Neste item, a norma apresenta os fatores a serem considerados para determinar se um dado é ou não um DP (identificável ou que identifica um titular). A norma recomenda que os sistemas de TIC possuam mecanismos para identificar um DP e controles apropriados para o seu compartilhamento. Em alguns casos, a identificabilidade do titular do DP é muito clara, como por exemplo: CPF, número de passaporte, conta bancária. Ou pode haver um dado identificador que pode estabelecer uma comunicação com o titular, como, por exemplo, um

número de telefone, localização geográfica, e há ainda casos em que determinados dados são relacionados entre si de modo a identificar o titular.

A norma apresenta outras características a serem consideradas que classificam dados como DP, a exemplo de dados biométricos, e complementa que "qualquer atributo que assuma um valor que identifique exclusivamente um titular de DP é considerado uma característica distintiva", mas que existem também situações nas quais uma pessoa natural é identificável mesmo se não existirem atributos simples que a identifiquem unicamente, como é o caso de combinações de atributos em um determinado domínio. Para exemplificar esses casos, a norma apresenta que a combinação dos atributos "feminino", "45" e "advogado" aplicada em uma companhia pode ser suficiente para identificar uma pessoa específica, porém será insuficiente para identificar uma pessoa natural fora deste domínio.

d) Dados pseudoanonimizados

Pseudônimos podem ser utilizados para restringir a capacidade de identificação de DP por controladores ou por operadores. A norma apresenta que para a substituição ser considerada uma pseudoanonimização é necessário que os atributos restantes ligados ao pseudônimo não sejam suficientes para identificar o titular de DP a quem eles se relacionam e que a atribuição de pseudônimo ocorra de forma que não seja possível ser revertida por esforços razoáveis das partes interessadas na privacidade, exceto por aquela que a realizou.

A norma explica que os processos de anonimização e de pseudoanonimização são diferentes, visto que na anonimização os DP são apagados e substituídos de maneira irreversível e não possuem a capacidade de vincular demais dados ao mesmo pseudônimo, dessa forma, dados anonimizados não são mais considerados DP. Já na pseudoanonimização, diferentes dados vinculados ao titular do DP podem ser associados a um determinado pseudônimo, e a norma ressalta que quanto maior o conjunto de dados associado a um determinado pseudônimo, maior é o risco de violação da privacidade.

e) Metadados

A norma coloca que DP podem ser armazenados em um sistema de TIC em metadados, porém recomenda que esse tipo de tratamento, assim como a finalidade, seja de conhecimento do titular do DP.

f) DP não solicitados

DP não solicitados, ou seja, aqueles obtidos de forma não intencional, podem ser armazenados em um sistema de TIC, porém a norma recomenda a aplicação do conceito de *Privacy by Design* no projeto do sistema de forma a reduzir o risco da coleta de DP não solicitados.

g) DP sensíveis

A norma define DP sensíveis como aqueles que se relacionam à esfera mais íntima do titular do DP ou que podem ter um impacto significativo sobre ele. Esta classificação de DP se estende a todos os DP que podem ser derivados dos DP sensíveis, ou seja, aqueles que, mesmo não contendo informações diretas sobre os DP sensíveis, possam inferir sobre essas informações. Para essa classificação de DP a norma recomenda a adoção de precauções especiais e ressalta a importância de observar as jurisdições aplicáveis, que podem desde proibir o tratamento desses dados até definir os controles específicos a serem adotados.

h) Requisitos de salvaguarda de privacidade

Esta seção da norma é destinada a apresentar os requisitos de salvaguarda de privacidade de DP e ressalta que eles estão relacionados a diferentes estágios dos dados (coleta e retenção; transferência para terceiros; relação contratual entre controlador e operador; transferência internacional etc.). Esses requisitos podem ser de natureza geral ou específica e podem envolver restrições muito específicas ao processar certos tipos de DP ou até mesmo exigir a implementação de controles específicos de privacidade, conforme o cenário. A norma recomenda que sistemas de TIC novos ou substancialmente modificados sejam precedidos por uma identificação dos requisitos de salvaguarda de privacidade pertinentes e indica que avaliações de impacto de privacidade relacionadas aos sistemas de TIC sejam inseridas como parte da estrutura de gestão de riscos de uma organização. Acrescenta que a gestão de riscos de privacidade deve ser influenciada pelos seguintes fatores: fatores legais e regulatórios, fatores contratuais, fatores de negócio e demais fatores que possam afetar o projeto de sistemas de TIC e os requisitos de salvaguarda de privacidade associados.

i) Políticas de privacidade

É recomendado pela norma que a organização documente sua política de privacidade, contemplando as regras e obrigações detalhadas das diferentes partes envolvidas no tratamento de DP, e que a política de privacidade contemple os seguintes requisitos: seja apropriada ao objetivo da organização; forneça a estrutura para a determinação de objetivos; inclua um compromisso em satisfazer os requisitos aplicáveis de salvaguarda da privacidade; inclua um compromisso com a melhoria contínua; seja comunicada dentro da organização; e esteja disponível para as partes interessadas, de forma apropriada.

j) Controle de privacidade

Controles de privacidade devem ser implementados pelas organizações para atender aos requisitos de proteção de privacidade identificados na avaliação e tratamento de riscos de privacidade. A norma destaca a importância de observar que nem todo tratamento de DP requer o mesmo nível e tipo de proteção. Dessa forma, é necessário distinguir as operações de tratamento de DP de acordo com os riscos identificados para determinar os controles de segurança apropriados para cada situação.

k) Os princípios de privacidade

A ISO 29100 apresenta 11 princípios de privacidade que foram derivados de princípios desenvolvidos por vários países e organizações internacionais. A estrutura apresentada pela ISO 29100 se concentra na implementação dos princípios de privacidade em sistemas de TIC e no desenvolvimento de rotinas de gestão de privacidade a serem implementadas nesses sistemas. Esta norma apresenta como base os seguintes princípios:

1. Consentimento e escolha;
2. Legitimidade e especificação de objetivo;
3. Limitação de coleta;
4. Minimização de dados;
5. Uso, retenção e limitação da divulgação;
6. Precisão e qualidade;
7. Abertura, transparência e notificação;
8. Participação individual e acesso;

9. Responsabilização;
10. Segurança da informação;
11. *Compliance* com a privacidade.

1. Consentimento e escolha

O objetivo deste princípio é possibilitar ao titular de DP o fornecimento e a retirada do consentimento de forma facilitada e sem ônus, além da escolha de como os seus DP serão tratados. Para estar aderente ao princípio do consentimento é necessário:

a) Apresentar ao titular de DP a escolha de permitir ou não o tratamento de seus DP, exceto quando o titular de DP não puder livremente reter o consentimento ou onde a legislação aplicável permitir especificamente o tratamento de DP sem o consentimento da pessoa natural. A escolha do titular de DP deve ser dada livremente, específica e com conhecimento;

b) Obter o consentimento *opt-in* de aceitação do titular de DP para coletar ou processar os DP sensíveis, exceto onde a lei aplicável permitir o processamento de DP sensível sem o consentimento da pessoa natural;

c) Informar aos titulares de DP, antes de obter o consentimento, sobre os seus direitos sob o princípio de participação e acesso individual;

d) Fornecer aos titulares de DP, antes da obtenção do consentimento, as informações indicadas pelo princípio da abertura, transparência e notificação; e

e) Explicar aos titulares de DP as implicações da concessão ou retenção do consentimento.

Além disso, deve ser disponibilizada ao titular de DP a escolha de como seus DP são tratados e permitir que o mesmo retire o consentimento caso desejar, com facilidade e sem ônus.

2. Especificação e legitimidade de objetivo

Para estar aderente ao princípio da legitimidade de objetivo é necessário:

a) Assegurar que o(s) objetivo(s) esteja(m) em conformidade com a legislação aplicável e conte(m) com uma base jurídica permissível;

b) Comunicar o(s) objetivo(s) ao titular de DP antes da coleta ou o primeiro uso da informação para um novo objetivo;

c) Usar linguagem para esta especificação que seja clara e apropriadamente adaptada às circunstâncias; e

d) Se aplicável, dar explicações suficientes para a necessidade de tratar os DP sensíveis.

3. Limitação de coleta

A limitação da coleta está relacionada ao propósito de seu uso, ou seja, a norma recomenda que as organizações coletem os DP necessários para cumprir o(s) objetivo(s) especificado(s) pelo controlador e que seja documentado o tipo de DP coletado e a justificativa da coleta nas políticas e práticas de manuseio de informações.

Para estar aderente ao princípio de limitação da coleta é necessário limitar a coleta de DP àquilo que está dentro dos limites da lei aplicável e estritamente necessário para o(s) objetivos(s) especificado(s).

4. Minimização dos dados

Este princípio está diretamente relacionado ao princípio da limitação da coleta. Se por um lado a limitação da coleta refere-se à obtenção de dados restrita à finalidade especificada, a minimização dos dados refere-se ao tratamento estritamente necessário dos DP.

Para estar aderente ao princípio da minimização dos dados é necessário conceber e implementar procedimentos e sistemas de TIC de forma a:

a) Minimizar o número de partes interessadas e pessoas a quem são divulgados os DP ou que têm permissão para tratá-los;

b) Assegurar a adoção do princípio de "necessidade de conhecer" (ou seja, convém que seja permitido tratar apenas os DP necessários para o desempenho de funções oficiais, no âmbito do objetivo legítimo do tratamento de DP);

c) Usar ou oferecer como opções-padrão, sempre que possível, interações e transações que não envolvam a identificação de titulares de DP, reduzam a observabilidade de seus comportamentos e limitem a vinculação de DP coletados; e

d) De modo seguro, descartar os DP quando o objetivo para o tratamento dos DP tiver expirado, e quando não houver requisitos legais para mantê-los.

5. Uso, retenção e limitação da divulgação

Para estar aderente ao princípio de uso, retenção e limitação da divulgação é necessário:

a) Limitar o uso, retenção e divulgação (incluindo a transferência) de DP ao que é

necessário para cumprir objetivos específicos, explícitos e legítimos;

b) Limitar o uso de DP aos objetivos especificados pelo controlador de DP antes da coleta, a menos que um objetivo diferente seja explicitamente exigido pela lei aplicável;

c) Reter os DP somente pelo tempo necessário para cumprir os objetivos declarados e, posteriormente, destruí-los ou anonimizá-los com segurança; e

d) Bloquear (ou seja, arquivar, proteger e isentar de tratamento adicional) qualquer DP quando e por quanto tempo as finalidades estabelecidas tiverem expirado, seguindo a leis aplicáveis quanto à retenção do DP.

6. Precisão e qualidade

Este princípio refere-se à precisão e confiabilidade dos dados, e para estar aderente a esse princípio é necessário:

a) Assegurar que os DP tratados sejam precisos, completos, atualizados (a menos que haja uma base legítima para mantê-los desatualizados), adequados e pertinentes para o objetivo de uso;

b) Assegurar a confiabilidade dos DP recolhidos a partir de uma fonte que não seja o titular de DP antes de ser tratado;

c) Verificar, por meios apropriados, a validade e a exatidão das reivindicações feitas pelo titular de DP antes de fazer qualquer alteração nos DP (a fim de assegurar que as alterações sejam devidamente autorizadas), quando for apropriado fazê-lo;

d) Estabelecer procedimentos de coleta de DP para ajudar a garantir a precisão e a qualidade; e

e) Estabelecer mecanismos de controle para verificar periodicamente a precisão e a qualidade dos DP coletados e armazenados.

7. Abertura, transparência e notificação

O princípio da abertura, transparência e notificação está relacionado à disponibilização de informações completas ao titular do DP sobre o tratamento de seu dado. Para atender este princípio é necessário:

a) Fornecer aos titulares de DP informações claras e de fácil acesso sobre as políticas, procedimentos e práticas do controlador de DP em relação ao tratamento de DP;

b) Incluir em notificações o tratamento que está sendo dado ao DP, o objetivo para o

qual isto é feito, os tipos de partes interessadas na privacidade, a quem os DP podem ser divulgados e a identidade do controlador de DP, incluindo informações sobre como entrar em contato com o controlador de DP;

c) Divulgar as escolhas e os meios oferecidos pelo controlador de DP aos titulares de DP para fins de limitação do tratamento e acesso, correção e remoção de suas informações; e

d) Notificar os titulares de DP quando ocorrerem mudanças importantes nos procedimentos de tratamento de DP.

Além disso, a norma recomenda que o propósito do tratamento dos DP seja detalhado o suficiente ao titular de tal forma que compreenda: quais DP são requeridos para o objetivo especificado; o objetivo especificado para a coleta de DP; o tratamento especificado (incluindo mecanismos de coleta, comunicação e armazenamento); os tipos de pessoas naturais autorizadas que terão acesso aos DP e para quem os DP podem ser transferidos; e os requisitos de retenção e descarte de DP especificados.

8. Participação individual e acesso

Este princípio trata sobre o direito do titular de DP à edição de seus dados de forma rápida e simplificada e da garantia aos titulares de DP quanto ao acesso apenas aos dados que lhes pertencem. Para estar aderente a esse princípio é necessário:

a) Dar aos titulares de DP a capacidade de acessar e analisar criticamente os seus DP, desde que a sua identidade seja primeiramente autenticada com um nível apropriado de garantia e tal acesso não seja proibido pela lei aplicável;

b) Permitir que os responsáveis pelos DP questionem a exatidão e a integridade dos DP e que estes sejam aperfeiçoados, corrigidos ou removidos conforme apropriado e possível no contexto específico;

c) Fornecer qualquer emenda, correção ou remoção aos operadores de DP e terceiros para os quais os DP foram divulgados, quando eles são conhecidos; e

d) Estabelecer procedimentos para permitir que os titulares de DP exerçam estes direitos de forma simples, rápida e eficiente, o que não implica atrasos ou custos indevidos.

9. Responsabilização

O princípio da responsabilização implica no dever de zelar e adotar medidas concretas e práticas para a proteção no tratamento dos DP. Para isso é necessário:

a) Documentar e comunicar oportunamente todas as políticas, procedimentos e boas práticas relacionadas à privacidade;

b) Atribuir a um indivíduo específico dentro da organização (podendo ser delegada a outros da organização, conforme apropriado) a tarefa de implementar as políticas, procedimentos e boas práticas relacionadas à privacidade;

c) Ao transferir os DP para terceiros, garantir que o terceiro destinatário seja obrigado a fornecer um nível equivalente de proteção da privacidade por meios contratuais ou outros, como políticas mandatórias internas (a lei aplicável pode conter requisitos adicionais relativos a transferências de dados internacionais);

d) Fornecer treinamento adequado para o pessoal do controlador de DP que terá acesso aos DP;

e) Estabelecer procedimentos internos eficientes de tratamento de reclamações e de recurso para uso pelos responsáveis pelos DP;

f) Informar os titulares de DP sobre violações de privacidade que possam causar danos substanciais a eles (a menos que seja proibido, por exemplo, enquanto se trabalha com a aplicação da lei), bem como as medidas tomadas para a resolução;

g) Notificar todas as partes interessadas pertinentes sobre a violação de privacidade, conforme exigido em algumas jurisdições (por exemplo, as autoridades de proteção de dados) e dependendo do nível de risco;

h) Permitir que um titular de DP prejudicado tenha acesso a sanções e/ou recursos adequados e eficazes, como retificação, expurgo ou restituição, se uma violação de privacidade ocorrer; e

i) Considerar procedimentos para compensação de situações em que será difícil ou impossível recuperar o status de privacidade da pessoa natural de volta a uma posição como se nada tivesse ocorrido.

10. Segurança da Informação

O princípio da segurança da informação refere-se à adoção de medidas de segurança pertinentes e satisfatórias de proteção no tratamento dos DP. Para estar aderente a este princípio é necessário:

a) Proteger os DP sob sua tutela com controles apropriados nos níveis operacional, funcional e estratégico, para assegurar a integridade, confidencialidade e disponibilidade dos

DP, e proteger contra riscos como acesso não autorizado, destruição, uso, modificação ou divulgação não autorizados por todo o seu ciclo de vida;

b) Escolher operadores de DP que apresentem garantias suficientes da aplicação de controles organizacionais, físicos e técnicos no tratamento de dados e que assegurem conformidade com esses controles;

c) Basear estes controles em requisitos legais aplicáveis, normas de segurança, resultados de análises de riscos sistemáticas, como descrito na ABNT NBR ISO 31000, e resultados de análises de custo/benefício;

d) Implementar os controles proporcionalmente à probabilidade e severidade das possíveis consequências, à sensitividade dos DP, a todos os titulares de DP que podem ser afetados e ao contexto em que isto se insere;

e) Limitar o acesso aos DP apenas àqueles que necessitam deles para o cumprimento de suas obrigações e às necessidades de acesso para a execução das funções que desempenham;

f) Solucionar os riscos e vulnerabilidades que são descobertos pelos processos de auditoria e pelas avaliações de riscos de privacidade; e

g) Submeter os controles a análises críticas periódicas e novas análises em um processo contínuo de gestão de riscos.

11. *Compliance* com a privacidade

O princípio de *Compliance* com a privacidade refere-se à cooperação com a(s) autoridades(s) supervisora(s) no monitoramento das leis de proteção de dados aplicáveis e observando suas diretrizes e requisições. Para estar aderente a este princípio é necessário:

a) Verificar e demonstrar que o tratamento atende aos requisitos de proteção de dados e de garantia da privacidade por meio de auditorias periódicas com auditores internos ou terceiros credenciados para esta atividade;

b) Ter controles internos apropriados e mecanismos de supervisão independentes implementados que assegurem conformidade com a legislação relevante sobre privacidade e com os procedimentos e políticas de segurança, proteção de dados e privacidade; e

c) Desenvolver e manter análises de riscos de privacidade, de forma a avaliar se os programas e as iniciativas de entrega de serviços, que envolvem o tratamento de DP, estão em conformidade com os requisitos de proteção de dados e requisitos de privacidade.

A norma apresenta ainda dois anexos, sendo eles:

- Anexo A (informativo) – Correspondência entre os conceitos de ABNT NBR ISO/IEC

29100 e os conceitos da ISO/IEC 27000; e

- Anexo NA (informativo) – Esclarecimentos sobre as opções de tradução.

A ISO 29100, a partir de um entendimento comum sobre proteção e privacidade de dados, fornece uma estrutura abordando aspectos organizacionais e técnicos que podem orientar empresas na implementação de requisitos e controles de proteção e privacidade de dados.

As normativas possuem caráter orientativo e apoiam a adequação de sistemas, serviços, produtos e ambientes aos princípios de proteção e privacidade de dados e em alguns casos direcionam para certificações específicas. Porém, essa temática, quando analisada sob a ótica legal, amplia seu escopo na esfera do direito civil.

2.3 LEIS DE PROTEÇÃO E PRIVACIDADE DE DADOS

As leis de proteção e privacidade de dados têm como objetivo garantir os direitos aos cidadãos titulares dos dados e trazem em seu conteúdo os princípios e controles que devem ser adotados por organizações que tratam dados pessoais, para prover os direitos de seus titulares.

Apesar da temática ser bastante antiga, leis específicas de proteção de dados pessoais começaram a surgir ao redor do mundo a partir das décadas de 1960 e 1970, com o advento das tecnologias da informação. O grande poder de processamento de dados pelos computadores foi o fator responsável pela evolução das legislações. Nesta subseção serão abordadas a Lei Geral de Proteção de Dados (GDPR) dos países da União Europeia e a Lei Geral de Proteção de Dados Pessoais (LGPD) brasileira.

2.3.1 *General Data Protection Regulation* (GDPR)

A GDPR é a regulamentação sucessora da Diretiva de Proteção de Dados 95/46, já abordada no início desta seção. Porém, para adentrar no percurso histórico da GDPR faz-se necessário expor mais alguns detalhes sobre a Diretiva. A Diretiva de Proteção de Dados 95/46/CE é um documento amplo na temática de proteção e privacidade de dados destinado a proteger os direitos e as liberdades das pessoas no que diz respeito ao tratamento de dados pessoais, com a adoção de critérios essenciais que conferem licitude ao tratamento e de princípios relativos à qualidade dos dados. Aprovada em 1995, estabeleceu-se três anos após a data de sua vigência, para que os países membros da União Europeia adotassem as medidas legislativas e regulamentares necessárias para incorporar suas regras. A Diretiva exigiu também que cada país membro da União Europeia tivesse uma agência ou comissário de proteção de

dados, que supervisionasse a aplicação dos princípios e leis de proteção à privacidade individualmente (DIRECTIVA 95/46/CE, 1995). A Diretiva de Proteção de Dados da UE (95/46/EC) foi implementada de forma diferente pelos Estados Membros da União Europeia nas respectivas jurisdições nacionais, resultando na fragmentação das leis nacionais de proteção de dados de cada país.

Os elementos e princípios básicos da Diretiva têm uma história de mais de quarenta anos, muito antes de sua utilização. Os princípios permaneceram os mesmos desde a promulgação da primeira lei de proteção de dados no governo federal alemão, estado de Hesse, em 1970. Posteriormente, foram incorporados em todos os atos de proteção de dados em nível dos Estados-Membros, até a sua adoção e formalização no texto da Diretiva em 1995 (DE HERT; PAPAKONSTANTINOU, 2012).

Em meados de 2018, a *General Data Protection Regulation* (GDPR) entrou em vigor substituindo a Diretiva de Proteção de Dados 95/46/EC, e é o regulamento referência para proteção e privacidade de dados. A GDPR foi projetada para harmonizar as leis de privacidade em toda a Europa, a fim de fornecer proteção e capacidade para os indivíduos controlarem o desempenho de seus dados pessoais, frente aos novos desenvolvimentos tecnológicos e aos novos desafios trazidos com eles (EUROPEAN UNION, 2018).

Os princípios de proteção de dados na GDPR permanecem em grande parte como eram na Diretiva, com algumas poucas modificações. A GDPR, no seu artigo 5º, preconiza que os dados pessoais devem ser:

- Processados legalmente, de forma justa e transparente (o "princípio da legalidade, justiça e transparência");

- Coletados para fins especificados, explícitos e legítimos e não processados de maneira incompatível com essas finalidades (o "princípio de limitação da finalidade");

- Adequados, relevantes e limitados ao que é necessário em relação ao(s) propósito(s) (o "princípio de minimização de dados");

- Precisos e, quando necessário, mantidos atualizados (o "princípio de precisão");

- Mantidos em uma forma que permite a identificação dos titulares dos dados por não mais tempo do que o necessário para o(s) propósito(s) para o(s) qual(is) os dados são processados (o "princípio de limitação de armazenamento");

- Processados de forma a garantir a segurança adequada dos dados pessoais, utilizando técnicas e medidas organizacionais (o "princípio de integridade e confidencialidade");

- O controlador é responsável por e deve ser capaz de demonstrar conformidade com os princípios acima mencionados ("princípio da responsabilidade"). (DLA PPIPER, 2021).

Torre *et al.* (2019) ressaltam que a GDPR é considerada a Lei mais abrangente, técnica e exigente entre os regulamentos de privacidade de dados pessoais já estabelecidos. O alto nível de rigor que garante a conformidade com a GDPR é cada vez mais comparável ao que é necessário para demonstrar conformidade com os padrões e regulamentos de segurança.

A GDPR é estruturada em 11 Capítulos e 99 Artigos, conforme apresentados a seguir:

- Capítulo I (Artigos de 1 a 4): **Disposições gerais** (âmbito, objetivos, definições)
- Capítulo II (Artigos de 5 a 11): **Princípios**
    - Princípios relacionados ao processamento de dados
    - Bases legais do processamento
    - Condições aplicáveis ao consentimento da criança
    - Processamento de categorias especiais de dados e processamento que não requer identificação
- Capítulo III (Artigos de 12 a 23): Direitos do titular dos dados
    - Direito à transparência e à informação
    - Direito ao acesso
    - Direito à retificação
    - Direito ao apagamento (“Direito de ser esquecido”)
    - Direito à retificação
    - Direito à restrição de processamento
    - Direito à portabilidade de dados
    - Direito de contestar a tomada de decisão automatizada
    - Direito à objeção
    - Restrições
- Capítulo IV (Artigos de 24 a 43): Responsabilidade do Controlador e Processador
    - *Privacy by Design and by Default*
    - Controladores Conjuntos
    - Representantes de controladores sem estabelecimento na União Europeia
    - Função e obrigações do “Processador”
    - Obrigação de garantir a segurança do processamento de dados
    - Notificação de Violação (Artigos 33, 34)
    - Avaliação de impacto à privacidade de dados
    - *Data Protection Officer* - obrigação, escopo e atribuições
    - Códigos de conduta e certificações

- Capítulo V (Artigos de 44 a 50): Transferência de Dados a outros países
  - Princípios e regras para a transferência de dados.
- Capítulo VI (Artigos de 51 a 59): Autoridades fiscalizadoras independentes
  - Requisitos, escopo, competência, atribuições e poderes
- Capítulo VII (Artigos de 60 a 76): Cooperação e consistência na aplicação da lei
  - Cooperação entre DPAs
  - Consistência/coerência nos pareceres
  - Criação do Conselho Europeu de Proteção de Dados (European Data Protection Board - EDPB)
- Capítulo VIII (Artigos de 77 a 84): Recursos, responsabilidades e penalidades
  - Direitos do titular dos dados
  - Representação dos titulares dos dados
  - Condições para a imposição de multas administrativas e outras penalidades
- Capítulo IX (Artigos de 85 a 91): Disposições relativas a situações específicas de processamento
  - Disposições sobre o processamento
  - Obrigações de sigilo
  - Regras para igrejas e associações religiosas
- Capítulo X (Artigos 92 e 93): Atos delegados e atos de execução
  - Exercício de delegação
  - Procedimento do comitê
- Capítulo XI (Artigos de 94 a 99 - Disposições finais

Em resumo, a GDPR é o marco regulatório europeu sobre proteção e privacidade de dados, o qual substituiu a Diretiva 95/46/CE e estabeleceu princípios e regras para direcionar o desenvolvimento tecnológico após a década de 1990. Por ser um regulamento, busca trazer de forma direta e objetiva as regras específicas para situações diversas. Esse regulamento é referência para leis de outros países, como é o caso do Brasil, o qual, inspirado na GDPR, sancionou a Lei Geral de Proteção de Dados Pessoais (LGPD) a ser abordada na próxima subseção.

2.3.2 Lei Geral de Proteção de Dados Pessoais (LGPD)

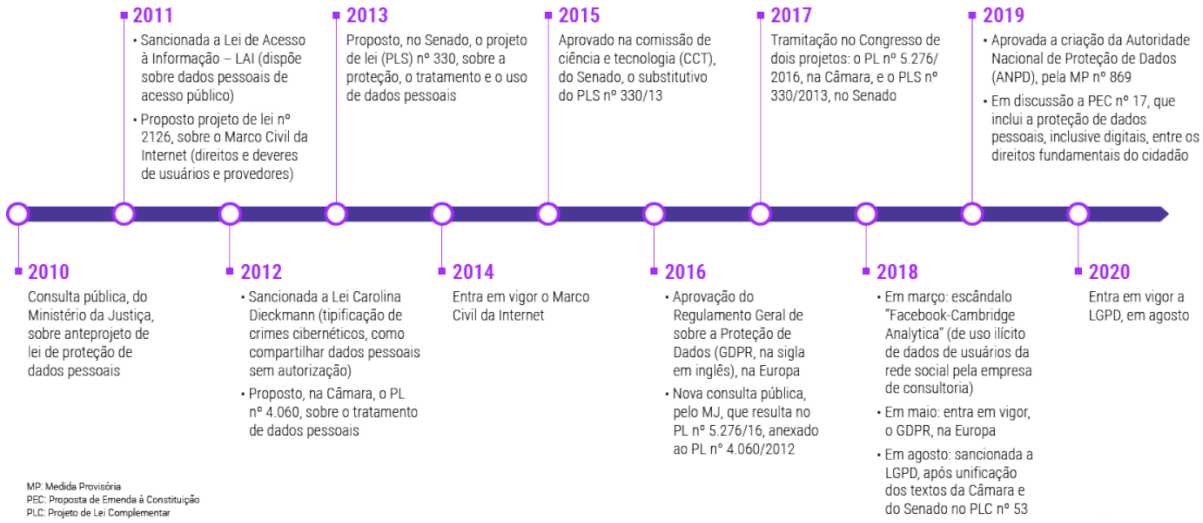
A Lei Geral de Proteção de Dados Pessoais (LGPD) é a legislação que regula o tratamento de dados pessoais no território brasileiro. Foi promulgada em 2018, denominada Lei

Federal n. 13.709/2018 (BRASIL, 2018), e está alinhada à GDPR.

Antes da LGPD, as regulamentações de privacidade de dados no Brasil consistiam em várias disposições espalhadas pela legislação brasileira — tais como: Constituição Federal de 1988, Marco Civil da Internet (Lei Federal n. 12.965/2014) e a Lei n. 12.737/2012 (que dispõe sobre a tipificação criminal de delitos informáticos) —, as quais impõem alguns requisitos relativos à segurança e ao processamento de dados pessoais e outras obrigações dos prestadores de serviços, provedores de redes e aplicativos, bem como direitos dos usuários da Internet. (DLA PIPER, 2021).

A LGPD reúne as disposições referentes à proteção e privacidade de dados em uma lei unificada, destinada exclusivamente para tratar sobre o tema. Até sua entrada em vigor em 2020, essa temática no Brasil passou por uma trajetória de 10 anos, conforme apresentado na Figura 1.

Figura 1 - Trajetória da LGPD



Fonte: Serviço Federal de Processamento de Dados (2021).

A Lei Geral de Proteção de Dados Pessoais (LGPD) dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

O conteúdo da LGPD se baseia em princípios a serem considerados no tratamento de dados pessoais e direitos aos titulares. Para Mendes (2014), pode-se considerar que esses princípios foram desenvolvidos por meio de instrumentos internacionais, trazidos para a legislação brasileira. Trata-se de princípios fundamentais dos cidadãos e devem ser efetivados pelas instituições que manipulam dados.

Em observância à LGPD, boa-fé no tratamento de dados pessoais é a premissa básica, porém é necessário refletir sobre questões tais como: objetivo do tratamento, quantidade de dados coletados, consentimento do titular, entre outras, as quais estão prescritas na Lei. (SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS, 2021).

A LGPD, Lei n. 13709/2018, está dividida em dez capítulos, com 65 artigos, conforme apresentados a seguir:

- Capítulo I (Artigos de 1 a 6): Disposições Preliminares
- Capítulo II (Artigos de 7 a 16):
    - Tratamento dos dados pessoais
    - Tratamento dos dados pessoais sensíveis
    - Tratamento dos dados pessoais de crianças e adolescentes
    - Término do tratamento
- Capítulo III (Artigos de 7 a 22): Direitos do Titular
- Capítulo IV (Artigos de 23 a 32): Tratamento de Dados pelo poder público
    - Regras e responsabilidades
- Capítulo V (Artigos de 33 a 36): Transferência Internacional de dados
- Capítulo VI (Artigos de 37 a 45): Agentes de tratamento de dados pessoais
    - Do controlador e do operador
    - Do encarregado pelo tratamento de dados
    - Responsabilidades e ressarcimento de danos
- Capítulo VII (Artigos de 46 a 51): Segurança e Boas Práticas
    - Segurança e sigilo dos dados
    - Boas práticas e governança
- Capítulo VIII (Artigos de 52 a 54): Fiscalização
    - Sanções administrativas
- Capítulo IX (Artigos de 55 a 59): Autoridade Nacional de Proteção de Dados (ANPD) e Conselho Nacional de Proteção de Dados Pessoais
    - ANPD
    - Conselho Nacional de Proteção de Dados Pessoais
- Capítulo X (Artigos de 60 a 65): Disposições finais e transitórias

O texto da LGPD foi inspirado na GDPR, e esse alinhamento também foi um dos objetivos da LGPD, porém algumas diferenças são apresentadas entre elas (FREUND; FAGUNDES; MACEDO, 2020). Uma análise comparativa entre as duas legislações é apresentada no Quadro 2.

Quadro 2 - Análise comparativa entre a LGPD e GDPR

Item de Conformidade	LGPD	GDPR
Definição e distinção do que são dados pessoais e dados sensíveis. Tal conceituação busca delimitar os diretos e as informações protegidas pelo ordenamento jurídico.	Define que dados pessoais é qualquer informação que identifique ou torne identificável a pessoa natural; já dados sensíveis são os dados pessoais sobre etnia, raça, crenças religiosas, opiniões políticas, dados genéticos/biométricos, além de informações sobre filiações a organizações quaisquer da pessoa natural.	Adota os mesmos princípios e conceitos para realizar a distinção e delimitação dos direitos relativos aos dados pessoais e dados sensíveis, e ainda pontua considerações acerca dos dados genéticos, biométricos e os relativos à saúde.
Obrigatoriedade do consentimento do usuário para a coleta de informações e limitações do tratamento dos dados conforme finalidade	A coleta e o tratamento de dados só poderão ser realizados se o usuário (dono dos dados ou responsável legal no caso de menores legais) der consentimento. Todo agente deve apontar finalidade certa, garantida e justificável ao tratamento do dado. Além disso, deve garantir que ele será utilizado somente para tal finalidade.	Prevê a necessidade de uso dos dados conforme a finalidade apontada. Traz exceções de tratamento por motivo de interesse público, segurança e saúde.
Distinção entre titularidade e responsabilidade sobre os dados, assim como delimitação das funções e responsabilidades assumidas no tratamento de dados.	Titular é a pessoa natural a quem se referem os dados que são objeto de tratamento; por outro lado, o responsável é a pessoa física ou jurídica, de direito público ou privado, que realiza decisões sobre o tratamento de dados. São definidos dois agentes de tratamento: o responsável – cuja competência é decidir sobre o tratamento dos dados – e o operador – a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento dos dados. Ambos os agentes são juridicamente responsáveis pela segurança e privacidade dos dados.	Há a mesma distinção entre titularidade e agentes, mas os agentes são divididos entre controlador e processador de dados. O controlador é quem realiza as decisões acerca do tratamento de dados, o processador, quem efetua o tratamento dos dados. Ambos são responsáveis pelo tratamento dos dados.

Indicação de um encarregado pela comunicação entre os agentes, titulares e órgãos competentes.	Além dos agentes, aponta-se a necessidade da indicação de um encarregado – pessoal natural – pela comunicação de qualquer informação ou fato relevante em relação ao tratamento dos dados. Ele deve atuar como um canal entre os agentes, titulares e órgãos competentes e deve ser indicado pela organização responsável pelo tratamento (Agente de Proteção de Dados)	Aponta que o controlador deve ter uma pessoa responsável por tudo que seja relacionado à proteção de dados (DPO).
Aplicação de mecanismos e práticas pautadas no livre acesso à informação e na transparência entre os usuários e as organizações.	Do consentimento ao fornecimento de dados ao término do tratamento dos dados, as informações acerca do processo devem ser claras, acessíveis e adequadas à linguagem e compreensão do usuário, de forma que o seu consentimento possa ser revogado a qualquer momento. O consentimento do usuário deve ser realizado por escrito ou de qualquer outro modo que demonstre a sua livre manifestação da vontade.	Os titulares também têm direito a informações claras e acessíveis do início ao fim do tratamento dos dados, podendo revogar o consentimento a qualquer momento.
Aplicação de medidas de segurança e dever de reportar	Da mesma forma que as organizações são responsáveis no caso de incidentes – como vazamentos – no tratamento dos dados, devem aplicar medidas de prevenção e proteção à segurança dos dados que manuseiam, como anonimização e encriptação de informações. Ainda assim, no caso de quaisquer incidentes é obrigação da organização notificar as autoridades imediatamente.	Também aponta que as empresas devem criar medidas – como pseudoanonimização e encriptação de dados – para garantir a segurança de forma preventiva. No caso de qualquer incidente, a notificação às autoridades deve ser imediata.
Possibilidade de alteração e exclusão do dado pessoal.	O titular do dado pode alterar ou excluir seu dado, exceto nas hipóteses previstas na lei, como fins	Os titulares dos dados também podem alterar ou excluir seus dados.

	fiscais, por exemplo. Da mesma forma, assim que o tratamento de dados chegar ao final – seja porque cumpriu sua finalidade, seja porque o usuário revogou o consentimento – as informações devem ser eliminadas.	

Fonte: Pinheiro (2020).

Com essa análise, observa-se que as diferenças são tênues, destacando-se apenas algumas relacionadas à nomenclatura, exceções e especificações.

Contudo, sob a ótica das legislações, assim como para certificações, implementar proteção e privacidade de dados é imprescindível para organizações que tratam dados pessoais e adotar práticas incorporadas na concepção de novos produtos, processos e sistemas deve se tornar um hábito. É isso que trata o conceito do *Privacy by Design*, assunto a ser abordado na próxima subseção.

2.4 *PRIVACY BY DESIGN*

Privacy by Design (PbD) é um conceito desenvolvido nos anos 80 por Ann Cavoukian, Comissária de Proteção de Dados de Ontário para ser aplicado nas TICs, em práticas organizacionais, estruturas físicas e no ecossistema de informações em redes em grande escala. Para a autora o PbD "avança a visão de que o futuro da privacidade não pode ser assegurado apenas pela conformidade com estruturas regulatória; em vez disso, a garantia de privacidade, deve, idealmente, tornar-se o modo de operação padrão de uma organização" (CAVOUKIAN *et al.*, 2009, p. 1). Este conceito desvincula a proteção e privacidade como algo adicional a ser implementado, e sim a algo integrante ao contexto de desenvolvimento das soluções informáticas.

Schaar (2010) cita o PbD como um princípio a ser vinculado tantos aos criadores e desenvolvedores das tecnologias quanto aos responsáveis pelo tratamento dos dados que decidem sobre a aquisição e uso de sistemas de TICs. Os responsáveis devem considerar a proteção e privacidade dos dados na fase de planejamento dos projetos e os fornecedores devem demonstrar que todas as medidas necessárias foram tomadas para cumprir os requisitos.

Cavoukian *et al.* (2009) definiu sete princípios fundamentais do PbD, sendo eles: 1. Proativo não reativo – Preventivo não corretivo; 2. Privacidade como padrão; 3. Privacidade

incorporado ao *design*; 4. Funcionalidade completa – Soma positiva, não Soma zero; 5. Segurança da ponta a ponta – proteção do ciclo de vida; 6. Visibilidade e transparência e 7. Respeito à privacidade do usuário. Esses princípios são apresentados no Quadro 3, acompanhados das implicações apontadas pela autora para implementação de cada um deles.

Quadro 3 - Princípios do PbD e suas implicações para a implementação

PRINCÍPIOS	IMPLICAÇÕES
1. Ser Proativo e não Reativo; ser preventivo e não corretivo Antecipar e prevenir-se de eventos de privacidade antes que ele aconteça. Trabalhar na prevenção antes que os riscos se concretizem.	- Compromisso em níveis mais altos para definir e aplicar padrões altos de privacidade. - Compromisso de privacidade compartilhado com comunidades de usuários e partes interessadas em uma cultura de melhoria contínua. - Métodos estabelecidos para reconhece estruturas de privacidade ruins corrigindo quaisquer impactos negativos, de forma proativa sistemática e inovadora.
2. Privacidade como padrão Nenhuma ação é necessária por parte do indivíduo, sua privacidade é incorporada ao sistema por padrão.	Atendimento às seguintes Fair Information Practices (FIPs): - Especificação da finalidade: finalidades claras, comunicadas ao titular dos dados antes ou durante a coleta dos dados. - Limitação da coleta: coleta de dados lícita e limitadas para os fins especificados. - Minimização dos dados: coleta e identificação de dados pessoais reduzidas ao mínimo necessário. - Limitação de uso, retenção e divulgação: uso, retenção e divulgação de dados pessoais limitados aos propósitos relevantes identificados pelo titular dos dados.
3. Privacidade incorporada ao *design* A privacidade por *design* está incorporada na arquitetura dos sistemas de TICs e nas práticas de negócio e é um componente essencial da funcionalidade dos sistemas, não é algo a ser incorporado de forma complementar após um fato ocorrer.	- Adotar uma abordagem sistêmica e baseada em princípios para incorporar a privacidade. Todas as práticas aplicadas com igual rigor em todas as etapas do projeto e operação. - Realizar avaliações de impacto e de riscos de privacidade, documentar e publicar, assim como todas as medidas tomadas para mitigar esses riscos. - Minimizar os impactos de privacidade resultantes na tecnologia, operação ou arquitetura de informação.
4. Funcionalidade completa – Soma positiva, não soma zero Tem o objetivo de manter os interesses legítimos e os controles de privacidade somar com os mesmos de uma maneira ganha-ganha.	- Ao incorporar a privacidade em uma determinada tecnologia, processo ou sistema, isso deve ser feito de forma que a funcionalidade total não seja prejudicada e, na medida do possível, que todos os requisitos sejam otimizados. - Incorpora objetivos legítimos de maneira inovadora e positiva.

	- Encontrar a multifuncionalidade considerando os interesses e objetivos, as funções desejadas e as métricas acordadas.
5. Segurança de ponta a ponta – Proteção completa no ciclo de vida Proteção e privacidade incorporados ao sistema antes da coleta dos dados, atuando em todo o ciclo de vida dos dados envolvidos. Garantir que os dados sejam coletados, retidos e destruídos com segurança e em tempo hábil.	- As entidades devem assumir a responsabilidade pela segurança de informações pessoais ao longo de todo o ciclo de vida de forma consistente com padrões reconhecidos. - Os padrões devem garantir a confidencialidade, integridade e disponibilidade dos dados ao longo de seu ciclo de vida.
6. Visibilidade e Transparência Manter os processos de tratamento dos dados aberto, com seus componentes visíveis e transparentes, procura assegurar a todos os interessados que está de fato operando de acordo com as promessas e objetivos declarados.	Atendimento às seguintes Fair Information Practices (FIPs): - Responsabilização: ser responsável por zelar pelos dados coletados de forma sistematizada e documentada. - Abertura: Abertura e transparência quanto as práticas adotadas para o tratamento dos dados. - Conformidade: Estabelecer mecanismos de reclamações, reparações e comunicações disponíveis aos titulares dos dados.
7. Respeito pela privacidade do usuário Manter os interesses dos indivíduos em primeiro lugar, oferecendo medidas fortes de privacidade, avisos apropriados e opções fáceis de usar.	Atendimento às seguintes Fair Information Practices (FIPs): - Consentimento: consentimento livre e esclarecido é necessário para coleta e uso dos dados, exceto quando permitido por lei. - Precisão: as informações pessoais devem ser tão precisas, completas e atualizadas quanto necessário para cumprir os propósitos especificados. - Acesso: os titulares devem ter acesso a seus dados para alterá-los quando necessário e ter informações sobre os acessos que são disponibilizados a eles. - Conformidade: Estabelecer mecanismos de reclamações, reparações e comunicações disponíveis aos titulares dos dados.

Fonte: Cavoukian *et al.* (2009).

Ao analisar os objetivos do PbD e seus princípios, observa-se que para colocá-lo em prática é preciso que engenheiros de soluções e sistemas assim como gestores e demais envolvidos em projetos que tratam dados, implementem além de requisitos tecnológicos de proteção, aqueles que não são de natureza técnica. Para isso é necessário que estejam preparados no âmbito metodológico e que a cultura organizacional favoreça essa implementação.

Spiekermann (2012) traz que dados pessoais são ativos centrais nos modelos de negócios de muitas empresas e por isso o envolvimento ativo da administração nas estratégias

de privacidade corporativa é fundamental. No entendimento de Wiese (2016) adotar o conceito de PbD não depende apenas de metodologias, pois, em seu ponto de vista, as leis são de igual importância e devem "preparar o terreno" para os projetos de privacidade por *design*.

Entende-se que o envolvimento e preparo de profissionais, metodologia, cultura e lei são de extrema importância para a implementação do PbD e que sua adoção é fundamental para que as adequações aos requisitos de proteção e privacidade de dados sejam incorporadas na concepção de produtos, processos e sistemas, colocando um fim às adequações que são realizadas após a existência dos mesmos, por solicitação de clientes ou mesmo após a ocorrência de algum incidente que demande essas adequações.

Contudo, sob a ótica do PbD proteção e privacidade de dados devem fazer parte dos requisitos de projetos como um processo de antecipação. Já para comprovar aderência a esses requisitos, a temática evidências ganha destaque e é abordada na sequência, na subseção a seguir.

2.5 GERENCIAMENTO DE EVIDÊNCIAS

Evidências são artefatos que podem ser utilizados para demonstrar e comprovar a aplicação de um controle, a configuração de uma regra, a execução de uma atividade ou qualquer outro fato ou feito em um determinado contexto (FORMOSO; FELICI, 2016). Além disso, evidências são necessárias por diversas razões em organizações, seja para confirmar um fato, para comprovar conformidade legal ou regulamentar, para investigar uma ação indevida ou incidentes, entre outros.

No contexto contábil as evidências são utilizadas com frequência em auditorias. Zuca (2015) define evidências como todas as informações utilizadas pelo auditor para embasar as avaliações e conclusões de uma auditoria e podem ser classificadas como: a) os registros contábeis subjacentes mantidos pela administração para apoiar a preparação dos demonstrativos financeiros; e b) outras informações obtidas de fontes externas e internas utilizadas em uma comprovação. O autor salienta a importância da confiabilidade e completeza das evidências e complementa que não existe uma definição de quantidade de evidências necessárias em uma auditoria, porém acrescenta que a suficiência e a adequação das evidências de auditoria são inter-relacionadas, ou seja, a quantidade de evidências necessárias diminui se a qualidade (adequação) das evidências obtidas aumenta. Além disso, Zuca (2015) considera que geralmente as evidências confiáveis possuem as seguintes características:

a) são obtidas de uma fonte experiente e independente fora da entidade;

b) a evidência gerada internamente é mais confiável se os controles internos relacionados à entidade são mais eficazes;
c) provas obtidas diretamente pelo auditor por meio de exame físico, observação, computação e inspeção são mais persuasivas do que as informações obtidas indiretamente ou por inferência;
d) A evidência de auditoria em forma documental, seja em papel ou digital, é mais confiável do que a evidência obtida oralmente;
e) Documentos originais fornecem evidências de auditoria mais confiáveis do que fotocópias.

Grobler e Louwrens (2010) reforçam que evidências consistentes são essenciais para organizações e são comumente utilizadas no contexto da TI para demonstrar diligência com relação à governança de TI e para investigar e gerenciar incidentes internos e externos. Os autores acreditam que é essencial identificar potenciais evidências proativamente e que boas evidências são um facilitador de negócios.

No universo do cibercrime, as evidências digitais são as mais utilizadas e são tratadas para que possam ser utilizadas e apresentadas como prova nos tribunais. Nesse contexto, uma das fases de uma investigação consiste em identificar, coletar, salvaguardar e examinar evidências. Mohammed (2018) considera que as evidências digitais podem ser obtidas com: a saída visual do monitor, as cópias impressas, a plotagem de provas impressas, o material gravado em disco ou em qualquer mídia removível e evidência autêntica e única da memória dos computadores. Na visão do autor, as evidências digitais possuem a vantagem de estarem menos expostas a impactos que possam afetar sua proteção em comparação a outros tipos de evidências, além da imparcialidade e confiabilidade das mesmas. Neste quesito é importante considerar as inúmeras formas de alterar evidências digitais devido a recursos tecnológicos avançados que permitem essas alterações. Entende-se que tanto para evidências físicas quanto para as digitais, existem as regulamentações de integridade que devem ser observadas com atenção para comprovar a idoneidade e integridade das mesmas.

Nair *et al.* (2015) entendem que as evidências são utilizadas para construir confiança mediante o cumprimento de requisitos que satisfaçam os padrões desejados. Em domínios como aviação, ferroviário e automotivo normalmente os sistemas são avaliados rigorosamente por órgãos certificadores que verificam a aderência dos sistemas aos padrões de segurança exigidos para a certificação de segurança. Nesse contexto, os autores definem evidências como sendo informações ou artefatos que contribuem para o desenvolvimento da confiança na operação de um sistema e para mostrar o cumprimento das exigências de uma ou mais normas de segurança.

Diante do exposto, é possível concluir que demonstrar conformidade com um padrão específico ou legislações, independente do tema, envolve reunir artefatos que possam ser utilizados como evidências convincentes sobre os critérios exigidos. Trazendo para o contexto desta pesquisa, as normativas apresentam as diretrizes de implementação e seus controles. Dessa forma, para cada controle implementado em atendimento a essas diretrizes, artefatos devem ser extraídos para serem utilizados na comprovação de sua conformidade. Assim, de forma organizada e estruturada, se torna possível demonstrar a aderência aos requisitos com rastreabilidade das evidências e das fontes de extração, promovendo maior confiabilidade nas alegações de conformidade.

Para isso, propõe-se a utilização da abordagem de casos de garantia, a qual já é consolidada no processo de desenvolvimento de sistemas, cujo conteúdo é apresentado na próxima subseção.

2.5.1 Casos de Garantia

Casos de garantia são estruturas apoiadas por evidências utilizados para justificar alegações, comumente aplicados para justificar a existência de requisitos de segurança e outras propriedades em sistemas complexos e garantir que elas foram abordadas durante o desenvolvimento. Para a OMG *GROUP et al.* (2020), casos de garantia consistem em uma coleção de afirmações auditáveis, argumentos e evidências criadas para apoiar a alegação de que um sistema/serviço irá satisfazer seus requisitos de garantia.

O Grupo OMG defende que:

> um caso de garantia é um documento que facilita a troca de informações entre várias partes interessadas do sistema, como fornecedores e adquirentes, e entre a operadora e o regulador, onde o conhecimento relacionado com a segurança e proteção do sistema é comunicado de forma clara e defensável. (OMG GROUP *et al.*, 2020).

Porém, essa abordagem se originou e vem sendo adotada em diferentes contextos. O precursor da abordagem de casos de garantia, ainda que não utilizasse tal nomenclatura, foi o relatório desenvolvido pelo comitê nomeado no governo do Reino Unido de Lord Robens, em 1972. Este relatório apresentou mudanças radicais nas abordagens de segurança, as quais apontaram para elementos de autorregulação. Relacionada a isso estava a ideia de que os regulamentos deveriam definir metas, ao invés de prescrever métodos e soluções (RUSHBY, 2015).

Em 1974, o Reino Unido adotou uma nova legislação para regulamentar a saúde e a

segurança das pessoas no local de trabalho, a qual deu origem a um reconhecido meio de avaliação de risco e de demonstração da existência de uma gestão satisfatória implementada, através da apresentação e manutenção de um caso de segurança. (INGE, 2007).

Com isso, diferentes indústrias desenvolveram diferentes casos de segurança em contextos distintos, porém Inge (2007) salienta que os princípios básicos são os mesmos e utilizam dois elementos: argumento e evidência, os quais se apoiam mutuamente. A evidência é necessária para justificar que o argumento é verdadeiro. O argumento é necessário para mostrar que a evidência é suficiente e relevante. O autor complementa que independentemente do contexto de aplicação, um caso de garantia de segurança aborda: a) o escopo do sistema ou atividade que está sendo abordada, junto com detalhes de seu contexto ou ambiente; b) o sistema de gestão utilizado para garantir a segurança; c) os requisitos, legislação, normas e políticas aplicáveis, com evidências de que foram cumpridos; d) evidência de que os riscos foram identificados e controlados de forma adequada, e que o nível residual do risco é aceitável; e, e) garantia independente de que o argumento e as evidências apresentadas são suficientes para a aplicação em questão.

Na visão de Bloomfield, Netkachova e Stroud (2013), um caso de segurança apoia um argumento na demonstração de que os requisitos necessários para um determinado sistema são atendidos. Sendo assim, o caso de segurança é composto por *reivindicações* sobre as propriedades do sistema e, seguindo uma abordagem sistemática, apresenta *argumentos* que demonstram que as reivindicações são fundamentadas ou refutadas por *evidências*.

Ge *et al.* (2012) complementam que é usual a prática de construção de argumentos bem fundamentados em vários contextos, porém a evidência, mesmo sendo essencial para uma determinada reivindicação de alto nível, nunca é suficiente por si só para sustentar que sistemas são aceitavelmente seguros. As evidências requerem uma conexão entre elas e a alegação de segurança que faça a ponte por meio de afirmações e argumentos, compondo uma estrutura denominada de casos de garantia.

Na visão de Sklyar e Kharchnko (2016), casos de garantia é uma metodologia comprovada em uso para demonstrar a conformidade de um sistema com requisitos críticos de segurança e proteção. Rushby (2015), por sua vez, reforça a aplicabilidade desta abordagem em demais cenários apresentado por Inge (2007), ao afirmar que a estrutura de reivindicações, argumentos e evidências é certamente o fundamento intelectual de qualquer meio racional para garantir e certificar a segurança ou outra propriedade crítica de qualquer tipo de sistema.

Diante do exposto, pode-se concluir que um caso de garantia é uma forma convincente que um sistema, serviço ou organização pode adotar para demonstrar que opera da forma

pretendida e/ou exigida, sendo representada por reivindicações e argumentos e apoiada por um corpo de evidências de conformidade consistentes.

Os casos de garantia são normalmente representados textualmente usando linguagem natural, ou graficamente usando notações estruturadas como o *Goal Structuring Notation* (GSN) ou *Claims*, *Arguments, Evidence* (CAE). Esta pesquisa foca nas notações gráficas por estas apresentarem maior visibilidade de sua estrutura, facilitando assim a compreensão e a análise do contexto.

2.5.2 Notação para Estruturação de Objetivos (GSN)

O *Goal Structuring Notation* (GSN) é um padrão para estruturar e representar metas utilizando notações gráficas. Aplica linguagem simples e pode ser adaptado e aplicado para representar uma estrutura de metas em qualquer domínio.

Foi originado na Universidade de Nova York no início de 1990 como parte de um projeto e desde então seguiu um processo de refinamento e melhorias em seu desenvolvimento. A primeira versão do GSN foi elaborada em um processo de consenso que envolveu usuários do padrão nos contextos da academia e da indústria, entre 2007 e 2011 — ano de publicação da primeira versão. E a última versão (versão 2), publicada em 2018, foi atualizada considerando comentários e sugestões de usuários com base em suas experiências de uso do GSN no período subsequente a publicação da primeira versão. (*ASSURANCE CASE WORKING GROUP et al.*, 2018).

Para Spriggs (2012), as estruturas de metas representadas por notações podem ser utilizadas para comprovar a outras pessoas sobre a veracidade das afirmações que são dispostas e na visão do autor, foram as documentações publicadas sobre os casos de garantia que facilitou o uso do GSN.

Diversos estudos foram desenvolvidos ao longo do tempo considerando a aplicação do GSN em cenários distintos. Abaixo são relatados alguns deles.

Ge *et al.* (2012) explora a GSN para utilizar uma abordagem semelhante à de um caso de segurança na tomada de decisão na prática clínica. Alden *et al.* (2015) propõem uma abordagem baseada na GSN para avaliar a mecânica de sistemas biológicos, a qual submetem um sistema a uma análise da conformidade em relação aos critérios identificados. Já Simmonds e Cook (2017) aplicam a GSN na formulação de alegações para aceitação e para argumentações referentes à integridade técnica (segurança, adequação para o serviço e conformidade ambiental) em projetos da força de defesa Australiana, para cada um dos tipos de serviços:

térrea, aeroespacial ou naval. Athe e Dinh (2019), propõem um *framework* para avaliação quanto à adequação do código de uma ferramenta de simulação para uma aplicação em reator nuclear. O *framework* proposto é desenvolvido com o uso da GSN. E, Kobayashi *et al.* (2020) apresentam um estudo que contempla a descrição de um caso de garantia utilizando a GSN para, com base na estrutura da ISO 27001, avaliar políticas de segurança da informação entre uma empresa e sua subsidiária ou subsidiárias fundidas ou adquiridas.

Para melhor compreendê-lo, os elementos do GSN serão apresentados quanto ao seu objetivo, à representação gráfica e declaração textual, nesta subseção. Vale ressaltar também que este estudo não possui a intenção de detalhar o GSN em sua totalidade e sim apresentar seus elementos de notação para o entendimento de seu funcionamento e para posterior compreensão de sua aplicação nessa pesquisa. Sendo assim, são abordados aqui os principais elementos de notação utilizados pelo GSN, que são: metas, estratégias, soluções, contextos, suposições e justificativas, além das instruções sobre as regras gramaticais que regem a declaração textual utilizada em cada elemento.

A seguir são apresentados os elementos da abordagem GSN e sua funcionalidades, sendo o conteúdo exposto, extraído do documento oficial do grupo de trabalho propulsor da abordagem – *Goal Structuring Notation Community Standard* – V.2. janeiro de 2018 – *The Assurance Case Working Group* (ACMG).

O padrão GSN define elementos, as relações permitidas entre eles e a linguagem de texto a ser utilizada nas representações. Cada elemento compreende em um símbolo gráfico e uma declaração textual, conforme apresentado no Quadro 4.

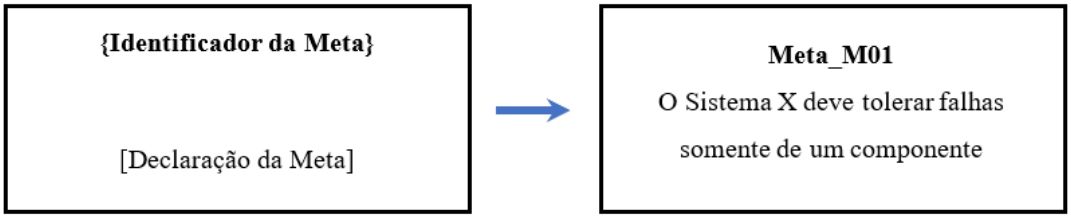
Quadro 4 - Elemento: Metas

Objetivo: elemento que declara o objetivo principal ou objetivos secundários que são suporte ao principal.	
Representação gráfica: uma meta é representada por um retângulo.	Declaração Textual: Cada *meta* GSN deve conter uma única declaração de objetivo, expressa como uma proposição na forma de uma frase nominal + frase verbal.

Fonte: Adaptado de *Assurance Case Working GROUP et al.* (2018).

Um exemplo de meta pode ser observado na Figura 2.

Figura 2 - Exemplo de Meta



Fonte: Adaptada de *Assurance Case Working Group et al.* (2018).

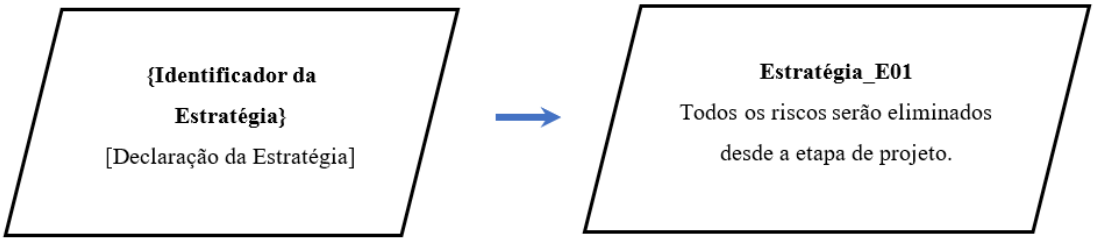
Quadro 5 - Elemento: Estratégias

Objetivo: elemento que declara como as metas (objetivo e seu(s) objetivo(s) de apoio) são sustentadas, ou seja, descrevem o raciocínio que as conectam.	
Representação gráfica: uma estratégia é representada por um paralelograma.	Declaração Textual: As declarações textuais devem conter uma breve descrição da inferência existente entre as metas permanecendo inalteradas as metas e as estruturas de conexão.

Fonte: Adaptado de *Assurance Case Working GROUP et al.* (2018).

Um exemplo de estratégia pode ser observado na Figura 3:

Figura 3 - Exemplo de Estratégia



Fonte: Adaptada de *Assurance Case Working GROUP et al.* (2018).

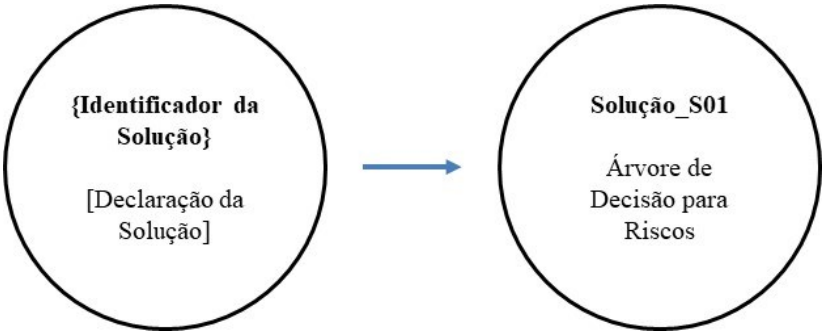
Quadro 6 - Elemento: Soluções

Objetivo: elemento que referencia as evidências que apoiam a verdade de alegação e fornecem suporte para as metas.	
Representação gráfica: uma solução é representada por um círculo.	Declaração Textual: As declarações textuais das soluções devem ser expressas com frases substantivas.

Fonte: Adaptado de *Assurance Case Working GROUP et al.* (2018).

Um exemplo de solução pode ser observado na Figura 4.

Figura 4 - Exemplo de Solução



Fonte: Adaptada de *Assurance Case Working GROUP et al.* (2018).

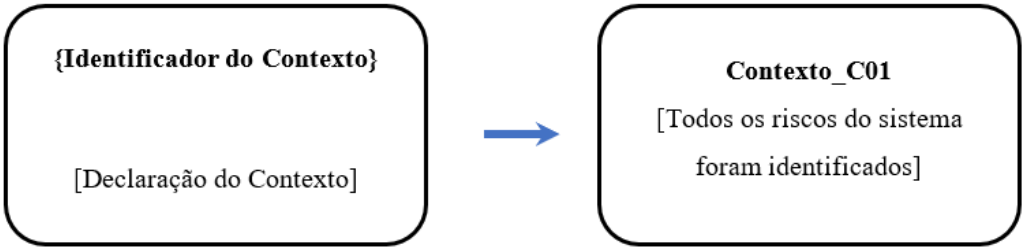
Quadro 7 - Elemento: Contextos

Objetivo: elemento que apresenta um artefato contextual que declara o contexto no qual uma meta, estratégia ou etapa de raciocínio deve ser interpretada. No GSN existem dois tipos de contexto, podendo ser: 1 - uma referência para algum tipo de artefato que contenha informações contextuais, ou 2 - uma declaração.	
Representação gráfica: um contexto é representado por um retângulo com as laterais arredondadas.	Declaração Textual: para o contexto do tipo 1 a declaração textual deve ser expressa como um sintagma nominal. Já para o contexto do tipo 2 a declaração textual deve contemplar informações explicativas (como a definição de algum termo, por exemplo) de forma resumida usando frases completas de uma frase nominal + estrutura verbo-frase.

Fonte: Adaptado de *Assurance Case Working GROUP et al.* (2018).

Um exemplo de contexto pode ser observado na Figura 5.

Figura 5 - Exemplo de Contexto



Fonte: Adaptada de *Assurance Case Working GROUP et al.* (2018).

Quadro 8 - Elemento: Suposição

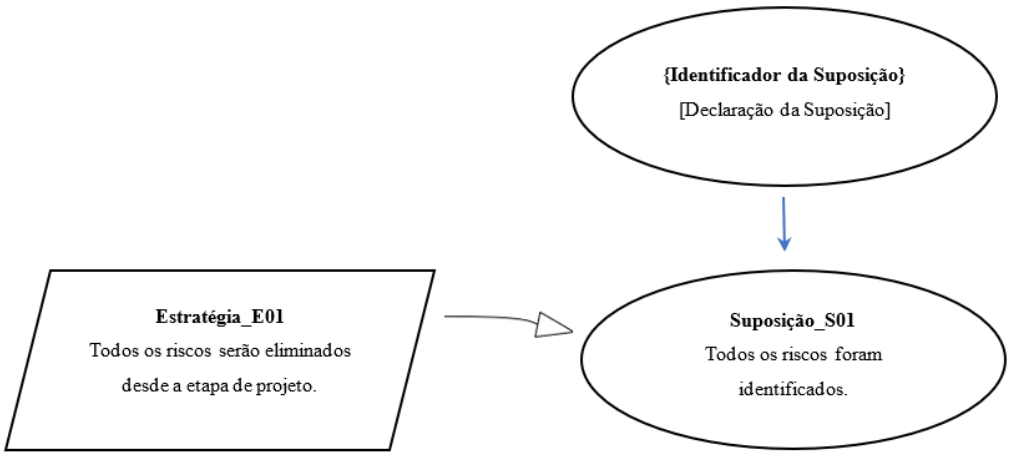
Objetivo: elemento opcional utilizado para declarar uma suposição/hipótese sobre metas e estratégias. As suposições não possuem fundamentação, fornecem informações adicionais necessárias para a compreensão das metas e/ou estratégias, e precisam ser válidas para que as metas ou estratégias a qual se referem sejam válidas.	
Representação gráfica: uma suposição é representada por uma elipse em formato oval, com a letra "S" no canto inferior direito.	Declaração Textual: Por tratar de informações adicionais para apoiar a compreensão de metas e estratégias, a declaração textual das suposições deve ser representada da forma que for necessário para cumprir seu propósito, usando frases completas na forma sintagma nominal +

	sintagma verbal

Fonte: Adaptado de Assurance Case Working GROUP *et al.* (2018).

Um exemplo de suposição pode ser observado na Figura 6. Nesse exemplo, a Estratégia_01 é declarada com a hipótese de que todos os riscos foram identificados corretamente.

Figura 6 - Exemplo de uma suposição relacionada a uma estratégia



Fonte: Adaptada de *Assurance Case Working GROUP et al.* (2018).

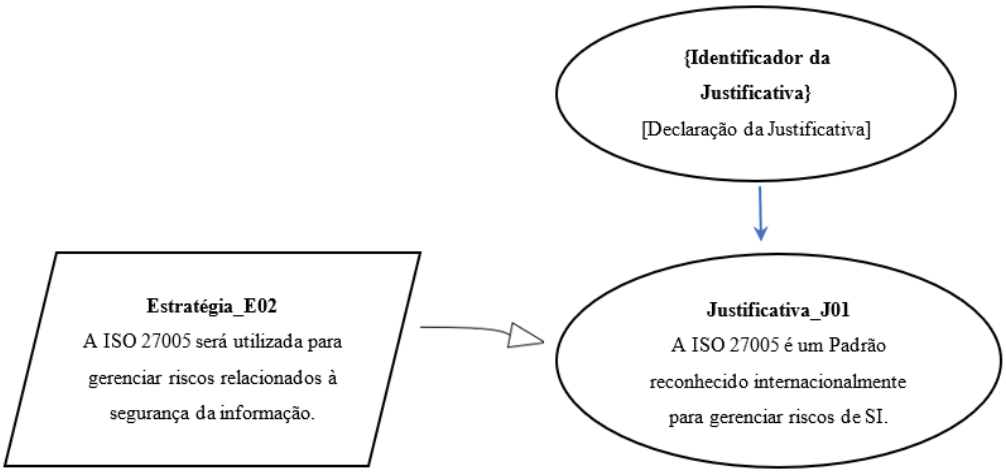
Quadro 9 - Elemento: Justificativa

Objetivo: elemento opcional utilizado para declarar uma justificativa e/ou explicação sobre o porquê uma determinada estratégia ou meta deve ser considerada aceitável.	
Representação gráfica: uma declaração de justificativa é representada por uma elipse em formato oval com a letra "J" no canto inferior direito.	Declaração Textual: Da mesma forma que nas suposições, as justificativas são informações adicionais para apoiar a compreensão de metas e estratégias. A declaração textual deve ser representada da forma que for necessário para cumprir seu propósito, usando frases completas na forma sintagma nominal + sintagma verbal.

Fonte: Adaptado de *Assurance Case Working GROUP et al.* (2018).

Um exemplo de justificativa pode ser observado na Figura 7. Neste exemplo a Estratégia_02 é declarada com justificativa do uso da ISO 27005 para o gerenciamento de Riscos de Segurança da Informação.

Figura 7 - Exemplo de uma justificativa



Fonte: Adaptada de *Assurance Case Working GROUP et al.* (2018).

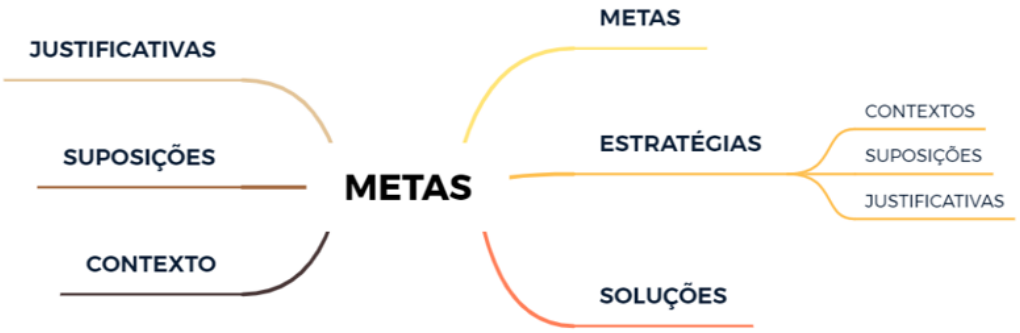
Os principais elementos definidos pelo GSN devem ser combinados e relacionados para representar as estruturas lógicas de metas. O GSN disponibiliza dois tipos de relacionamento que podem ser utilizados para conectar esses elementos, são eles: “Apoiado por” e “No contexto de”.

“Apoiado por “	O relacionamento do tipo “Apoiado por” é representado por uma linha contínua com a seta solida e indica relações entre os elementos, sendo estas inferenciais (declaram que há uma inferência entre os elementos) ou evidenciais (declaram a ligação entre um elemento e as evidências utilizadas para sustentá-lo). Permite conectar: metas com metas, metas com estratégias, metas a soluções e estratégias a metas.
“No contexto de”	O relacionamento do tipo “No contexto de” é representado por uma linha contínua com a seta oca e declara uma relação contextual. Permite conectar: Metas para contextos, metas para suposições, metas para justificativas e estratégias para contextos.

Ambos os tipos de relacionamento declaram a relação entre um elemento de origem e um elemento de destino e a seta deve ser utilizada apontando para o alvo.

Algumas regras regem as relações entre os elementos gráficos do GSN e os relacionamentos são permitidos conforme representando na Figura 8.

Figura 8 - Relacionamentos permitidos entre os elementos GSN



Fonte: Elaborado pela autora (2021).

O elemento Meta pode ser relacionado com:

a) Outras metas de apoio;

b) Estratégias que argumentam a meta principal ou uma ou mais metas de apoio;

c) Uma ou mais soluções (evidências) que afirmam a meta principal;

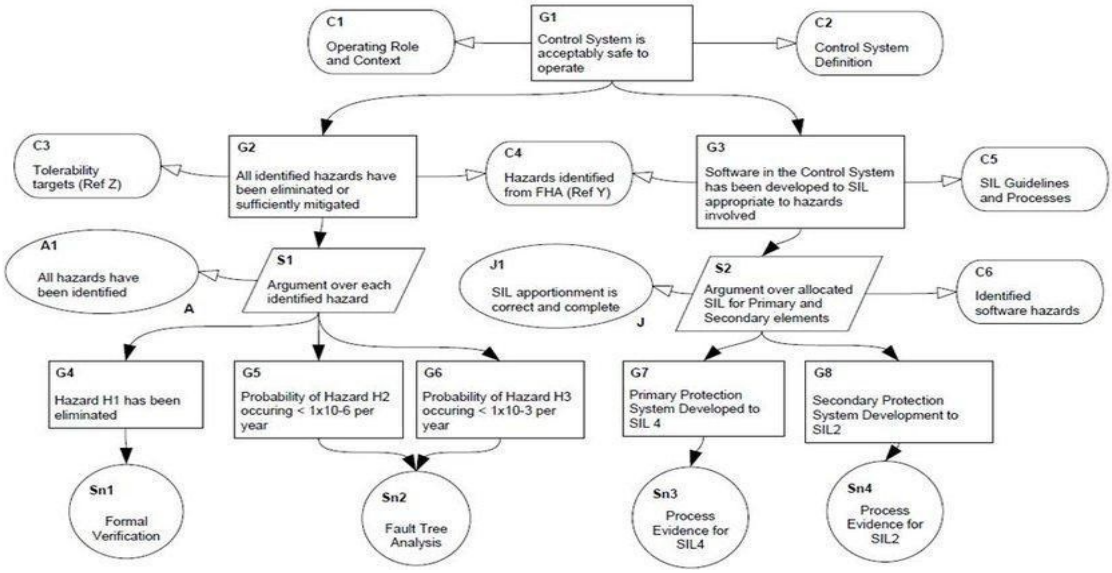
d) Com Contexto usado para declarar informações complementares relacionadas à Meta principal;

f) Com Suposições e Justificativas.

Já o elemento Estratégias pode ser relacionado com: Contextos, Suposições e Justificativas.

Um exemplo de estrutura de metas pode ser visualizado na Figura 9.

Figura 9 - Exemplo de estrutura de metas



Fonte: *Assurance Case Working GROUP et al.* (2018).

Observa-se no exemplo acima que com a notação gráfica GSN, as argumentações de segurança e os elementos que as suportam, tornam os direcionamentos, mecanismos e controles adotados claros, facilitando a compreensão entre as partes envolvidas (desenvolvedores e avaliadores de maneira geral) e a comprovação de conformidade para a aceitação do sistema.

Dando continuidade às abordagens de notação gráfica para estruturação de objetivos, a seguir será exposta a abordagem de Notação *Claims, Arguments, Evidence* (CAE).

2.5.3 Notação para Estruturação de Reivindicações (CAE)

Claims, Arguments, Evidence (CAE) é uma notação gráfica semelhante ao GSN para representar casos de garantia, documentando um conjunto de afirmações apoiadas por argumentos e evidências relacionadas.

Rhodes *et al.* (2010) apontam a nomenclatura e o sentido de progressão da abordagem com as principais diferenças entre elas. Em relação à nomenclatura, a GSN, conforme abordada no conteúdo anterior, utiliza a representação orientada a objetivos, e para isso define nós para Objetivos, Estratégia e Soluções. Por sua vez, a CAE, define nós para reivindicações (GSN – objetivos), argumentos (GSN – estratégias) e evidências (GSN – soluções). Já em relação ao sentido de progressão, a GSN desenvolve a abordagem de cima para baixo, definindo o objetivo principal e partir dele são definidos os demais componentes, e a CAE suporta a visão *Bottom-up* iniciando pelas evidências para então chegar à reivindicação.

Selviandro, Hawkins e Habli (2020) consideram que uma reivindicação em CAE pode ser definida como uma declaração afirmada dentro do argumento, que pode ser avaliada como verdadeira ou falsa. Um argumento como uma descrição apresentada em apoio a uma reivindicação, e uma evidência como uma referência às evidências apresentadas em apoio à reivindicação ou ao argumento.

Já em *Claim, Argument, Evidence*[1] traz as seguintes definições para os componentes da CAE:

Reivindicação - Uma afirmação verdadeira/falsa sobre uma propriedade de um objeto específico. Uma reivindicação pode ser entendida como uma imposição, uma exigência a qual é sustentada pelos demais componentes do diagrama e que se pretende convencer como verdadeira, como por exemplo “o sistema é seguro”.

Argumento - Um argumento é uma regra que relaciona o que se sabe ou está sendo

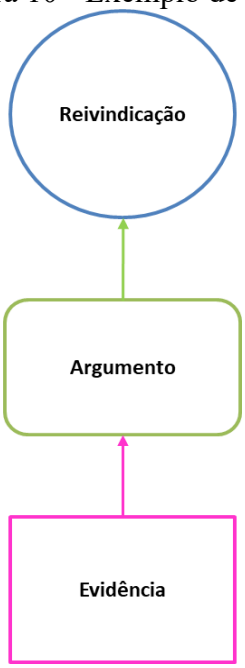
[1] https://claimsargumentsevidence.org/notations/claims-arguments-evidence-cae/

assumido (subalegações ou evidências) e a alegação a ser investigada (a reinvindicação), como por exemplo “o uso de criptografia é obrigatório”.

Evidência - é um artefato que estabelece fatos nos quais se pode confiar e confirma a reivindicação. Muitas fontes podem ser utilizadas para extrair artefatos para as evidências, o que torna essa evidência válida é o apoio ou refutação que ela fornece a uma reivindicação, como por exemplo “um print do algoritmo de criptografia utilizado no sistema”.

A Figura 10 ilustra os componentes da abordagem CAE.

Figura 10 - Exemplo de CAE



Fonte: Traduzido de CAE Frameworks (2021).

A abordagem CAE foi desenvolvida pela Adelard, empresa associada à City University em Londres, Reino Unido a qual disponibiliza a ferramenta ASCE para tal modelagem.

Para promover a padronização e interoperabilidade, foi especificado pelo Grupo de Gerenciamento de Objetos (OMG) um Metamodelo de Caso de Garantia, no inglês Structured Assurance Case Metamodel (SACM) para a representação de casos de garantia GSN e CAE, o qual é abordado no próximo conteúdo.

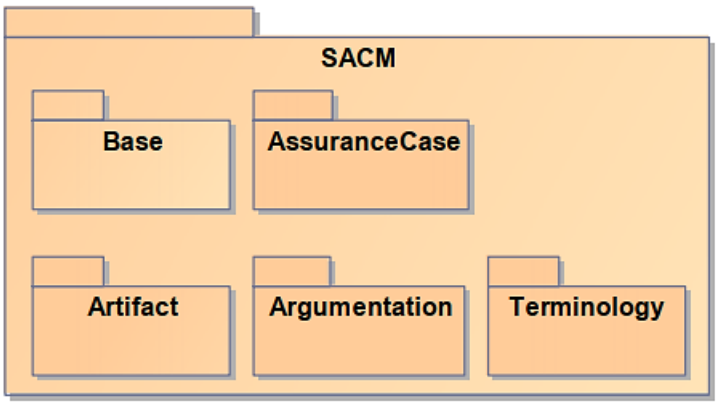
2.5.4 Structured Assurance Case Metamodel (SACM)

O SACM é um metamodelo desenvolvido para representar casos de garantia, com o objetivo de facilitar projetos, permitindo a comunicação de forma sucinta e estruturada como

seus sistemas e serviços (OMG *GROUP et al.*, 2020).

Para Yan (2020), SACM é uma linguagem de modelagem e pode criar um modelo legível por máquina que facilita a troca de informações entre várias partes interessadas no sistema. O SACM é constituído por cinco componentes: (1) o pacote "AssuranceCase" representa o módulo de caso de garantia e fornece uma visão de como ele é organizado; (2) o componente "Base" define os elementos fundamentais do SACM, como nomes e descrições de elementos; (3) o componente "Artefato" captura os conceitos usados para fornecer evidências para os argumentos feitos para as propriedades do sistema, promovendo a modularidade; (4) o componente "Terminologia" captura os conceitos usados para expressar as reivindicações relacionadas às propriedades do sistema, permitindo que os usuários decifrem o vocabulário controlado utilizado para descrever a argumentação com maior precisão; e (5) o componente "Argumentação" captura os conceitos usados na argumentação (necessários para modelar argumentos estruturados) relativos às propriedades do sistema (WEI *et al.*, 2019). Esses componentes são elucidados na Figura 11.

Figura 11 - Componentes do SACM



Fonte: Wei *et al.* (2019).

Em abril de 2020 a OMG disponibilizou a versão 2.1 do SACM a qual apresenta conformidade com os tipos de modelo: Modelo de Argumentação, Modelo de artefato, Modelo de Caso de Garantia e Modelo de Terminologia (OMG *GROUP et al.,* 2020). Para essa versão, recursos que não eram suportados anteriormente pelo GSN e CAE foram avaliados e incluídos no SACM. Uma seleção de tais recursos foram resumidos por Wei *et al.* (2019), conforme seguem descritos:

a) Modularidade: esta versão refina a modularidade de forma que é possível declarar seletivamente os elementos de argumento/artefato/terminologia externamente, e em seguida, relacioná-los, proporcionando, assim, melhor entendimento sobre a integração dos casos de

garantia;

b) Suporte a vários idiomas: suporte para vários idiomas não somente para descrever argumentos em várias línguas naturais, mas também para descrever argumentos usando linguagens de computador;

c) Vocabulário controlado: disponibiliza aos usuários, a opção de criação de vocabulário controlado;

d) Descrição o nível de confiança em argumentos: possibilidade de associar níveis de confiança, permitindo que os usuários discutam o nível de confiança para elementos de argumento;

e) Contra-argumentos em casos de garantia: possibilidade de declarar um argumento de reversão;

f) Rastreabilidade da evidência ao artefato: rastreabilidade naturalmente suportada sem a necessidade de um modelo externo, permitindo a rastreabilidade da evidência até o artefato real;

g) Instanciação de caso de garantia automatizada: permite a reutilização dos casos de garantia.

Wei *et al.* (2019) conclui que o SACM fornece uma base sólida para garantia de sistema com base em modelo, devido à variedade de recursos que foram avaliados e adicionados a ele, a partir de experiências de duas notações de caso de garantia bem estabelecidas: GSN e CAE.

Sendo assim, pode-se verificar que o SACM não oferece o processo para o gerenciamento de evidência, mas oferece meios para modelar e padronizar as abordagens de notações gráficas, que permitem vincular modelos e automatizar funcionalidades de casos de garantia.

3 REVISÃO SISTEMÁTICA DE LITERATURA

Com o propósito de identificar o ineditismo e a originalidade desta tese, foi realizada uma Revisão Sistemática de Literatura (RSL) para identificar trabalhos relacionados ou similares ao proposto. A escolha pela RSL se dá por tratar de uma modalidade de pesquisa que utiliza protocolos definidos para dar coerência a um conjunto de documentos. Nessa perspectiva, a RSL desenvolvida para esta pesquisa foi realizada com base no trabalho de Galvão e Pereira (2014), sintetizada nas seguintes etapas: (i) elaboração da pergunta de pesquisa que se pretende responder; (ii) seleção das bases e definição das estratégias a serem adotadas nas buscas; (iii) execução da busca na literatura; (iv) definição dos critérios de inclusão e exclusão a serem adotados para selecionar os artigos; (v) extração dos artigos conforme os critérios definidos; (vi) elaboração dos resumos dos artigos selecionados e publicação dos resultados.

A questão definida para nortear a realização da RSL foi: Quais os estudos publicados que contemplam abordagens de gerenciamento de evidências para auxiliar na validação de requisitos relacionados à proteção e privacidade de dados?

Para responder à referida questão, foram realizadas buscas nas seguintes bases de dados: IEEE *Xplore Digital Library* (IEEE); *Information Science & Technology Abstracts* (ISTA); *Library, Information Science & Technology Abstracts* (LISTA), *Proquest Dissertations & Theses Global* (PROQUEST); SCOPUS e *Web of Science* (WoS).

Para a escolha das bases considerou-se o reconhecimento nacional e internacional e as que indexam um número significativo de periódicos relacionados à temática da pesquisa. Para otimizar as buscas nas bases de periódicos, contemplando o maior número de publicações possíveis, foram adotados dois grupos de termos por assunto para serem utilizados combinados, conforme apresentado no Quadro 10.

Quadro 10 - Grupo de termos por assunto para a RSL

Grupo de termos Assuntos 1 **Proteção e Privacidade de Dados**	**Grupo de termos Assuntos 2** **Evidências**
"*Data Protection*"; "*Data privacy*"; "*General data Protection Regulation*"; GDPR; "*Privacy Framework*"; "*Privacy Model*".	"*Evidence Management*"; "*Assurance case*"; "*Safety evidence*"; "*Privacy by evidence*"

Fonte: Elaborado pela autora (2021).

As pesquisas nas bases de periódicos foram realizadas entre os dias 2 e 3 de março de

2021 e os termos pesquisados foram adequados conforme as configurações fornecidas pelas bases de dados. Os campos utilizados para as buscas foram o título, abstract e as palavras-chave nas bases IEEE, PROQUEST, SCOPUS e WoS. Nas bases ISTA e LISTA as buscas foram realizadas considerando o texto completo, com o intuito de obter resultados de trabalhos que possam ter utilizados termos distintos sobre a temática. No Quadro 11 são apresentadas as estratégias utilizadas para as buscas nas bases de periódicos.

Quadro 11 - Bases de periódicos e as estratégias de busca

Bases	Quantidade de Artigos	Estratégia de Busca
IEEE	233	(“Document Title”:“Data Protection” OR “Document Title”:“Data privacy” OR “Document Title”:“General data Protection Regulation” OR “Document Title”:GDPR OR “Document Title”:“Privacy Framework” OR “Document Title”:“Privacy Model”) AND (“Document Title”:“Evidence management” OR “Document Title”:“Assurance case” OR “Document Title”:“Safety evidence” OR “Document Title”:“Privacy by evidence”) (“Author keywords”:“Data Protection” OR “Author keywords”:“Data privacy” OR “Author keywords”:“General data Protection Regulation” OR “Author keywords”:GDPR OR “Author keywords”:“Privacy Framework” OR “Author keywords”:“Privacy Model”) AND (“Author keywords”:“Evidence management” OR “Author keywords”:“Assurance case” OR “Author keywords”:“Safety evidence” OR “Author keywords”:“Privacy by evidence”) (“Abstract”:“Data Protection” OR “Abstract”:“Data privacy” OR “Abstract”:“General data Protection Regulation” OR “Abstract”:GDPR OR “Abstract”:“Privacy Framework” OR “Abstract”:“Privacy Model”) AND (“Abstract”:“Evidence management” OR “Abstract”:“Assurance case” OR “Abstract”:“Safety evidence” OR “Abstract”:“Privacy by evidence”) (“Index Terms”:“Data Protection” OR “Index Terms”:“Data privacy” OR “Index Terms”:“General data Protection Regulation” OR “Index Terms”:GDPR OR “Index Terms”:“Privacy Framework” OR “Index Terms”:“Privacy Model”) AND (“Index Terms”:“Evidence management” OR “Index Terms”:“Assurance case” OR “Index Terms”:“Safety evidence” OR “Index Terms”:“Privacy by evidence”)

ISTA	0	TI (“Data Protection” OR “Data privacy” OR GDPR OR “General data Protection Regulation” OR “Privacy Framework” OR “Privacy Model”) AND TI (“Evidence management” OR “Assurance case” OR “Safety evidence” OR “Privacy by evidence”) Limitadores: Data de publicação: 20000101-20201231 Tipo de documento: Article AB (“Data Protection” OR “Data privacy” OR GDPR OR “General data Protection Regulation” OR “Privacy Framework” OR “Privacy Model”) AND AB (“Evidence management” OR “Assurance case” OR “Safety evidence” OR “Privacy by evidence”) Limitadores: Data de publicação: 20000101-20201231 Tipo de documento: Article KW (“Data Protection” OR “Data privacy” OR GDPR OR “General data Protection Regulation” OR “Privacy Framework” OR “Privacy Model”) AND KW (“Evidence management” OR “Assurance case” OR “Safety evidence” OR “Privacy by evidence”) Limitadores: Data de publicação: 20000101-20201231 Tipo de documento: Article SU (“Data Protection” OR “Data privacy” OR GDPR OR “General data Protection Regulation” OR “Privacy Framework” OR “Privacy Model”) AND SU (“Evidence management” OR “Assurance case” OR “Safety evidence” OR “Privacy by evidence”) Limitadores: Data de publicação: 20000101-20201231 Tipo de documento: Article TX (“Data Protection” OR “Data privacy” OR GDPR OR “General data Protection Regulation” OR “Privacy Framework” OR “Privacy Model”) AND TX (“Evidence management” OR “Assurance case” OR “Safety evidence” OR “Privacy by evidence”) Limitadores: Data de publicação: 20000101-20201231 Tipo de documento: Article
LISTA	1	TI (“Data Protection” OR “Data privacy” OR GDPR OR “General data Protection Regulation” OR “Privacy Framework” OR “Privacy Model”) AND TI (“Evidence management” OR “Assurance case” OR “Safety evidence” OR “Privacy by evidence”) Limitadores: Data de publicação: 20000101-20201231 Tipo de documento: Article AB (“Data Protection” OR “Data privacy” OR GDPR OR “General data Protection Regulation” OR “Privacy Framework” OR “Privacy Model”) AND AB (“Evidence

		management” OR “Assurance case” OR “Safety evidence” OR “Privacy by evidence”) Limitadores: Data de publicação: 20000101-20201231 Tipo de documento: Article KW (“Data Protection” OR “Data privacy” OR GDPR OR “General data Protection Regulation” OR “Privacy Framework” OR “Privacy Model”) AND KW (“Evidence management” OR “Assurance case” OR “Safety evidence” OR “Privacy by evidence”) Limitadores: Data de publicação: 20000101-20201231 Tipo de documento: Article SU (“Data Protection” OR “Data privacy” OR GDPR OR “General data Protection Regulation” OR “Privacy Framework” OR “Privacy Model”) AND SU (“Evidence management” OR “Assurance case” OR “Safety evidence” OR “Privacy by evidence”) Limitadores: Data de publicação: 20000101-20201231 Tipo de documento: Article TX (“Data Protection” OR “Data privacy” OR GDPR OR “General data Protection Regulation” OR “Privacy Framework” OR “Privacy Model”) AND TX (“Evidence management” OR “Assurance case” OR “Safety evidence” OR “Privacy by evidence”) Limitadores: Data de publicação: 20000101-20201231 Tipo de documento: Article
PROQUEST	0	noft(“Data Protection” OR “Data privacy” OR GDPR OR “General data Protection Regulation” OR “Privacy Framework” OR “Privacy Model”) AND noft(“Evidence management” OR “Assurance case” OR “Safety evidence” OR “Privacy by evidence”)
SCOPUS	7	(TITLE-ABS-KEY({Data Protection} OR {Data privacy} OR gdpr OR {General data protection regulation} OR {Privacy Framework} OR {Privacy Model}) AND TITLE-ABS-KEY({Evidence management} OR {Assurance case} OR {Safety evidence} OR {Privacy by evidence})) AND PUBYEAR > 2010 AND PUBYEAR < 2021
WoS	0	TÓPICO=(“Data Protection” OR “Data privacy” OR GDPR OR “General data Protection Regulation” OR “Privacy Framework” OR “Privacy Model”) AND TÓPICO=(“Evidence management” OR “Assurance case” OR “Safety evidence” OR “Privacy by evidence”) Índices=SCI-EXPANDED, SSCI, A&HCI, CPCI-S, CPCI-SSH, ESCI Tempo estipulado=2010-2020

Fonte: Elaborado pela autora (2021).

As buscas na WoS não foram limitadas somente a artigos, visto que as mesmas não

resultaram em nenhum artigo encontrado. Por esse motivo, procurou-se ampliar o escopo das buscas na tentativa de obter melhores resultados.

Como critérios de inclusão foi configurado, nas bases de dados, o intervalo para as buscas entre os anos de 2010 e 2020, considerando a atualidade do tema pesquisado, em documentos que fossem do tipo, publicações em periódicos ou publicações em anais de congressos e publicações nos idiomas português, inglês ou espanhol. No Quadro 12 apresenta-se, para cada uma das bases de dados, considerando as estratégias de busca apresentadas no Quadro 11, o campo pesquisado e os resultados quantitativos de acordo com as estratégias definidas.

Quadro 12 - Resultados quantitativos da RSL

Bases	**Campos de Busca**					**TOTAL**
	Título	**Resumo**	**Palavra-chave**	**Termos Indexados**	**Texto Completo**	
IEEE	x	x	x	x	-	233
ISTA	x	x	x	-	x	0
LISTA	x	x	x	x	x	1
PROQUEST	x	x	x	-	-	0
SCOPUS	x	x	x	-	-	7
WoS	x	x	x	-	-	0
					TOTAL	241

Fonte: Elaborado pela autora (2021).

Conforme pode ser observado no Quadro 12, o total de publicações encontradas nas seis bases consultadas foi de 241. Após a busca em cada uma das bases, as 241 publicações dos periódicos foram analisadas para identificar e excluir os resultados que apareceram erroneamente, tais como constando apenas índices/nome de eventos etc. e foram exportadas para a ferramenta *Mendeley Desktop* para identificar as duplicidades. Com a exclusão dos erros e as publicações duplicadas, resultaram 191 publicações de periódicos.

Posteriormente, foi executado o primeiro ciclo de leitura o qual avaliou os títulos, resumos, palavras-chave e conclusões de todas as publicações resultantes e foram excluídas as que não tratavam de assuntos relacionados especificamente sobre o uso de evidências no contexto da proteção e privacidade de dados, mecanismos relacionados à prestação de contas de conformidade de maneira geral e casos de garantia no contexto da segurança da informação e/ou proteção de dados. O resultado dessa primeira análise foi a exclusão de 167 artigos, resultando em 24 trabalhos. Durante a leitura dos artigos e em observância às citações dos mesmos, identificou-se uma tese de interesse, a qual foi incluída nas leituras e segue disposta

no item 2 do Quadro 13.

Quadro 13 - Trabalhos resultantes do primeiro ciclo de leitura da RSL

N.	Título	Autores	Ano	Base de Dados
1	Blockchain based trust management mechanism for IoT	Asma Lahbib; Khalifa Toumi; Anis Laouiti; Alexandre Laube; e Steven Martin	2019	IEEE
2	Privacy by Evidence: a software development methodology to provide privacy assurance	Pedro Yóssis Silva Barbosa	2018	CAPES
3	Assurance of security and privacy requirements for cloud deployment models	Islam Shareeful; Moussa Ouedraogo; Christos Kalloniatis; Haralambos Mouratidis; e Stefanos Gritzalis	2018	IEEE
4	Optimal evidence collection for accountability in the cloud	Fatma Masmoudi; Mohamed Sellami; Monia Loulou; e Ahmed Hadj Kacem	2018	IEEE
5	Towards a security assurance framework for connected vehicles	Panagiotis Pantazopoulos; Sammy Haddad; Costas Lambrinoudakis; Christos Kalloniatis; Konstantinos Maliatsos; Athanasios Kanatas; Andras Varádi; Matthieu Gay; e Angelos Amditis	2018	IEEE
6	Trust and reputation management in healthcare systems: taxonomy, requirements and open issues	Farhana Jabeen; Zara Hamid; Adnan Akhunzada; Wadood Abdul; e Sanaa Ghouzali	2018	IEEE
7	A Literature study on privacy patterns research	Jörg Lenhard; Lothar Fritsch; e Sebastian Herold	2017	IEEE
8	A thought experiment on evolution of assurance cases: From a logical aspect	Shuji Kinoshita e Yoshiki Kinoshita	2017	Scopus
9	Evidence-based trust mechanism using clustering algorithms for distributed storage systems	Giulia Traverso; Carlos Garcia Cordero; Mehrdad Nojoumian; Reza Azarderakhsh; Denise Demirel; Sheikh Mahbub Habib; e Johannes Buchmann	2017	IEEE

10	Managing assurance cases in model based software systems	Sahar Kokaly	2017	IEEE
11	Uniform model interface for assurance case integration with system models	Andrezej Wardziński; e Paul Jones	2017	Scopus
12	Using an assurance case framework to develop security strategy and policies	Robin Bloomfield; Peter Bishop P.; Eoin Butler; e Kate Netkachova	2017	Scopus
13	Model management for regulatory compliance: a position paper	Sahar Kokaly; Rick Salay; Mehrdad Sabetzadeh; Marsha Chechik; e Tom Maibaum	2016	IEEE
14	Secure and privacy preserving protocol for cloud-based vehicular DTNs	Jun Zhou; Xiaolei Dong; Zhenfu Cao; e Athanasios V. Vasilakos	2015	IEEE
15	The Importance of Security Cases: Proof Is Good, But Not Enough	John Knight	2015	IEEE
16	An authentication and auditing architecture for enhancing security on e-government services	Denys A. Flores	2014	IEEE
17	An Interactive Trust Model for Application Market of the Internet of Things	Kai Kang; Zhibo Pang; Li Da Xu; Liya Ma; e Cong Wang	2014	IEEE
18	Privacy: a review of publication trends	Charlie Hinde; e Jacques Ophoff	2014	IEEE
19	Accountable cloud	Ashish Gehani; Gabriela F. Ciocarlie; e Natarajan Shankar	2013	IEEE
20	Supporting Cloud Accountability by Collecting Evidence Using Audit Agents	Thomas Ruebsamen; e Christoph Reich	2013	IEEE
21	Combined safety and security certification	G. Romanski	2012	IEEE
22	Evidence-Based Elections	Philip B. Stark; e David Wagner	2012	IEEE
23	Hybrid scheme for trust management in pervasive computing	Abubakr Sirageldin; Baharum Baharudin; e Low Tang Jung	2012	IEEE
24	What does the assurance case approach deliver for critical information infrastructure protection in cybersecurity?	AC Goodger; NHM Caldwell; e JT Knowles	2012	IEEE

25	Towards a privacy management framework for distributed cybersecurity in the new data ecology	Travis D. Breaux; e Catherine B. Lotrionte	2011	IEEE

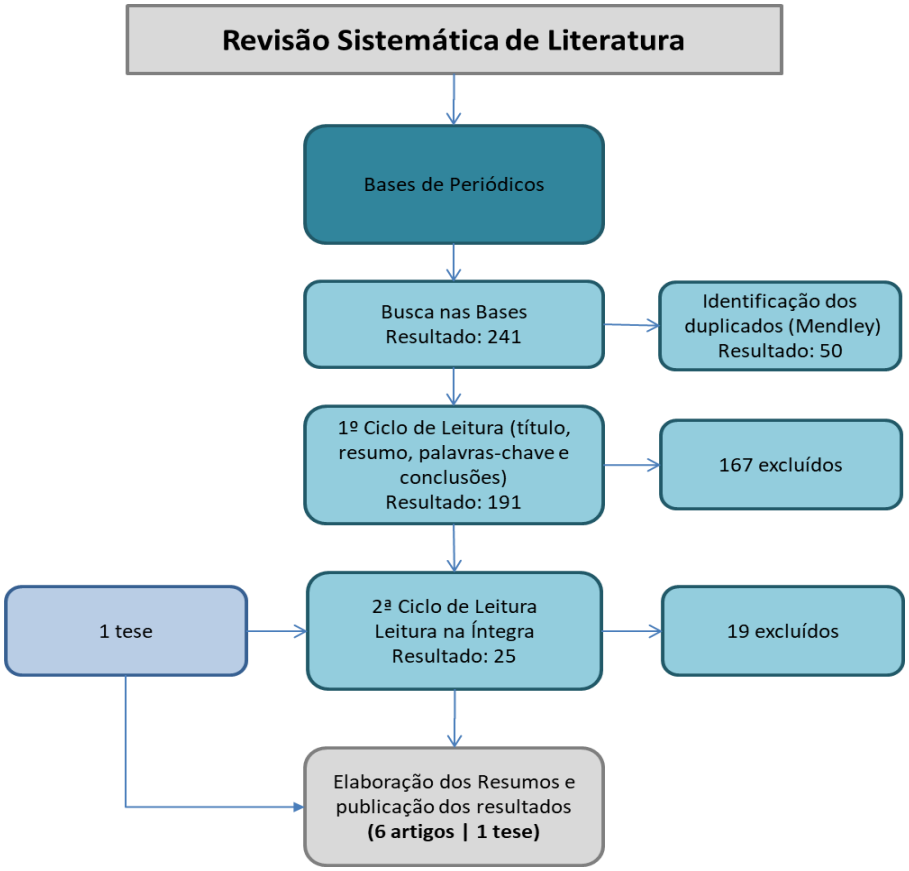
Fonte: Elaborado pela autora (2021).

Os 25 trabalhos apresentados no Quadro 13 foram lidos na íntegra no segundo ciclo de avaliação e nesta etapa foram excluídos os estudos que não apresentaram:

a) Abordagens utilizando artefatos/evidências para avaliação, validação ou aferição de proteção e privacidade de dados
b) Mecanismos relacionados à prestação de contas a conformidade de maneira geral com normativas de segurança da informação e privacidade de dados;
c) Casos de garantia no contexto da segurança da informação e/ou proteção de dados; e
d) Aplicação das abordagens propostas e os resultados obtidos;

Após a leitura, aplicando os critérios de exclusão citados acima, foram obtidos como resultado final seis artigos e uma tese. A Figura 12 apresenta o resumo do número de estudos retornados em cada etapa de condução da RSL.

Figura 12 - Número de publicações conforme condução da RSL



Fonte: Elaborada pela autora (2021).

Dessa forma, foi possível selecionar somente os artigos que atenderam aos critérios de seleção anteriormente especificados e possíveis de responderem às questões da RSL. Os artigos selecionados são apresentados no Quadro 14, entretanto, não foram encontrados assuntos análogos à temática desta pesquisa, mas foram encontrados estudos que apresentaram alguma relação com o modelo proposto nesta tese.

Quadro 14 - Trabalhos relacionados

N.	Título	Autores	Ano	Base de Dados
1	Blockchain based trust management mechanism for IoT	Lahbib *et al.*	2019	IEEE
2	Assurance of security and privacy requirements for cloud deployment models	Shareeful *et al.*	2018	IEEE
3	Optimal evidence collection for accountability in the cloud	Masmoudi *et al.*	2018	IEEE
4	Managing assurance cases in model based software systems	Kokaly	2017	IEEE
5	Accountable clouds	Gehani, Ciocarlie e Shankar.	2013	IEEE
6	What does the assurance case approach deliver for critical information infrastructure protection in cybersecurity?	Goodger, Caldwell e Knowles	2012	IEEE
7	Privacy by evidence: a software development methodology to provide privacy assurance	Barbosa	2018	CAPES

Fonte: Elaborado pela autora (2021).

3.1 TRABALHOS RELACIONADOS

No estudo realizado por Lahbib *et al.* (2019), os autores propõem um sistema de gestão de confiança no contexto de "Internet das Coisas"[2] com base na tecnologia Blockchain, para garantir confiabilidade da informação durante seu compartilhamento e armazenamento. Para isso, os autores aproveitam as vantagens dos recursos de segurança que a tecnologia Blockchain oferece em relação à confiabilidade, rastreabilidade, integridade da informação e a não possibilidade de adulteração de dados de prova, propondo uma arquitetura para coletar

[2] "A Internet das Coisas (IoT) descreve a rede de objetos físicos incorporados a sensores, software e outras tecnologias com o objetivo de conectar e trocar dados com outros dispositivos e sistemas pela internet. Esses dispositivos variam de objetos domésticos comuns a ferramentas industriais sofisticadas". Fonte: https://www.oracle.com/br/internet-of-things/what-is-iot/

evidências das entidades de um cenário Internet das Coisas, definindo uma pontuação de confiança para cada dispositivo e, assim, permitindo uma relação de confiança entre eles. A relação desse trabalho com ao que se propõe nesta tese é o uso de evidências, mas como prova de resiliência, no artigo as evidências são utilizadas para pontuar e classificar uma entidade/componente como confiável ou não, porém ele não relaciona a arquitetura com o atendimento a uma normativa e também não propõe formas de gerenciar as evidências para apoiar na comprovação de conformidade.

No contexto do uso de evidências para comprovar a garantia de proteção e privacidade de dados no âmbito da computação em nuvem estão os estudos de: Shareeful *et al.* (2018); Masmoudi *et al.* (2018) e Gehani, Ciocarlie e Shankar. (2013). O trabalho de Shareeful *et al.* (2018) propõe uma abordagem metodológica e sistemática que considera conceitos de engenharia de requisitos para estruturar os requisitos de segurança e privacidade, utilizando evidências para apoiar na análise e comprovação de garantia e mecanismos de auditoria. O objetivo dos autores é apoiar no processo de migração e escolha de soluções de nuvem com métricas que auxiliem na seleção dos modelos de nuvem que melhor atenda as expectativas de segurança e privacidade do consumidor da nuvem. Para isso, utiliza como parte do processo, a análise de evidências como garantia de segurança e privacidade. O trabalho não aplica requisitos de normativas, seu objetivo é permitir que os usuários da nuvem definam seus requisitos de garantia conforme o contexto organizacional e selecione os modelos de nuvem mais apropriados a eles. O ponto de associação desse trabalho com esta tese está no uso de evidências como prova de garantia de segurança e privacidade, porém não apresentam abordagem para gerenciá-las e também não adotam nenhuma fonte regulatória para suportar os processos propostos.

Por sua vez, Masmoudi *et al.* (2018) propõem uma abordagem para otimização na coleta das evidências em serviços de nuvem multilocatário, com o objetivo de contribuir na comprovação de ocorrência de uma violação no ambiente. Diante da grande quantidade de evidências disponíveis durante um incidente, usando um programa linear, o artigo apresenta um método para a coleta somente das evidências mínimas necessárias para qualificar uma violação. Utilizam os elementos-chave da GDPR como base para fazer a seleção das evidências. A relação desse trabalho com a pesquisa a ser desenvolvida aqui refere-se ao uso de evidências e de uma fonte regulatória como base para a proposta da abordagem. Porém, o artigo é focado em serviços de nuvem e não apresenta abordagens para gerenciar as evidências, e sim para a coleta e análise das mesmas.

Gehani, Ciocarlie e Shankar (2013) propõem um conjunto de mecanismos para

aprimorar o nível de segurança da tecnologia de computação em nuvem com foco em auditoria forense. Para os autores, a garantia de segurança na computação em nuvem deve ser formalizada em cláusulas de SLA. Nesse trabalho são apresentadas as etapas que apoiam a coleta proativa de evidências forenses para que, em caso de violações de segurança, a estrutura esteja preparada para validar ou repudiar uma reivindicação de incidente. Os mecanismos propostos pelos autores incluem: mapeamento de lei em requisitos probatórios, uso de criptografia como forma de proteção das evidências, trilhas de auditoria para serem oferecidos em níveis diversos, de acordo com o nível de segurança forense necessário a cada cliente. Esse trabalho não utiliza casos de garantia em sua abordagem e sua relação com esta tese se dá na possibilidade de mapear requisitos de fontes regulatórias para direcionar a extração de evidência e o uso dessas como prova de conformidade e resiliência.

Voltado ao processo de desenvolvimento de sistemas e com foco em prover a conformidade de softwares com padrões regulamentadores, Kokaly (2017) apresenta a aplicação de técnicas de gestão do modelo para apoiar a gestão de casos de garantia no contexto de conformidade regulamentar. Apresenta o trabalho realizado que aborda o desafio de reutilizar e gerenciar casos de garantia de acordo com a evolução dos sistemas. Utiliza o GSN como proposta de modelagem e assume que um caso de garantia pode ser modelado de diversas maneiras, desde que apresente os componentes principais: reivindicações, argumentos e evidências. Kokaly (2017) não utiliza normativas de proteção e privacidade de dados em sua proposta e, sim, um padrão normativo para segurança de veículos rodoviários, na validação. O relacionamento identificado no trabalho do autor com esta pesquisa se refere ao uso de casos de garantia e a utilização de evidências como artefato de argumentação de uma reivindicação em um contexto de conformidade regulatória.

Por sua vez, Barbosa (2018) propôs em sua tese de doutorado uma metodologia de desenvolvimento de software para orientar desenvolvedores na aplicação de regras e técnicas de privacidade. O intuito da metodologia proposta é prover privacidade em um conceito de privacidade por evidência (*Privacy by Evidence*). Preconiza que as documentações de mitigação sejam em forma de evidência de privacidade, contempla a notação de casos de garantia GSN e está de acordo com os sete princípios definidos pelo conceito *de Privacy by Design*, porém não adota uma fonte regulatória de proteção e privacidade de dados, mas todo o trabalho é voltado em atender padrões, normativas e legislações sobre o tema. A relação desse trabalho com esta tese esta na utilização de evidências como prova de conformidade com a privacidade, o uso de notações de casos de garantia como uma de suas abordagens, uso de *Privacy by Design* e a privacidade como foco da metodologia proposta.

Já no contexto de cibersegurança, o trabalho de Goodger, Caldwell e Knowles (2012) apresentam uma abordagem de caso de garantia adaptada e aplicada à segurança cibernética, que se propõe a fornecer uma supervisão integrada combinando proteção e confiabilidade em uma única estrutura. Usando o conceito de malha, os autores integram casos de garantia, os quais resumem em uma visão global de um ambiente. Para isso foram combinados o ciclo de aprendizagem organizacional e um processo constituído de seis etapas com base nas estruturas de notação *Goal Structuring Notation* (GSN) e *Claim, Argument, Evidence* (CAE). A relação do artigo com esta pesquisa está no uso de estrutura de notações com base em evidências para a comprovação de segurança, porém os autores não adotam fontes regulatórias e a privacidade de dados como parâmetro na aplicação da abordagem proposta.

Conforme apresentado, os assuntos proteção e privacidade de dados relacionados com o uso de evidências, dentre os trabalhos selecionados, aparecem aplicados no contexto de Internet das Coisas, computação em nuvem, processo de desenvolvimento de sistemas e aplicada em infraestrutura de cibersegurança. O Quadro 15 apresenta um comparativo desses trabalhos, que sintetiza os seguintes aspectos: o domínio de aplicação das propostas de cada estudo, se mencionam alguma fonte regulatória de proteção e privacidade de dados e se utilizam abordagens de casos de garantia em suas propostas.

Quadro 15 - Comparativo entre os trabalhos relacionados

Estudos	**Domínio de Aplicação**	**Menção a Fontes Regulatórias**	**Abordagens de Caso de Garantia**
Lahbib *et al.* (2019)	IoT	-	-
Shareeful *et al.* (2018)	Computação em nuvem	-	-
Masmoudi *et al.* (2018)	Computação em nuvem	GDPR	-
Gehani, Ciocarlie e Shankar (2013)	Computação em nuvem	HIPAA	-
Kokaly (2017)	Desenvolvimento de Sistemas	-	GSN
Barbosa (2018)	Desenvolvimento de Sistemas	HIPAA, GDPR	GSN
Goodger, Caldwell e Knowles (2012)	Cibersegurança	-	GSN e CAE

Fonte: Elaborado pela autora (2021).

Diante do exposto e em resposta à questão que norteou a realização da RSL, observa-se que a literatura fornece trabalhos que enfocam o uso de evidências para comprovar requisitos de proteção e privacidade de dados nos contextos apresentados acima, os quais apresentam alguma relação com o modelo a ser apresentado nesta tese, entretanto, tais trabalhos não

apresentam propostas estruturadas que assemelhe a esta pesquisa. Os trabalhos relacionados apresentam suas propostas para aplicação em escopos específicos e não contemplam uma abordagem metodológica detalhada para estruturar artefatos que possam ser utilizados como evidências na comprovação de conformidade com normativas de proteção e privacidade de dados, tampouco modelos para gerenciá-las, aplicáveis a processos, sistemas, serviços e ambiente. Assim, esta pesquisa avança os estudos nessa direção.

4 PROCEDIMENTOS METODOLÓGICOS

Nesta seção são apresentados os procedimentos metodológicos adotados para a realização deste trabalho com o intuito de responder à questão de pesquisa e atender os objetivos deste projeto. Os procedimentos metodológicos consistem em explicar detalhadamente as ações desenvolvidas no trabalho de pesquisa, ou seja, a metodologia utilizada em seu desenvolvimento. Para Deslandes (1994, p. 16), "a metodologia é o caminho do pensamento e a prática exercida na abordagem da realidade".

4.1 CARACTERIZAÇÃO DA PESQUISA

A caracterização da pesquisa pode ser classificada quanto à sua: natureza, abordagem, objetivos e procedimentos. O Quadro 16 apresenta a classificação adotada e o método utilizado para o direcionamento das atividades.

Quadro 16 - Caracterização da pesquisa

Quanto à Natureza	Pesquisa Aplicada
Quanto à Abordagem do Problema	Pesquisa Mista - Qualitativa e Quantitativa
Quanto aos Objetivos	Pesquisa Exploratória e Descritiva
Quanto aos Procedimentos Técnicos	Pesquisa Bibliográfica Revisão Sistemática de Literatura Pesquisa com Especialistas Pesquisa Experimental Observação Sistemática
Instrumentos de Pesquisa	Entrevista estruturada Apresentação Formulários Questionário Painel com Especialistas
Método de Pesquisa	DSR *(Design Science Research)*

Fonte: Elaborado pela autora (2022).

Esta pesquisa é classificada como aplicada quanto à sua natureza. De acordo com Silva e Menezes (2005, p. 20), uma pesquisa aplicada "objetiva gerar conhecimentos para aplicação prática, dirigidos à solução de problemas específicos. Envolve verdades e interesses locais". Neste estudo, a pesquisa aplicada está presente na proposição de elaboração de um modelo para o gerenciamento de evidências no âmbito de proteção e privacidade de dados para auxiliar no processo de comprovação das alegações de conformidade, com o intuito de solucionar problemas reais.

Conforme definido por Creswell (2010), pesquisas de métodos mistos possuem uma

abordagem de investigação que combinam ou associam as formas da pesquisa qualitativa e da quantitativa no mesmo estudo. Para Knechtel (2014), a pesquisa quantitativa atua sobre um problema humano ou social, com base no teste de uma teoria e composta por variáveis quantificadas em números, as quais são analisadas de modo estatístico, com o objetivo de determinar se as generalizações previstas na teoria se sustentam ou não. Já a pesquisa qualitativa, segundo Goldenberg (1997, p. 34), não se preocupa com a representatividade numérica, mas, sim, com o aprofundamento da compreensão de um grupo social, de uma organização, sendo considerada uma forma adequada para entender a natureza de um fenômeno social (RICHARDSON, 1999). Diante do exposto, quanto à abordagem do problema, este estudo utiliza métodos mistos, sendo classificado como quantitativa e qualitativa. A abordagem quantitativa se relaciona com todo o processo de desenvolvimento do modelo proposto, desde a sua definição até sua concepção. Já a abordagem qualitativa está relacionada com a etapa de avaliação do modelo, a qual foi realizada por especialistas, através da aplicação de um questionário cujas respostas foram analisadas utilizando métodos qualitativos.

Do ponto de vista dos objetivos, esta pesquisa é exploratória e descritiva. Exploratória, visto que, conforme Gil (2002), este tipo de pesquisa tem como objetivo proporcionar uma visão geral decorrente de uma realidade observada, além de obter maior familiaridade com o problema, para torná-lo mais explícito ou construir hipóteses. O autor complementa que a maioria das pesquisas exploratórias envolve: (a) levantamento bibliográfico; (b) entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado; e (c) análise de exemplos que visem à compreensão. É descritiva pois de acordo com Triviños (1987), este tipo de pesquisa apresenta uma série de informações sobre o que deseja pesquisar descrevendo os fatos e fenômenos de determinada realidade. A natureza exploratória e descritiva se dá por ter como parte do escopo, proporcionar mais familiaridade com o problema e torná-lo mais explícito descrevendo princípios, casos e abordagens relacionadas ao gerenciamento de evidências de proteção e privacidade de dados.

Quanto aos procedimentos técnicos, esta pesquisa é classificada como bibliográfica, experimental e utilizará a observação sistemática e a pesquisa com especialistas. Vergara (2007) apresenta que a pesquisa bibliográfica consiste na etapa inicial de todo trabalho científico, pois visa reunir informações acerca do assunto objeto do estudo. É desenvolvida com base em materiais publicados em livros, jornais, revistas, *sites* na Internet, disponibilizados ao público em geral. Neste estudo, a pesquisa bibliográfica está presente na elaboração da revisão de literatura, bem como auxiliou nas análises e no desenvolvimento do modelo a ser proposto.

A pesquisa com especialistas, segundo Santos (1999), é um procedimento útil

especialmente em pesquisas exploratórias e descritivas que buscam informações diretamente com um grupo de interesse nos dados que se deseja obter. Fonseca (2002) complementa que a pesquisa com especialistas utiliza questionários como um instrumento para se obter dados ou informações sobre características ou opiniões de determinado grupo de pessoas, indicado como representante de uma população-alvo. Com o intuito de identificar as práticas adotadas atualmente pelas organizações, foram aplicados questionários para identificar: a) os tipos de informações e artefatos que estão sendo coletados e preservados como evidências no âmbito da proteção e privacidade dos dados; b) as técnicas de estruturação e avaliação dessas evidências; c) as práticas que apoiam na gestão da evolução e mudanças ocorridas que possam afetar as evidências coletadas; d) os desafios que os profissionais enfrentam atualmente no preparo e na avaliação das evidências; e, e) os critérios exigidos na avaliação e validação das evidências. Ressalta-se que os objetivos desses questionários foi obter maior compreensão das práticas adotadas e utilizar as respostas como contribuição para o modelo proposto. A pesquisa com especialistas também foi adotada neste trabalho para a validação do modelo apresentado.

Já a pesquisa experimental, segundo Triviños (1987), segue um planejamento rigoroso em etapas, iniciando pela formulação exata do problema e das hipóteses as quais delimitarão as variáveis precisas e controladas que atuarão no fenômeno estudado. Corroborando a definição de Triviños, Gil (2007) apresenta que a pesquisa experimental consiste em determinar um objeto de estudo, selecionar as variáveis que serão capazes de influenciá-lo, definir as formas de controle e de observação dos efeitos que a variável produz no objeto. Sendo assim, pode-se dizer que esta pesquisa é considerada experimental, pois para a validação do modelo proposto foi realizada a sua aplicação em um cenário real, o que possibilitou a observação e identificação de melhorias durante o processo de utilização do mesmo.

No que envolve a técnica de observação sistemática, também é conhecida como direta ou estruturada, na qual define-se um conjunto de comportamento a ser observado, o momento adequado e a forma de registros dos dados coletados (YIN, 2005; VERGARA, 2012). A mesma foi utilizada para registrar em um formulário os pontos identificados durante a aplicação do modelo.

Ainda no que se refere à aplicação do modelo proposto, a entrevista estruturada foi utilizada como instrumento. Na entrevista estruturada as perguntas são predeterminadas, e o entrevistador (pesquisador) segue um roteiro previamente estabelecido registrando as respostas (LAKATOS; MARCONI, 2003; YIN, 2005). Os registros da entrevista de aplicação do modelo também foram realizados em formulários.

Outro procedimento técnico utilizado nesta pesquisa foi a realização de uma RSL para justificar seu ineditismo, a mesma foi apresentada no capítulo 3 deste trabalho. De acordo com Linde e Willich (2003), Petticrew e Roberts (2006) e Kitchenham *et al*. (2009), a RSL é um tipo de investigação científica que utiliza como fonte de dados a literatura existente sobre um tema específico, com o objetivo de reunir, avaliar criticamente e conduzir uma síntese dos resultados de múltiplos estudos primários. Esse tipo de pesquisa é guiado por uma pergunta claramente formulada, a qual pretende-se responder, e são utilizados métodos sistemáticos e explícitos para a busca, análise crítica e síntese dos estudos selecionados. Para Galvão e Pereira (2014), a RSL deve ser preparada de forma abrangente e não tendenciosa e os critérios adotados em sua execução devem ser divulgados para permitir que outros pesquisadores repitam o procedimento.

Já na avaliação do modelo foi utilizado o instrumento questionário para obter a opinião de especialista sobre a avaliação do modelo proposto. Para esta avaliação foi utilizado o método painel de especialista o qual consiste em reunir grupos de pessoas que trabalham em conjunto para executar uma determinada tarefa, fazer diagnósticos ou chegar a uma decisão (ROCHA; HONOTARO; COSTA, 2016). Os especialistas são profissionais capazes de avaliar as questões envolvidas no objetivo da pesquisa a que se propõem, analisando-as e expondo sua visão sobre o tema (PINHEIRO; FARIAS; LIMA, 2013).

Optou-se pela adoção do método *Design Science Research* (DSR) para a realização deste estudo. O DSR é considerado um método que busca responder a questões relevantes para os problemas humanos por meio da criação de artefatos inovadores, contribuindo, assim, com novos conhecimentos para o corpo de evidência científica (HEVNER; CHATTERJEE, 2010).

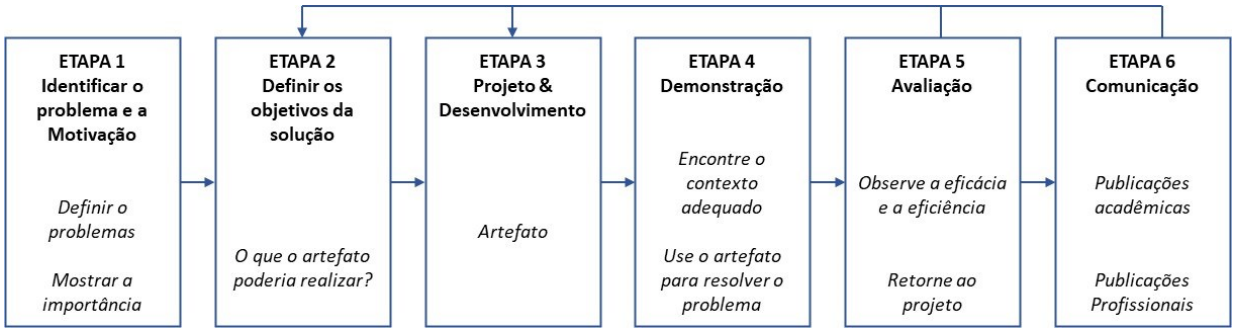
Na visão de Wieringa (2009), o DSR é um tipo de método destinado a resolver problemas, sendo eles: problemas práticos e problemas de conhecimento que se relacionam. Para o autor, os problemas práticos podem ser entendidos como a diferença entre como o mundo é vivido pelas partes interessadas e a forma que estas gostariam que fosse. E os problemas de conhecimento se referem à diferença entre o conhecimento atual das partes interessadas sobre o mundo e o conhecimento que gostariam de ter.

Hevner e Chatterjee (2010), Wieringa (2009) e Simon (1996) definem DSR como um paradigma de pesquisa pragmático, que demanda criação de artefatos inovadores para resolver problemas do mundo. Já para Van Aken (2005), o propósito do DSR é desenvolver conhecimento que pesquisadores e profissionais possam usar para coprojetar soluções e construir artefatos para tratar seus problemas de campo.

Este trabalho de pesquisa está alinhado aos propósitos do DSR, pelo cunho prático do modelo apresentado, uma vez que se propõe a desenvolver um modelo (artefato) inovador para gerenciar evidência de proteção e privacidade de dados, capaz de apoiar no desafio de comprovar conformidade com normativas de referência sobre o tema.

A aplicação das etapas do DSR é sintetizada por Peffers *et al.* (2007) e apresentado no *framework* da Figura 13.

Figura 13 - *Framework* metodológico para aplicação do *Design Science Research*



Fonte: Adaptado de Peffers *et al.* (2007).

Onde:

Etapa 1: Identificar o problema e motivação – define o problema específico da pesquisa e justifica o valor da solução. O problema será utilizado para desenvolver um artefato que possa efetivamente fornecer a solução;

Etapa 2: Definir objetivos e a solução – infere os objetivos de uma solução a partir da definição do problema e do conhecimento do que é possível e viável;

Etapa 3: Projetar e desenvolver o artefato – determina a funcionalidade desejada do artefato e sua arquitetura e, assim, cria o artefato real;

Etapa 4: Demonstrar o artefato na solução do problema – demonstração do uso do artefato para resolver uma ou mais instâncias do problema. Pode ser instanciado por experimentação, simulação, estudo de caso, prova ou outra atividade apropriada;

Etapa 5: Avaliar o artefato – observa e mensura como o artefato suporta a solução do problema, ressaltando-se que a natureza do local de pesquisa pode determinar se tal interação é viável ou não;

Etapa 6: Comunicar – comunicação do problema e sua importância, do artefato e sua utilidade e novidade, do rigor do projeto, e sua efetividade para pesquisadores e outros públicos relevantes, como profissionais e especialistas na área.

No que se refere aos artefatos que são desenvolvidos utilizando o DSR, March e Smith (1995) os abordam como produtos da pesquisa e os classificam em quatro tipos: estrutura, modelos, métodos e implementações. Os autores complementam que assim como nas ciências naturais, é necessário adotar uma base de conceito (estrutura), a qual caracteriza os fenômenos, sendo que estas podem ser combinadas e utilizadas para descrever tarefas, situações ou artefatos (modelos). Também podem ser desenvolvidos métodos que são maneiras de realizar atividades direcionadas a um objetivo, e todos eles podem ser instanciados em produtos específicos, ou implementações físicas destinadas a realizar certas tarefas. Já Vaishnavi e Kuechler (2015) especificam os artefatos do DSR como: construtos, modelos, f*rameworks*, arquiteturas, princípios de projeto, métodos, geradores de instância ou teorias de projeto.

Hevner *et al.* (2004), ao direcionarem o DSR para os feitos tecnológicos, entendem que artefatos de TI são amplamente definidos como: construções (vocabulário e símbolos), modelos (abstrações e representações), métodos (algoritmos e práticas) e instanciações (sistemas implementados e protótipos). Diante disso, buscou-se identificar na literatura a nomenclatura mais adequada para o artefato desenvolvido neste trabalho. Ao trazer a temática para reflexão na busca de identificar esta definição nos conceitos, os artefatos modelos e métodos se destacaram. Esta suposição se confirma ao considerar as definições de March e Smith (1995), os quais identificam modelos como declarações de problemas e soluções e entendem que são proposições de como as coisas são ou deveriam ser. Assim como a de Shehabuddeen *et al.* (1999) que incorporam as principais definições da literatura e sustentam que os modelos retratam a realidade com representações, são dinâmicos por natureza, apresentam as relações existentes entre diferentes elementos e preveem impactos que as mudanças em seus elementos podem causar. Com isso, os autores sumarizam seu propósito ao afirmar que "Um modelo apoia a compreensão da interação dinâmica entre os elementos de um sistema". (SHEHABUDDEEN *et al.*, 1999, p. 13).

Sobre os métodos, March e Smith (1995) explicam que são artefatos utilizados para apoiar a realização do modelo definido para a solução. Embora eles possam não estar explicitamente relacionados, as representações de tarefas e resultados são intrínsecas aos métodos. Os métodos podem ser vinculados a modelos particulares em que as etapas fazem parte do modelo. Além disso, os métodos são frequentemente usados para traduzir um modelo no decurso da resolução de um problema. Já Vaishnavi, Kuechler e Petter (2004) abordam os métodos como um conjunto de etapas usadas para realizar tarefas, ou seja, apresentam o conhecimento de como executá-las.

Diante do exposto, conclui-se que gerou-se nesta pesquisa dois tipos de artefatos: um **modelo** para gerenciar evidências de proteção e privacidade de dados e os **métodos** para sua aplicação. Além de propor representações para a solução de um problema, esta pesquisa apresenta um conjunto de informações a serem utilizadas para sua aplicação.

Ressalta-se que no decorrer deste documento, o artefato proposto é denominado apenas de **Modelo**, mas sua proposição é acompanhada de um método para sua aplicabilidade. Para cada camada e módulo definidos no modelo, é proposto o método de aplicação, ou seja, são apresentados: uma forma para realizar as ações específicas, e os instrumentos a serem adotados para alcançar o propósito da camada, tais como matrizes e formulários.

Além da utilização do DSR como procedimento metodológico, as atividades desta pesquisa foram planejadas a partir dos objetivos e dos resultados esperados os quais foram relacionados às técnicas e métodos adotados para a realização de cada um deles, conforme apresentados no Quadro 17.

Quadro 17 - Objetivos e resultados

Objetivo Geral Propor um modelo para o gerenciamento de evidências de proteção e privacidade dos dados para demonstrar conformidade com normativas de referência.			
Objetivos Específicos	**Resumo das Atividades**	**Resultados Esperados**	**Técnicas e Métodos Adotados**
a) Identificar os componentes que constituirão o modelo, estabelecendo os elementos essenciais e a estrutura.	- Definir as camadas de atuação do modelo. - Determinar os requisitos de privacidade e o fluxo de atividades para a identificação dos demais requisitos e pré-requisitos que irão compor o modelo. - Definir as operações de tratamento dos dados e relacioná-las com os requisitos.	Estrutura do modelo	- Pesquisa Bibliográfica - DSR: etapa 3
b) Elaborar o modelo para gerenciar evidências de proteção e privacidade de dados e o método de aplicação, empregando os componentes e a abordagem	- Coletar informações com especialistas sobre as técnicas e ferramentas utilizadas atualmente para o gerenciamento de evidências de conformidade. - Estabelecer os métodos para identificar/coletar evidências e sua organização. - Desenvolver o modelo descrevendo cada componente	Modelo conceitual e prático Método delineado, para o gerenciamento de evidências.	- Pesquisa Bibliográfica - Pesquisa com especialistas - DSR: etapa 3

definida.	definido. - Descrever as estratégias de gerenciamento propostas para uso. - Estabelecer e descrever as orientações de implantação e a forma de aplicação do modelo. - Estabelecer o método para o gerenciamento de evidências do modelo.		
c) Aplicar o modelo identificando as melhorias a serem ajustadas.	- Aplicar o modelo em um cenário real e ajustá-lo conforme as melhorias identificadas durante a observação sistemática. - Realizar a entrevista de aplicação do modelo adequando-o para a versão preliminar.	Versão Preliminar do Modelo para a avaliação	- Pesquisa Qualitativa e Quantitativa - Pesquisa Experimental - Observação Sistemática - Instrumentos: Entrevista estruturada e formulário - DSR: etapa 4
d) Validar o modelo, submetendo à apreciação de especialistas.	- Submeter o modelo para avaliação de especialistas. - Analisar os resultados da avaliação e aplicar as melhorias identificadas. - Finalizar a versão do modelo para entrega.	Modelo finalizado para a entrega.	- Pesquisa Quantitativa - Painel com especialistas - Pesquisa com especialistas - Instrumento: Questionário - DSR: etapa 5

Fonte: Elaborado pela autora (2022).

Conforme pode ser observado na descrição das atividades, a pesquisa com especialista foi adotada em dois momentos deste estudo, para atender aos objetivos específicos “b” e “d”. A primeira pesquisa com especialistas realizada para atender o objetivo específico “b” foi aplicada a especialistas e auditores para identificar ferramentas já utilizadas para o gerenciamento de evidências no âmbito da proteção e privacidade de dados e para verificar a existência de outras abordagens e o que as empresas estavam utilizando para este fim. O resultado dessa pesquisa é apresentado no APÊNDICE E deste documento. Já a segunda pesquisa realizada com especialistas, para atender o objetivo específico “d” tem o propósito de validar o modelo apresentado neste estudo e sua contribuição na visão dos especialistas participantes e exibe seu resultado na seção 6.4 deste documento.

4.2 ETAPAS DA PESQUISA

As etapas desta pesquisa seguiram como base o *framework* metodológico de aplicação do modelo DSR sintetizado por Peffers *et al.* (2007) apresentado na Figura 13 e conforme descrito a seguir.

4.2.1 Etapa 1: Identificar o problema e motivação

Com base na literatura sobre proteção e privacidade de dados apresentada na subseção 2.1, observou-se a importância de as organizações estarem em conformidade com normativas de boas práticas, visto que, leis específicas de proteção e privacidade de dados foram sancionadas em âmbito mundial. Verificou-se também que um dos principais desafios é, além de implementar os requisitos de proteção e privacidade de dados, prover como e em quais evidências os mesmos podem ser validados.

Os modelos, *frameworks* e estruturas apresentados na literatura buscam demonstrar formas para a adequação e implementação dos requisitos. Dessa forma, conforme constatou-se na seção 3, poucos estudos se concentram na comprovação e responsabilidade com a conformidade, sendo importante salientar que além de estar em conformidade, é necessário ser capaz de comprovar que se está, fato que torna relevante a adoção de estruturas orientativas neste sentido. Com base nos problemas identificados, buscou-se sistematizar um modelo de gerenciamento de evidências de proteção e privacidade de dados que apoie na comprovação de alegações referentes a essa temática.

4.2.2 Etapa 2: Definir objetivos e a solução

Observou-se na literatura que o gerenciamento de evidências em casos de garantia é utilizado para demonstrar conformidade com padrões e normas de referência, porém em outros contextos e com mais frequência para garantir conformidade de padrões de segurança no desenvolvimento de sistemas. Diante dos problemas identificados, buscou-se apresentar um modelo e adequar as abordagens de gerenciamento de evidências em casos de garantia para que possam ser utilizadas no âmbito da proteção e privacidade dos dados e auxiliar na validação de requisitos e controles.

4.2.3 Etapa 3: Projetar e desenvolver o artefato

Para esta etapa foram realizadas as seguintes atividades:

1 – Foram definidas as camadas de atuação do modelo, cujo resultado é apresentado na subseção 5.2. A utilização de camadas tem o propósito de segmentar as atividades, para que, de forma sistematizada, seja construído um arcabouço de evidências a ser gerenciado.

2 – Foram determinados os requisitos de privacidade e o fluxo de atividades para a identificação dos demais requisitos e pré-requisitos que irão compor o modelo. Para isso, foi realizada a correlação dos princípios da normativa ISO 29100 com os princípios mandatórios da GDPR e da LGPD, a fim de avaliar a correspondência entre eles e validar a nomenclatura dos itens que irão compor os princípios do modelo[3].

A análise para identificar a correlação entre as leis e a normativa apresentou coerência entre os princípios avaliados e a proposição dos requisitos de privacidade segue a nomenclatura da ISO 29100. O resultado da atividade que determinou os requisitos de privacidade é apresentado na subseção 5.2.1.1.

3 – Foi feita a proposição do método para a identificação de requisitos e pré-requisitos provenientes de outras fontes regulatórias que devem ser atendidos em conjunto com a privacidade. Para isso, é proposta uma sequência de atividades envolvendo análises interpretativas e correlações com as operações de tratamento dos dados. O resultado desta atividade é apresentado na subseção 5.2.1.2.

4 – Foram definidas as operações de tratamento dos dados que irão compor o modelo. Esta atividade envolveu uma análise conceitual dos termos utilizados para dispor as operações de tratamento de dados, nas mesmas referências utilizadas na atividade anterior: ISO 29100, GDPR e LGPD. Esta atividade é apresentada na subseção 5.1.3. Considerando as sobreposições e semelhanças conceituais identificadas nos termos, foram propostas nove operações para tratamento dos dados. Nessa atividade também foi contemplada a proposição de um questionamento para orientar a construção da matriz que apresenta as relações existentes entre

[3] Optou-se pelo uso da ISO 29100 como referência para este trabalho por ela apresentar uma estrutura para a privacidade de dados com conceitos alinhados mundialmente, aplicados em diferentes legislações, diretivas entre outros artefatos de referência para a privacidade de dados, com características neutras quanto a soluções tecnológicas. Quanto ao uso da GDPR, optou-se pela sua utilização por ser a legislação referência e apresentar as tendências mundiais sobre o tema. Muitos países visam alcançar alinhamento com essa Lei (essa é uma das exigências da GDPR para transacionar dados com países da União Europeia) e para isso seguem os preceitos da GDPR na criação de atualização de suas leis. Já a LGPD, por ser promulgada no Brasil sendo uma versão adaptada da GPDR para tratar a privacidade dos dados em território nacional.

os requisitos (princípios) e as operações de tratamento. O resultado dessas atividades é apresentado na subseção 5.2.2.1.

5 – Foi estabelecido o método para identificar/coletar evidências e sua organização. Foi proposto um instrumento de apoio para conduzir as entrevistas para identificação das evidências e uma abordagem em perspectivas para facilitar e sistematizar essa busca. Um formulário para registrar as evidências identificadas também foi proposto para detalhar as características de cada uma delas. O resultado dessas atividades está disposto na subseção 5.2.2.1.

6 – Foram realizados estudos e análises das abordagens de gerenciamento de evidências de casos de garantia, aplicadas no âmbito de sistema e em demais contextos, com o objetivo de extrair experiências e adequações nas formas de aplicação, com o objetivo de configurá-las e ajustá-las ao contexto de proteção e privacidade de dados.

Para esta última atividade também foi realizada uma pesquisa com especialistas que consistiu na aplicação de questionários aos participantes com os seguintes perfis:

a) profissionais que atuam em organizações de diferentes segmentos (Sistemas e Serviços; Financeira; Educação/Pesquisa e Saúde) responsáveis por preparar as organizações e torná-las aderente aos requisitos de proteção e privacidade de dados[4] e;

b) profissionais responsáveis por avaliar e aferir (auditores) se um processo, produto, serviço, sistema ou ambiente estão aderentes aos requisitos de proteção e privacidade de dados[5].

O objetivo desta etapa da pesquisa foi compreender: (i) como as organizações vêm pensando e praticando o gerenciamento de evidências, as técnicas e ferramentas utilizadas no âmbito da proteção e privacidade de dados; (ii) como as evidências são avaliadas por profissionais responsáveis por aferir se um ambiente, sistema ou serviço está aderente a requisitos de proteção e privacidade de dados; e (iii) avaliar as respostas como contribuição para o modelo a ser proposto.

Esta pesquisa, foi aprovada pelo Comitê de Ética da Universidade Federal de Santa Catarina sob o processo nº 44022921.5.0000.0121, disposto no APÊNDICE A e seus resultados são apresentados na seção 5 deste trabalho.

7 – Foi estabelecido o método para o gerenciamento de evidências do modelo.

8 – Foi desenvolvido o modelo descrevendo cada componente definido.

9 – Foram descritas as estratégias de gerenciamento propostas para uso.

---

[4] Pesquisa disponível em: não consegui acessar https://docs.google.com/forms/d/e/1FAIpQLSdg3UA8l_vSfm6-iw7HtIpTNLf0P44xpwiOYjA2SOKsDVOlcg/viewform

[5] Pesquisa disponível em: https://docs.google.com/forms/d/e/1FAIpQLSdQkwA_cpv51j5-NMgWFcDUyGXNAzyaFYOe9nUSvjhEVkMvmA/viewform

10 – Foram estabelecidas e descritas as orientações de implantação e a forma de aplicação do modelo.

4.2.4 Etapa 4: Demonstrar o artefato

Esta etapa contemplou a aplicação do modelo e teve como objetivo validar as hipóteses definidas para esta tese, assim como verificar se os objetivos desta pesquisa foram atendidos.

Para comprovar a eficácia do modelo, validando o método proposto e se as contribuições que podem ser obtidas com seu uso são satisfatórias, optou-se pela aplicação do modelo em uma instituição atuante na área da saúde, considerando que dados de saúde são classificados como dados pessoais sensíveis de acordo com o LGPD, e necessitam de ações seguras e com privacidade em seu tratamento. A aplicação do modelo neste contexto oportunizou a sua avaliação em um cenário que tem a necessidade real e constante de comprovar conformidade com normativas. O modelo foi aplicado na CASACARESC[6] e detalhes sobre a instituição são apresentados na subseção 5.3 desta tese.

A aplicação do modelo foi realizada em um ciclo de validação de evidências em um processo, teve a duração de 1 mês, sem custo e com acompanhamento. Durante a aplicação, procurou-se observar e identificar possíveis desvios, dificuldades na aplicação e uso, falta de algum requisito e demais ajustes necessários para que o modelo atenda os objetivos e contribuições definidas para essa pesquisa. A aplicação foi conduzida pela pesquisadora e por uma representante da instituição responsável pela adequação aos requisitos de proteção e privacidade de dados. Durante a aplicação do modelo foram observadas e analisadas as seguintes questões: (i) pertinência dos princípios e nomenclaturas definidas para o modelo; (ii) adequação nas ações sugeridas em cada uma das camadas; (iii) pertinência da abordagem definida para gerenciar as evidências; (iv) sugestões e opiniões obtidas e/ou percebidas durante a aplicação do modelo; e (v) problemas ou dificuldades enfrentadas. As análises obtidas na aplicação do modelo foram registradas no formulário disposto no APÊNDICE B – Avaliação de Adequação do Modelo – Aplicação.

4.2.5 Etapa 5: Avaliar o artefato

Após a aplicação do modelo, a avaliação foi realizada por especialistas com a aplicação

[6] https://www.casacaresc.org.br/

do método painel de especialistas. Foram selecionados especialistas que estão atuando em projetos de adequação das empresas de diferentes segmentos, às leis ou normativas de proteção e privacidade de dados ou que estão trabalhando em pesquisas ou no desenvolvimento de produtos que abordem a temática. Os mesmos foram convidados a participar da avaliação e contatados por telefone e e-mail. O modelo foi apresentado aos especialistas em reuniões virtuais individuais. O instrumento de avaliação do modelo foi um questionário em formato digital com questões fechadas e em cada uma delas foi disponibilizada uma questão para observações e/ou sugestões.

As dimensões para a avaliação foram estruturadas contemplando: escopo, profundidade e precisão, generalidade, robustez e completeza, clareza, consistência e contribuição/recomendação, sendo as opções disponibilizadas a serem avaliadas com base em uma adaptação da escala Likert para 3 pontos, sendo estes: *1 – Discordo, 2 – Nem discordo, nem concordo e 3 – Concordo.*

Os dados resultantes da avaliação foram compilados, analisados e os ajustes das melhorias identificadas foram aplicados para a versão final do modelo para a entrega, conforme descrito na seção 6 deste trabalho.

4.2.6 Etapa 6: Comunicar os resultados

A comunicação dos resultados se dará com a publicação em documento de tese a ser disponibilizado na Biblioteca Universitária da UFSC e na publicação de artigos dos resultados parciais e final, além da apresentação em conferências e eventos em geral da área de Ciência da Informação e demais áreas que tratam os temas abordados na pesquisa.

5 COM.PRIVACY

Nesta seção é apresentado o modelo desenvolvido para o gerenciamento e evidências de proteção e privacidade de dados e as atividades estabelecidas na etapa 3 – Projetar e Desenvolver o Artefato, do método DSR adotado nesta pesquisa, quais sejam: a) definir as camadas de atuação do modelo; b) determinar os requisitos de privacidade e o fluxo de atividades para a identificação dos demais requisitos e pré-requisitos que irão compor o modelo; d) definir as operações de tratamento dos dados e relacioná-las com os requisitos; e) coletar informações com especialistas sobre as técnicas e ferramentas utilizadas atualmente para o gerenciamento de evidências de conformidade; f) estabelecer os métodos para identificar/coletar evidências e sua organização; g) desenvolver o modelo descrevendo cada componente definido; h) descrever as estratégias de gerenciamento propostas para uso; i) estabelecer e descrever as orientações de implantação e a forma de aplicação do modelo; e j) estabelecer o método para o gerenciamento de evidências do modelo.

O modelo a ser apresentado foi nomeado como COM.PRIVACY, em que COM representa as palavras no inglês "comprove" e "*compliance*", e PRIVACY de forma a representar em sua tradução para o português: "comprove, conformidade de privacidade" e o símbolo representa o "check" adotados em checklists utilizados para avaliar conformidade, de acordo com a Figura 14.

Figura 14 - Nome do modelo apresentado

Fonte: Elaborado pela autora (2022)

Conforme citado na subseção 4.2.3 deste estudo, com o intuito de verificar com os especialistas e auditores quais as práticas adotadas para o gerenciamento de evidência no âmbito da proteção e privacidade de dados, foi realizada uma pesquisa com esses profissionais. Essa pesquisa foi realizada para se obter a compreensão sobre o planejamento e as práticas adotadas pelas organizações e pelos profissionais que aferem a aderência das organizações aos requisitos de proteção e privacidade de dados, e os resultados obtidos embasaram a construção do modelo COM.PRIVACY. A estrutura dos questionários utilizados na pesquisa é apresentada nos APÊNDICE C e D e os resultados são apresentados APÊNDICE E.

Nesta seção, são apresentadas as três bases estruturantes adotadas na concepção do modelo, são elas: *Privacy by Design*, a normativa de referência ISO 29100 e as nove operações de tratamento dos dados. Além disso, são apresentadas as camadas definidas na estruturação do COM.PRIVACY, as quais contemplam: uma primeira camada destinada à identificação dos requisitos e pré-requisitos oriundos da normativa de proteção e privacidade e de fontes regulatórias adjacentes; uma camada intermediária destinada à identificação e coleta das evidências e uma terceira camada destinada à gestão das evidências coletadas.

Por fim, são apresentadas as etapas de aplicação do modelo em um cenário real e as considerações finais da seção.

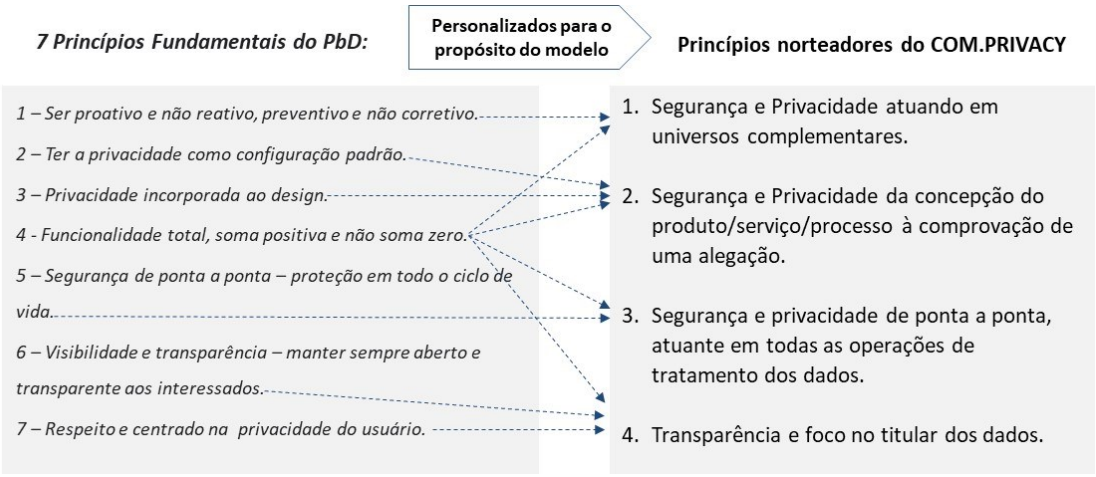
5.1 BASES ESTRUTURANTES

Nesta subseção, são apresentadas as três bases estruturantes adotadas na concepção do modelo COM.PRIVACY: *Privacy by Design*, a normativa de referência ISO 29100 e as operações de tratamento dos dados.

5.1.1 *Privacy by Design*

O conceito de PbD é utilizado como uma das bases estruturantes do COM.PRIVACY. Seu objetivo é tornar a proteção e a privacidade dos dados parte integrante de sistemas, produtos e processos desde a concepção dos mesmos, estando assim alinhado ao propósito do modelo proposto. Além disso, normativas de boas práticas recomendam sua adoção, assim como citado em algumas legislações de proteção e privacidade de dados. Portanto, optou-se pela sua adoção e, para sua utilização, os sete princípios definidos pela autora Ann Cavoukian foram personalizados para gerar os princípios norteadores do COM.PRIVACY. Para essa personalização, os sete princípios do PbD foram consolidados em quatro princípios norteadores do modelo, conforme apresentado na Figura 15.

Figura 15 - Personalização dos princípios do PbD



Fonte: elaborado pela autora (2022).

Os princípios norteadores para o modelo são:

1. **Segurança e Privacidade atuando em universos complementares**: os requisitos de privacidade irão complementar os requisitos de segurança e vice-versa. Ambos atuarão de forma preventiva, complementar, estruturando uma solução completa e necessária;
2. **Segurança e privacidade de ponta a ponta, atuante em todas as operações de tratamento dos dados**: implementar requisitos de proteção e privacidade dos dados desde antes da coleta dos mesmos até seu descarte, atuando em cada operação de tratamento dos dados;
3. **Segurança e Privacidade da concepção do produto/serviço/processo à comprovação de uma alegação**: demonstrar a preocupação e o comprometimento com a proteção e privacidade dos dados desde a fase de projeto, além de comprovar as implementações realizadas e suas alegações;
4. **Transparência e foco no titular dos dados**: o modelo tem a intenção de tornar o processo de tratamento de dados mais transparente para favorecer seu titular, permitindo a ele visualizar as comprovações de atendimento aos requisitos de proteção e privacidade de dados implementados em seus dados.

5.1.2 ISO 29100

Optou-se pelo uso da ISO 29100 como referência para este trabalho por ela apresentar uma estrutura para a privacidade de dados com conceitos alinhados mundialmente, aplicados

em diferentes legislações, diretivas entre outros artefatos de referência para a privacidade de dados, com características neutras quanto a soluções tecnológicas.

Para a comprovação dessa afirmação, foi realizada uma análise de compatibilidade entre as temáticas contidas nos três artefatos: normativa ISO 29100 e Leis GDPR e LGPD. Esta subseção apresenta o resultado desta análise e o conjunto de requisitos resultantes que foram utilizados na aplicação do modelo. A análise utilizou como referência a ISO 29100, visto que a intenção é utilizar a nomenclatura e o conjunto de princípios definidos por ela, porém foi necessário analisar e comprovar a coerência destes princípios com os temas apresentados nas Leis GDPR e LGPD.

Optou-se por utilizar a GDPR para a análise por esta ser a Lei de referência utilizada pelos demais países na adequação de suas legislações, assim como o Brasil ao institucionalizar a LGPD. Com a obrigatoriedade do cumprimento das legislações, torna-se importante considerá-las na apuração dos requisitos a serem adotados no modelo. Já a escolha pelo uso dos princípios preconizados pela norma ISO 29100 se deu em decorrência do modelo buscar independência em relação à fonte regulatória de referência, cujo propósito é ser aplicável em contextos de gerenciamento de evidências de proteção e privacidade de dados e conformidade com diferentes normativas de referência.

Sendo assim, foi realizada uma análise conceitual dos princípios apresentados na ISO 29100 e os preconizados pelas legislações (GDPR e LGPD). O Quadro 18, apresenta as relações existentes e os itens correspondentes em cada documento.

Quadro 18 - Relações entre os princípios da ISO 29100, GDPR e LGPD

GDPR	**ISO 29100**	**LGPD**
Considerações iniciais – item 32 CAPÍTULO II Artigo 7º - Condições aplicáveis ao consentimento	1. Consentimento e escolha	CAPÍTULO II - Do tratamento de dados pessoais Seção I - Dos Requisitos para o Tratamento de Dados Pessoais Art. 8º Art. 8º § 5º
CAPÍTULO II Artigo 5º a) Licitude, lealdade e transparência	2. Legitimidade e especificação do objetivo	CAPÍTULO I - Disposições preliminares Art. 6º - I: Finalidade
CAPÍTULO II Artigo 5º c) Minimização	3. Limitação de coleta	CAPÍTULO I - Disposições Preliminares Art. 6º - III: Necessidade
CAPÍTULO II Artigo 5º c) Minimização	4. Minimização de dados	CAPÍTULO I - Disposições preliminares Art. 6º - III: Necessidade

CAPÍTULO II Artigo 5º: b) Limitação das Finalidades e) Limitação da Conservação	5. Limitação de uso, retenção e divulgação	CAPÍTULO I - Disposições Preliminares Art. 6º - II: Adequação
CAPÍTULO II Artigo 5º d) Exatidão	6. Precisão e qualidade	CAPÍTULO I - Disposições Preliminares Art. 6º - V: Qualidade dos dados
CAPÍTULO II Artigo 5º a) Licitude, lealdade e transparência	7. Abertura, transparência e notificação	CAPÍTULO I - Disposições Preliminares Art. 6º - IV: Livre acesso Art. 6º - VI: Transparência
CAPÍTULO II Artigo 5º d) Exatidão	8. Acesso e participação individual	CAPÍTULO I - Disposições Preliminares Art. 6º - IV: Livre acesso
CAPÍTULO II Artigo 5º g) Responsabilidade	9. Responsabilização	CAPÍTULO I - Disposições Preliminares Art. 6º - X: Responsabilização e prestação de contas
CAPÍTULO II Artigo 5º f) Integridade de Confidencialidade	10. Segurança da Informação	CAPÍTULO I - Disposições Preliminares Art. 6º - VII - Segurança
CAPÍTULO II - Princípios Item 2 - Responsabilidade *CAPÍTULO IV* *Seção 1 – Obrigações gerais* *Artigo 24º* *Responsabilidade do responsável pelo tratamento*	11. *Compliance* com a privacidade	CAPÍTULO I - Disposições Preliminares Art. 6º - X - Responsabilização e prestação de contas

Fonte: Elaborado pela autora (2021).

O eixo central da análise são os princípios da ISO 29100 e as temáticas de correspondência nas Leis GDPR (à esquerda do Quadro 18) e a LGPD (à direita do Quadro 18). Após a identificação da correspondência entre os temas, buscou-se comprovar essas relações apresentando as descrições de cada um deles, conforme apresentado nos Quadro 19 a 29.

Quadro 19 - Relações entre o princípio consentimento e escolha e a GDPR e LGPD – detalhamento

CONSENTIMENTO E ESCOLHA **ISO 29100** O objetivo desse princípio é possibilitar ao titular do DP o fornecimento e a retirada do consentimento de forma facilitada e sem ônus além da escolha de como os seus DP serão tratados.	
GDPR	**LGPD**

Considerações iniciais - item 32: O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrônico, ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um sítio *web* na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins. Se o consentimento tiver de ser dado no seguimento de um pedido apresentado por via eletrônica, esse pedido tem de ser claro e conciso e não pode perturbar desnecessariamente a utilização do serviço para o qual é fornecido. ***Artigo 7º - Condições aplicáveis ao consentimento:*** este item apresenta instruções quanto ao consentimento ser apresentado de forma clara e desvinculada de outros assuntos, o direito de revogação do consentimento e a capacidade de comprovar o consentimento fornecido.	***CAPÍTULO II - DO TRATAMENTO DE DADOS PESSOAIS*** ***Seção I - Dos Requisitos para o Tratamento de Dados Pessoais*** ***Art. 8º*** O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. ***Art. 8º § 5º*** O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei. *Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:* *I - mediante o fornecimento de consentimento pelo titular*

Fonte: Elaborado pela autora (2021).

Quadro 20 - Relações entre o princípio legitimidade e especificação de objeto e a GDPR e LGPD – detalhamento

LEGITIMIDADE E ESPECIFICAÇÃO DE OBJETIVO **ISO 29100**
Este princípio tem o propósito de assegurar que os objetivos os quais o DP foi coletado está respaldados por uma base legal permissível e a comunicação dos objetivos da coleta ao titular, antes que ela aconteça com o uso de linguagem clara e explicação suficiente sobre o tratamento dos dados.

GDPR	LGPD
CAPÍTULO II - Princípios ***Artigo 5º a) Licitude, lealdade e transparência*** DP devem ser objeto de tratamento lícito, leal e transparente em relação ao titular dos dados.	***CAPÍTULO I - Disposições Preliminares*** ***Art. 6º - I*** ***Finalidade:*** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Fonte: Elaborado pela autora (2021).

Quadro 21 - Relações entre o Princípio Limitação de Escolha e a GDPR e LGPD – detalhamento

LIMITAÇÃO DE COLETA **ISO 29100** A limitação da coleta está relacionada com o propósito de uso, ou seja, a norma recomenda que sejam coletados somente os DP necessários para cumprir o(s) objetivo(s) especificado(s) pelo controlador e que seja documentado o tipo de DP coletado e a justificativa da coleta nas políticas e práticas de manuseio de informações.	
GDPR	**LGPD**
CAPÍTULO II - Princípios ***Artigo 5º a) Minimização dos dados*** Os DP devem ser adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados.	***CAPÍTULO I - Disposições Preliminares*** ***Art. 6º - III*** ***Necessidade:*** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Fonte: Elaborado pela autora (2021).

Quadro 22 - Relações entre o Princípio Minimização dos Dados e a GDPR e LGPD – detalhamento

MINIMIZAÇÃO DOS DADOS **ISO 29100** Este princípio está diretamente relacionado com o princípio da limitação da coleta. Se por um lado a limitação da coleta refere-se à obtenção de dados restritos à finalidade especificada, a minimização dos dados refere-se ao tratamento do DP estritamente necessário.	
GDPR	**LGPD**
CAPÍTULO II - Princípios ***Artigo 5º a) Minimização dos dados*** Os DP devem ser adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados.	***CAPÍTULO I - Disposições Preliminares*** ***Art. 6º - III*** ***Necessidade:*** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Fonte: Elaborado pela autora (2021).

Quadro 23 - Relações entre o Princípio Limitação de Uso, Retenção e Divulgação e a GDPR e LGPD – detalhamento

LIMITAÇÃO DE USO, RETENÇÃO E DIVULGAÇÃO **ISO 29100** Esse princípio possui caráter complementar aos princípios (Limitação da Coleta e Minimização dos Dados). Especifica que os acessos aos dados coletados devem ser limitados, assim como o compartilhamento e transferência dos dados, e que o tempo de retenção dos dados seja controlado de forma que o descarte seja realizado de forma segura, logo que os objetivos sejam cumpridos e/ou as finalidades estabelecidas forem expiradas ou alteradas.	
GDPR	**LGPD**
CAPÍTULO II - Princípios ***Artigo 5º b) Limitação das finalidades*** ***Artigo 5º b) Limitação da conservação*** ***b) Limitação das finalidades*** - Os DP devem ser coletados para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89, n. 1. ***e)Limitação da conservação –*** Os DP devem ser ***c***onservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.o, n. 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados. *Artigo 89.o n. 1 - 1. O tratamento para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, está sujeito a garantias adequadas, nos termos do presente regulamento, para os direitos e liberdades do titular dos dados. Essas garantias asseguram*	***CAPÍTULO I - Disposições Preliminares*** ***Art. 6º - II*** ***Adequação:*** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

a adoção de medidas técnicas e organizativas a fim de assegurar, nomeadamente, o respeito do princípio da minimização dos dados. Essas medidas podem incluir a pseudoanonimização, desde que os fins visados possam ser atingidos desse modo. Sempre que esses fins possam ser atingidos por novos tratamentos que não permitam, ou já não permitam, a identificação dos titulares dos dados, os referidos fins são atingidos desse modo.	

Fonte: Elaborado pela autora (2021).

Quadro 24 - Relações entre o princípio precisão e qualidade e a GDPR e LGPD – detalhamento

PRECISÃO E QUALIDADE **ISO 29100** Este princípio refere-se à confiabilidade dos dados, ou seja, a extração de fonte confiável, a precisão, a completeza, a atualização e a adequação dos dados ao seu objetivo de uso.	
GDPR	**LGPD**
CAPÍTULO II - Princípios ***Artigo 5º d) Exatidão*** Os DP devem ser exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora.	***CAPÍTULO I - Disposições Preliminares*** ***Art. 6º - V*** ***Qualidade dos dados***: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

Fonte: Elaborado pela autora (2021).

Quadro 25 - Relações entre o Princípio Abertura, Transparência e Notificação e a GDPR e LGPD – detalhamento

ABERTURA, TRANSPARÊNCIA E NOTIFICAÇÃO **ISO 29100** O princípio da abertura, transparência e notificação está relacionado com a disponibilização de informações completas e claras ao titular do DP sobre o tratamento de seu dado e os meios oferecidos a ele para acesso, correção e remoção de seus dados.	
GDPR	**LGPD**
CAPÍTULO II - Princípios ***Artigo 5º a) Licitude, lealdade e transparência*** DP devem ser objeto de tratamento lícito, leal e transparente em relação ao titular dos dados.	***CAPÍTULO I - Disposições Preliminares*** ***Art. 6º - IV*** ***Livre acesso:*** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais. ***Art. 6º - VI*** ***Transparência:*** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento,

	observados os segredos comercial e industrial.

Fonte: Elaborado pela autora (2021).

Quadro 26 - Relações entre o Princípio Acesso e Participação Individual e a GDPR e LGPD – detalhamento

ACESSO E PARTICIPAÇÃO INDIVIDUAL **ISO 29100** Este princípio trata sobre o direito ao titular do DP de acesso, análise, edição e exclusão de seus dados de forma rápida, eficiente, simplificada e sem custos garantindo que o acesso se dará apenas aos dados que lhes pertence.	
GDPR	**LGPD**
CAPÍTULO II - Princípios ***Artigo 5º d) Exatidão*** Os DP devem ser exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora.	***CAPÍTULO I - Disposições Preliminares*** ***Art. 6º - IV*** ***Livre acesso***: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

Fonte: Elaborado pela autora (2021).

Quadro 27 - Relações entre o Princípio Responsabilização e a GDPR e LGPD – detalhamento

RESPONSABILIZAÇÃO **ISO 29100** O princípio da responsabilização implica no dever de zelar e adotar medidas concretas e práticas para a proteção em toda a cadeia (controlador, operador e terceiros) envolvida no tratamento dos DP. Além de estabelecer procedimento para comunicações e tratamentos em caso de violação de privacidade.	
GDPR	**LGPD**
CAPÍTULO II - Princípios ***Item 2 - Responsabilidade*** O responsável pelo tratamento é responsável pelo cumprimento dos requisitos de proteção e privacidade de dados dispostos na legislação e ser capaz de comprová-lo.	***CAPÍTULO I - Disposições Preliminares*** ***Art. 6º - X*** **Responsabilização e prestação de contas:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Fonte: Elaborado pela autora (2021).

Quadro 28 - Relações entre o Princípio Responsabilização e a GDPR e LGPD – detalhamento

SEGURANÇA DA INFORMAÇÃO **ISO 29100** O princípio da segurança da informação refere-se à adoção de medidas de segurança pertinentes e satisfatórias de proteção no tratamento dos DP, contemplando controles apropriados nos níveis operacional, funcional e estratégico para assegurar a confidencialidade, integridade e disponibilidade da informação.	
GDPR	**LGPD**

CAPÍTULO II - Princípios ***Artigo 5º f) Integridade de Confidencialidade*** Os DP devem ser tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizacionais adequadas.	***CAPÍTULO I - Disposições Preliminares*** ***Art. 6º - VII*** ***Segurança:*** utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Fonte: Elaborado pela autora (2021).

Quadro 29 - Relações entre o Princípio *Compliance* com a Privacidade e a GDPR e LGPD – detalhamento

***COMPLIANCE* COM A PRIVACIDADE** **ISO 29100** O princípio de *Compliance* com a privacidade refere-se a ter, manter e demonstrar que os requisitos de proteção dos dados e a garantia da privacidade estão garantidos e quando aplicável, cooperar com a(s) autoridades(s) supervisora(s) no monitoramento das leis de proteção de dados.	
GDPR	**LGPD**
CAPÍTULO II - Princípios ***Item 2 - Responsabilidade*** O responsável pelo tratamento é responsável pelo cumprimento dos requisitos de proteção e privacidade de dados dispostos na legislação e ser capaz de comprová-lo. ***CAPÍTULO IV*** ***Seção 1 – Obrigações gerais*** ***Artigo 24º Responsabilidade do responsável pelo tratamento*** 1. Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante às necessidades.	***CAPÍTULO I - Disposições Preliminares*** ***Art. 6º - X*** **Responsabilização e prestação de contas:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Fonte: Dados da pesquisa (2021).

Conforme apresentado, é possível observar a correlação conceitual das temáticas contidas nos princípios da Normativa ISO 29100 utilizada como referência para esta pesquisa e as leis selecionadas, com o objetivo de justificar a escolha por essa normativa. Vale ressaltar

que o objetivo dessa análise foi verificar se os temas abordados na ISO 29100 são abordados nas Leis em questão, não estando no escopo da mesma realizar uma análise jurisprudencial.

5.1.3 Operações de Tratamento de Dados

As operações de tratamento dos dados referem-se às ações realizadas com os dados e sendo assim, entende-se que elas nortearão as atividades a serem adotadas no modelo. Para a definição das operações de tratamento dos dados a serem adotadas, foram analisadas as operações de tratamento indicadas nos mesmos artefatos adotados para o levantamento dos requisitos: ISO 29100, GDPR e LGPD.

A ISO 29100 apresenta em seu item 2.21 a seguinte definição para tratamento de dados pessoais: "operação ou conjunto de operações realizadas sobre dados pessoais (DP)". Em nota apresenta exemplos de operações de tratamento de DP sendo elas, mas não estando limitados à: coleta, armazenamento, alteração, recuperação, consulta, divulgação, anonimização, pseudoanonimização, disseminação ou disponibilização, exclusão ou destruição de dados pessoais.

O artigo 5º da LGPD traz no item X que tratamento de dados pessoais é:

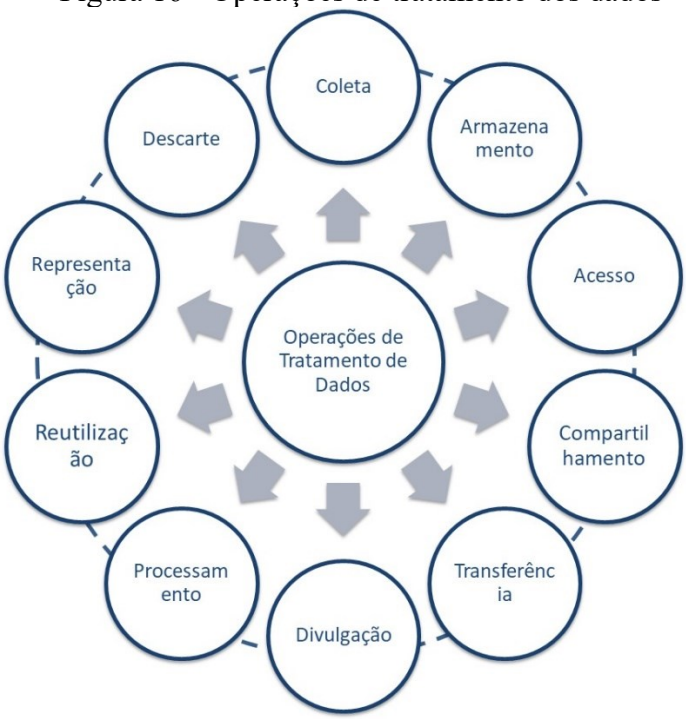
> Toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Por sua vez, a GDPR em seu art. 4º, item 2, apresenta a seguinte definição sobre tratamento de dados:

> Uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a coleta, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

Observa-se que não há um consenso entre as operações no que se refere às nomenclaturas. Como proposição a ser adotada para a aplicação do modelo, a partir da análise realizada nas definições dos três artefatos, foram definidas dez operações de tratamento dos dados, conforme demonstradas na Figura 16.

Figura 16 - Operações de tratamento dos dados



Fonte: Elaborada pela autora (2021).

Na forma apresentada, as operações de tratamento de dados contidas nos três artefatos analisados foram contempladas nesta tese, sendo que algumas foram absorvidas e tratadas em termos similares, conforme descrito a seguir:

a) Coleta: ato de obter/receber os dados;
b) Armazenamento: ato de arquivar/guardar/registrar/manter os dados;
c) Acesso: ato de chegar até os dados para uso;
d) Compartilhamento: ato de disponibilizar os dados (permitir o uso do dado a outras entidades);
e) Transferência: ato de transferir/entregar os dados (ficando uma cópia ou não);
f) Divulgação: ato de disponibilizar os dados (com o objetivo de disseminar/comunicar os dados);
g) Processamento: ato de organizar/manipular/modificar os dados seja com a classificação, alteração, ocultação (anonimização, pseudoanonimização, criptografia);
h) Reutilização: ato do reuso ou sejam reutilizar os dados para outros fins os quais foram coletados;
i) Representação: ato de descrever os dados com metadados.
j) Descarte: ato de eliminar/excluir/destruir os dados.

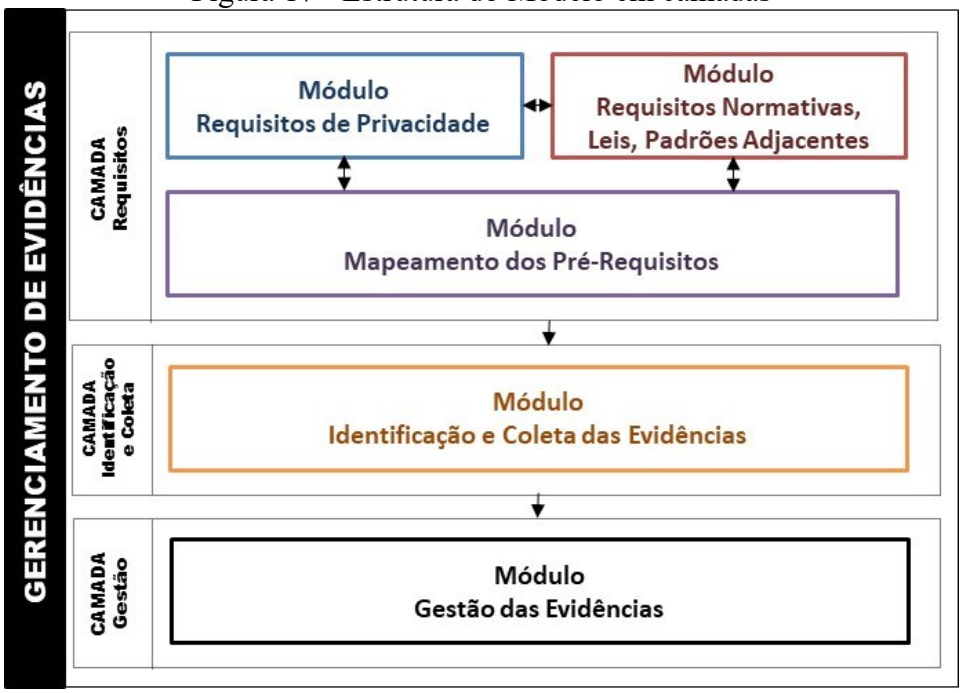
Importante salientar que para a utilização do modelo é necessário adotar um conjunto de operações de tratamento do dado que contemple desde a coleta até o seu descarte. As

operações de tratamento apresentadas acima se referem a uma proposição criada a partir das definições da normativa utilizada como referência para esta pesquisa, porém outros grupos de operações podem ser definidos e adotados desde que contemplem as contidas nas normativas de referência que se pretende adotar.

5.2 CAMADAS DO COM.PRIVACY

Com o objetivo de segmentar as etapas e atividades, o modelo foi estruturado em três camadas, sendo elas: uma para atividades relacionadas aos requisitos a serem atendidos, outra referente à identificação e coleta de evidências e a outra destinada à gestão das evidências. Esta subseção apresenta a estruturação do modelo e suas especificações e a Figura 17 ilustra a estrutura do modelo em camadas.

Figura 17 - Estrutura do Modelo em camadas



Fonte: Elaborada pela autora (2022).

Conforme a estrutura apresentada, com base em requisitos e pré-requisitos oriundos de normativas de referência e fontes regulatórias adjacentes (primeira camada), se faz necessário identificá-las (camada intermediária) para ser possível gerenciar as evidências (última camada do modelo). Além disso, no âmbito da proteção e privacidade de dados esses requisitos devem ser atendidos e praticados em todas as operações de tratamento dos dados, de forma a representarem variáveis importantes a serem consideradas em apoio à identificação de coleta de evidências.

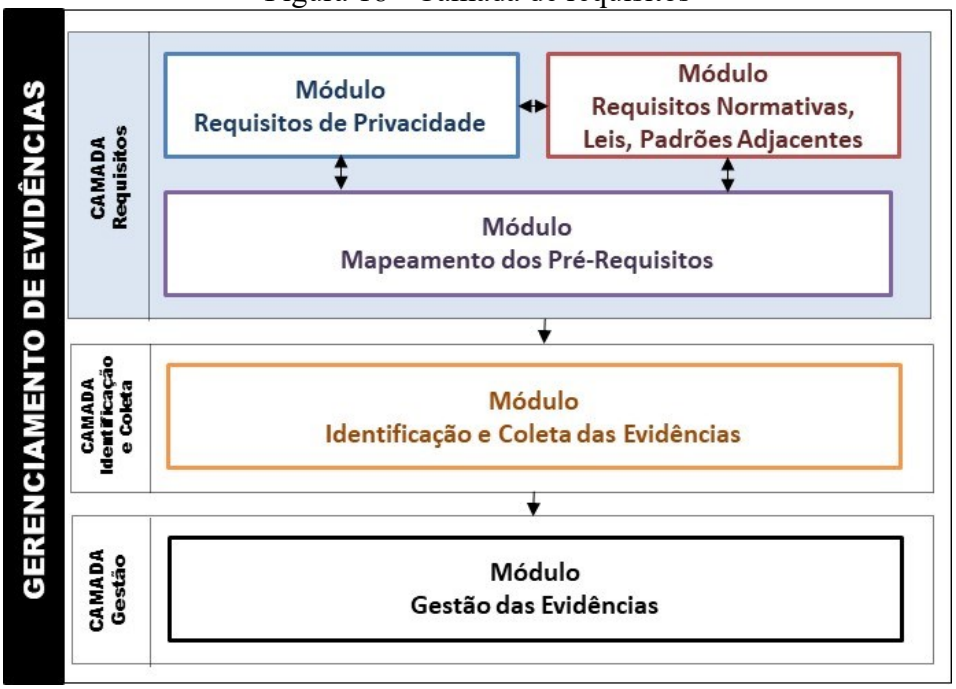
Devido à estrutura de dependência entre esses quesitos, optou-se por abordar essas atividades no modelo segmentando-as em camadas e módulos com o intuito de propor uma solução completa para o gerenciamento de evidências de proteção e privacidade de dados.

A seguir são apresentadas as especificações das camadas seguindo o fluxo em *top-down*.

5.2.1 Camada de Requisitos

Nesta camada são tratados os requisitos de conformidade com a proteção e privacidade de dados e demais fontes relacionadas que apresentam interferência sobre eles e que se pretende atender. Nesse contexto, requisitos são todas as condições necessárias para satisfazer ao objetivo de proteger e garantir a privacidade de dados considerando as normativas de referência.

Figura 18 - Camada de requisitos



Fonte: Elaborada pela autora (2022).

Entende-se que uma vez identificados, os requisitos de proteção e privacidade de dados devem ser observados e atendidos desde a concepção de novos serviços, produtos e processos e, também, durante as atualizações/manutenções nos mesmos aplicando o conceito de *Privacy by Design* — privacidade desde a geração. Com base nessa visão, Sadiq e Governatori (2015) reforçam que uma característica fundamental da abordagem de conformidade por *design* é a capacidade de capturar requisitos de conformidade por meio de uma estrutura de modelagem de requisitos genérica e propagá-los aplicando em modelos de processos de negócios e

aplicativos corporativos.

Com o intuito de segmentar e facilitar a identificação dos requisitos, esta camada foi dividida em três módulos, sendo eles:

a) um módulo que trata dos requisitos de proteção e privacidade de dados — denominados aqui como requisitos primários;

b) um módulo para a identificação de requisitos relacionados à temática em fontes regulatórias adjacentes a serem adotados em conjunto com os requisitos de privacidade — também denominados como requisitos primários; e

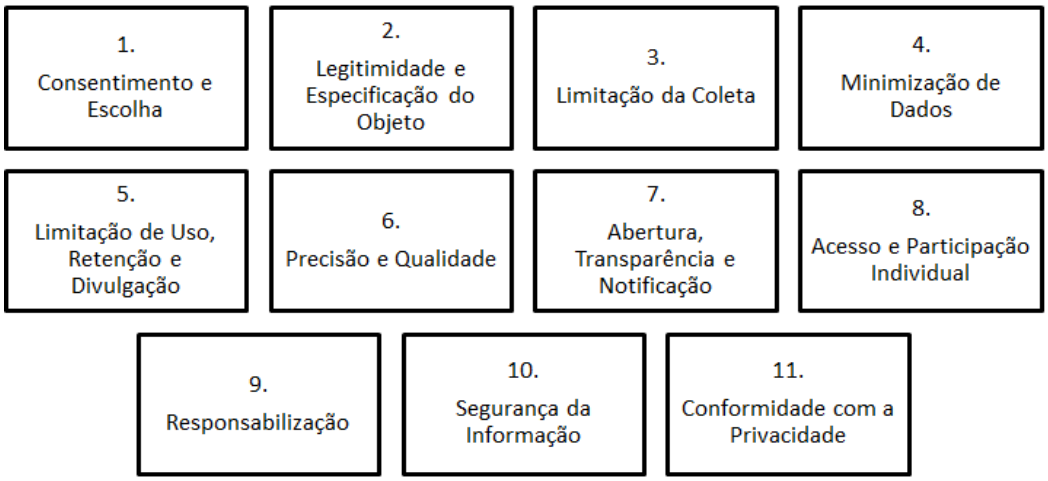
c) um módulo para mapear os pré-requisitos necessários para atender os requisitos primários.

Para o módulo de requisitos de proteção e privacidade de dados, o modelo propõe o uso de um conjunto de requisitos oriundo da normativa ISO 29100, podendo estes serem extraídos de qualquer outra fonte desejável. Já para os módulos requisitos de fontes regulatórias adjacentes e mapeamento dos pré-requisitos, o modelo apresenta os métodos que podem ser utilizados para a extração desses requisitos, assim como para o mapeamento dos pré-requisitos.

5.2.1.1 Módulo Requisitos de Privacidade

Conforme apresentado na subseção 5.1.2, a ISO 29100 — dentro do escopo desta pesquisa — trata de uma normativa de base que possui compatibilidade de conceitos com as principais leis no âmbito da proteção e privacidade de dados. Com essa comprovação, optou-se por adotar como requisitos primários de proteção e privacidade de dados para este modelo, os 11 princípios apresentados pela ISO 29100 dispostos na Figura 19. Ressalta-se que o termo requisito primário foi adotado para indicar o nível mais alto dos requisitos e para diferenciá-los do termo pré-requisitos que serão tratados na subseção 5.2.1.3.

Figura 19 - Nomenclatura dos 11 princípios



Fonte: Elaborado pela autora (2021).

A descrição de cada um dos princípios é apresentada a seguir de acordo com as definições descritas na ISO 29100.

1. Consentimento e Escolha: possibilita ao titular do DP o fornecimento e a retirada do consentimento de forma facilitada e sem ônus, além da escolha de como os seus DP serão tratados.

2. Legitimidade e Especificação do Objeto: o objetivo desse princípio é assegurar que os objetivos os quais o DP foi coletado estejam respaldados por uma base legal permissível e a comunicação dos objetivos da coleta ao titular, e que ela aconteça com o uso de linguagem clara e explicação suficiente sobre o tratamento dos dados.

3. Limitação da Coleta: a limitação da coleta está relacionada com o propósito de uso, ou seja, a norma recomenda que sejam coletados somente os DP necessários para cumprir o(s) objetivo(s) especificado(s) pelo controlador e que seja documentado o tipo de DP coletado e a justificativa da coleta nas políticas e práticas de manuseio de informações.

4. Minimização de Dados: este princípio está diretamente relacionado com o princípio da limitação da coleta. Se por um lado a limitação da coleta refere-se à obtenção de dados restritos à finalidade especificada, a minimização dos dados refere-se ao tratamento do DP estritamente necessário.

5. Limitação de Uso, Retenção e Divulgação: este princípio possui caráter complementar aos princípios 3 e 4. Especifica que os acessos aos dados coletados devem ser limitados, assim como o compartilhamento e transferência dos dados, e que o tempo de retenção dos dados seja controlado de maneira que o descarte seja realizado de forma segura, logo que os objetivos sejam cumpridos e/ou as finalidades estabelecidas forem expiradas ou alteradas.

6. Precisão e Qualidade: este princípio refere-se à confiabilidade dos dados, ou seja, à extração de fonte confiável, à precisão, à completeza, à atualização e à adequação dos dados ao seu objetivo de uso.

7. Abertura, Transparência e Notificação: o princípio da abertura, transparência e notificação está relacionado à disponibilização de informações completas e claras ao titular do DP sobre o tratamento de seu dado e os meios oferecidos a ele para acesso, correção e remoção de seus dados.

8. Acesso e Participação Individual: este princípio trata sobre o direito ao titular do DP de acesso, análise, edição e exclusão de seus dados de forma rápida, eficiente, simplificada e sem custos, garantindo que o acesso se dará apenas aos dados que lhes pertence.

9. Responsabilização: o princípio da responsabilização implica no dever de zelar e adotar medidas concretas e práticas para a proteção em toda a cadeia (controlador, operador e terceiros) envolvida no tratamento dos DP. Além de estabelecer procedimentos para comunicações e tratamentos em caso de violação de privacidade.

10. Segurança da Informação: o princípio da segurança da informação refere-se à adoção de medidas de segurança pertinentes e satisfatórias de proteção no tratamento dos DP, contemplando controles apropriados nos níveis operacional, funcional e estratégico para assegurar a confidencialidade, integridade e disponibilidade da informação.

11. Conformidade com a Privacidade: o princípio de *Compliance* com a privacidade refere-se a ter, manter e demonstrar que os requisitos de proteção dos dados e a garantia da privacidade estão garantidos e, quando aplicável, cooperar com a(s) autoridade(s) supervisora(s) no monitoramento das leis de proteção de dados.

Os estudos de correlação de temas realizados para a proposição dos requisitos primários de proteção e privacidade apresentados neste trabalho foram necessários para clarificar a aderência destes às Leis (GDPR e LGPD) utilizadas para esta pesquisa, sendo apresentados como forma de contribuição para o uso do modelo. Caso o cenário de aplicação utilize leis de países, as quais adotam outras nomenclaturas ou divisões conceituais que requeiram alterações na forma apresentada dos requisitos, os mesmos podem ser reestabelecidos de acordo com o que for mais adequado ao cenário de aplicação, da mesma forma que um estudo de correlação dos temas da ISO 29100 com outras leis podem ser utilizado para avaliação.

5.2.1.2 Módulo Requisitos de Fontes Regulatórias Adjacentes

Este módulo destina-se a identificar, de acordo com o escopo de aplicação do modelo,

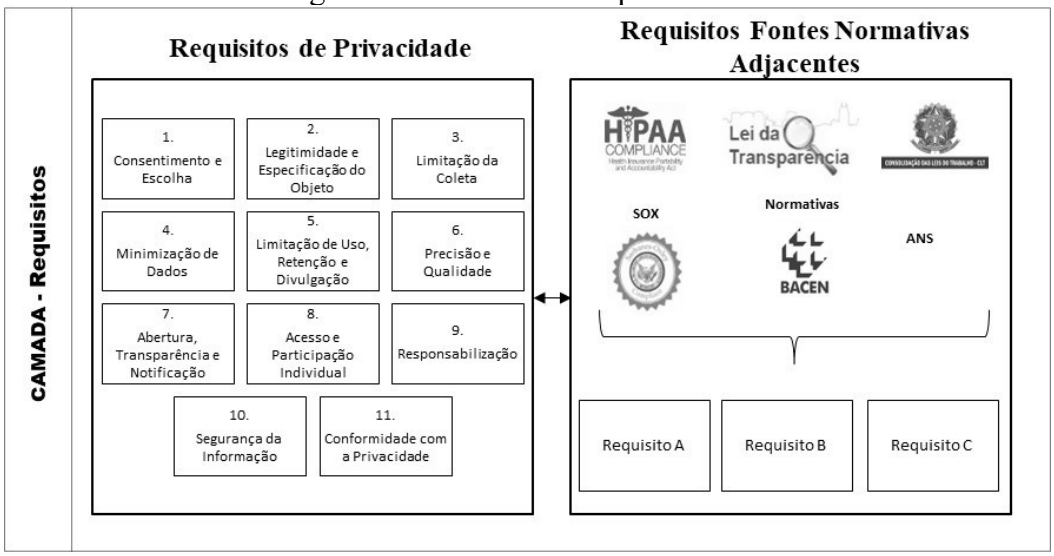
demais fontes regulatórias de cunho obrigatório ao contexto, as quais mesmo não tendo como foco principal o tratamento de dados, traz em seu conteúdo exigências relacionadas a alguma das operações de tratamento dos dados: Coleta, Armazenamento; Acesso; Compartilhamento; Transferência; Divulgação; Processamento; Reutilização e Descarte, abordado na subseção 5.1.3.

Vale ressaltar que devem ser consideradas somente as fontes regulatórias "obrigatórias" para o contexto de aplicação do modelo. Aquelas fontes que são apenas boas práticas, não devem ser consideradas neste levantamento. Para essa identificação no início dos trabalhos, o entrevistado deve ser consultado, além do departamento jurídico, demais departamentos internos e as entidades de classe aplicáveis ao cenário. Importante que todas as fontes regulatórias adjacentes, que de alguma forma abordem o tratamento de dados, sejam identificadas neste módulo.

Identificadas as fontes regulatórias adjacentes aplicáveis ao contexto, uma avaliação textual através de leitura deve ser realizada em busca de requisitos que remetem às operações de tratamento dos dados e que precisam ser atendidos. Os mesmos devem ser listados para serem aplicados na matriz apresentada no Quadro 33 da subseção 5.2.2.1.

Com o intuito de exemplificar a camada de fontes regulatórias adjacentes, a Figura 20 ilustra a camada de requisitos e os dois módulos apresentados.

Figura 20 - Camada de requisitos



Fonte: Elaborada pela autora (2022).

Conforme pode ser observado, na parte esquerda da Figura 21 constam os 11 requisitos de privacidade descritos na subseção 5.1.2 e à direita são representadas algumas fontes

regulatórias aplicáveis a diferentes áreas, tais como: *Health Insurance Portability and Accountability Act* (HIIPA)[7], aplicável a organizações de saúde norte-americanas; Lei de Acesso às Informações[8], aplicável a empresas públicas brasileiras, a qual obriga a divulgação de gastos, incluindo salários de funcionários; Consolidação das Lei do Trabalho (CLT)[9]: aplicável a empregados de organizações brasileiras contratados com essa legislação; SOX (Sarbanes Oxley)[10], legislação americana na área contábil para combate a fraudes financeiras, aplicável a empresas americanas com capital aberto e seus fornecedores; Normativas do Banco Central do Brasil (BACEN)[11] aplicáveis a órgãos e entidades da administração pública federal e seus fornecedores e Agência Nacional de Saúde (ANS)[12] aplicável às instituições que regulam o mercado de planos de saúde privados.

Para a realização das buscas de requisitos nos artefatos adjacentes, os termos relacionados aos requisitos da ISO 29100 e as operações de tratamento dos dados apresentados na subseção 5.1.3 devem ser utilizados como referência. Vale ressaltar que diferentes fontes regulatórias adjacentes podem apresentar diferentes termos de referência em relação aos apresentados aqui, os quais podem possuir o mesmo significado. Para essa atividade recomenda-se que os glossários dos documentos sejam consultados e compreendidos antes de iniciar as buscas.

Observa-se que os requisitos oriundos dessa análise podem ser complementares aos requisitos de privacidade, devendo estes serem atendidos juntamente aos requisitos de proteção e privacidade, ou apresentarem definições divergentes às estabelecidas nos requisitos e pré-requisitos. Para a situação em que os requisitos são complementares, ambos devem ser utilizados dando sequência na aplicação do modelo, já para os casos de requisitos divergentes dos obtidos de leis de privacidade, a prioridade de atendimento está condicionada à predominância da lei de origem. Sendo assim, a identificação da predominância das leis deve ser realizada nesta camada e ser sinalizada na cor vermelha ao incluí-las na matriz apresentada no Quadro 34 da subseção 5.2.2.1. Para a identificação da predominância das leis, recomenda-

[7] Mais informações sobre a HIIPA podem ser obtidas em https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996
[8] Mais informações sobre a Lei de Acesso às Informações podem ser obtidas em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm
[9] Mais informações dobre a CLT podem ser obtidas em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm
[10] Mais informações sobre a SOX podem ser obtidas em: https://www.govinfo.gov/content/pkg/COMPS-1883/pdf/COMPS-1883.pdf
[11] Mais informações sobre as normativas do BACEN podem ser obtidas em: https://www.bcb.gov.br/estabilidadefinanceira/buscanormas
[12] Mais informações sobre as normativas da ANS podem ser obtidas em: http://www.ans.gov.br/perfil-do-setor/normas-mais-acessadas

se consultar o departamento jurídico.

5.2.1.3 Módulo Mapeamento dos Pré-Requisitos

Os requisitos primários abordados na subseção anterior retratam as condições determinantes para a conformidade que se busca alcançar, porém para que estas sejam atendidas é necessário mapear os pré-requisitos essenciais para que os primários sejam cumpridos satisfatoriamente. Destaca-se que esta camada desce em um nível de abstração referente à camada de identificação dos requisitos primários, pois demanda uma análise mais profunda no documento de referência do qual o requisito primário foi extraído ou em documentos de apoio, detalhando o que é necessário para atendê-lo.

Para isso, os documentos de origem dos quais os requisitos primários foram extraídos devem ser analisados minuciosamente em busca desses pré-requisitos. Esta análise deve considerar cada requisito primário como guia para as buscas e o resultado da análise deve ser registrado em uma tabela que será utilizada na camada de Identificação de Evidências. O Quadro 30 apresenta o formulário proposto para ser utilizado nesta atividade.

Quadro 30 - Formulário para levantamento de pré-requisitos

<Requisito Primário>		
Fonte*:<documento de origem do requisito primário>*		
Referência *<nº/nome do item que dispõe o pré-requisito>*	Nome Pré-Requisitos	Descrição
	1.	
	2.	
	3.	

Fonte: Elaborado pela autora (2022).

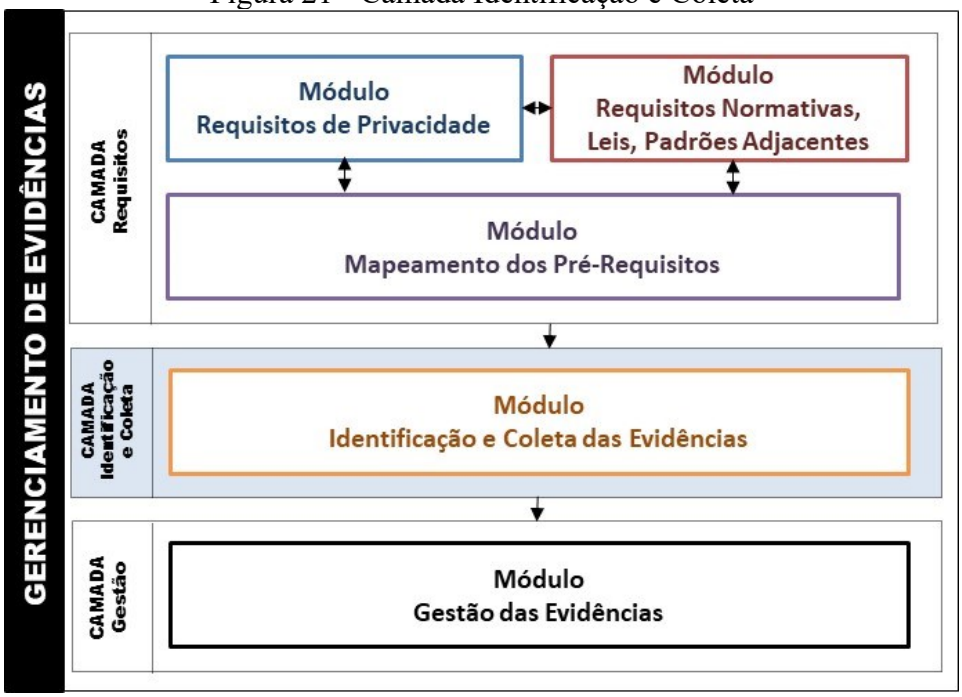
Para o preenchimento da terceira coluna do formulário (Descrição), devem ser considerados os mecanismos e controles de proteção e privacidade requeridos para a implementação do pré-requisito.

5.2.2 Camada de Identificação e Coleta de Evidências

Esta camada destina-se a identificar e coletar artefatos que serão utilizados como evidências, as quais podem ser classificadas como evidências estáticas ou dinâmicas. As estáticas referem-se às que podem ser extraídas e permanecem válidas por um período de tempo

determinado, ou até que alguma mudança ocorra e demande novas extrações, como por exemplo: um organograma, um fluxo de dados, uma arquitetura de redes, entre outros. Já as evidências dinâmicas são aquelas que modificam com frequência e devem ser extraídas o mais recente possível de sua apresentação, como por exemplo: arquivos de CFTV, imagens, registros de ponto, entre outros. Para os casos de evidências estáticas, aplica-se tanto a identificação quanto a coleta dos mesmos. Já as evidências dinâmicas, devido sua característica de atualização, não são coletadas apenas identificadas. E para ambos os tipos de evidências (estáticas e dinâmicas), em sua identificação será realizado um levantamento de características para possibilitar que sejam catalogados e geridos na camada seguinte do modelo.

Figura 21 - Camada Identificação e Coleta



Fonte: Elaborada pela autora (2022).

Para registro das evidências, as questões apresentadas no Quadro 31 devem ser respondidas para cada artefato identificado.

Quadro 31 - Questões para registro das evidências

Q.2. O artefato trata de qual tipo de evidências?
( ) Estática ( ) Dinâmica
Q.3. Qual é a fonte de extração do artefato? _____

Para evidências do tipo estáticas:
Q.4. Onde o artefato ficará armazenado? (descrever o caminho de armazenamento)
Q.5. Qual é o identificador do artefato? (nome/código e a extensão do arquivo)
Q.6. Qual é a data de extração do artefato?

Q.7. Qual é o prazo de validade do artefato? Para evidências do tipo dinâmicas: *Q.7. Como o artefato deve ser extraído de sua fonte?*

Fonte: Elaborado pela autora (2022).

As respostas a essas questões proporcionam um mapeamento das características de cada artefato a ser utilizado como evidência, e possibilitará que os mesmos sejam catalogados, modelados e gerenciados na próxima camada do modelo. As informações coletadas nesta camada, devem ser registradas no formulário apresentado no Quadro 32.

Quadro 32 - Formulário para registro do detalhamento das evidências

Artefato:	
Fonte de Extração:	
Tipo: ( ) Estática - Local de armazenamento do artefato (caminho): - Identificador do artefato (nome/código e extensão): - Data de extração: - Prazo de validade: ( ) Dinâmica - Como o artefato deve ser extraído da fonte?	Observação
A estrutura acima deve ser repetida para todas as evidências identificadas.	

Fonte: Elaborado pela autora (2022).

Para identificar e coletar as evidências, o modelo adota dois instrumentos de apoio que auxiliam no processo de identificação dos artefatos, são eles: 1) a matriz que relaciona as operações de tratamento dos dados com os requisitos de privacidade e 2) a abordagem em perspectivas. Esses instrumentos são utilizados para guiar as entrevistas e apoiar o processo de identificação dos artefatos a serem utilizados como evidência.

5.2.2.1 Instrumentos de Apoio

a) Matriz que relaciona as operações de tratamento dos dados e os requisitos de privacidade

Com a definição das operações de tratamento dos dados apresentadas na subseção 5.1.3, para compor a matriz, buscou-se relacioná-las com os requisitos de privacidade definidos na camada anterior. Nesta atividade, para cada requisito de proteção e privacidade de dados,

procurou-se responder ao seguinte questionamento: Observada a definição do requisito <*requisito de privacidade a ser avaliado*> e os pré-requisitos relacionados a ele, quais as operações de tratamento dos dados que necessitam de atuação para atendê-lo?

Para as respostas que apontaram a necessidade de atuação, foi inserido o símbolo ☑ no ponto de interseção, para serem considerados na coleta de evidências.

O Quadro 33 apresenta a matriz resultante da análise realizada sobre as operações de tratamento com os requisitos de proteção e privacidade de dados.

Quadro 33 - Matriz de análise das etapas do ciclo de tratamento com os requisitos de proteção de privacidade dos dados

Requisitos / Oper. de Tratamento	1	2	3	4	5	6	7	8	9	10	11
Coleta	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Armazenamento	-	-	-	-	☑	☑	-	-	☑	☑	☑
Acesso	-	-	-	-	☑	☑	☑	☑	☑	☑	☑
Compartilhamento	-	-	-	-	☑	-	-	-	☑	☑	☑
Transferência	-	-	-	-	☑	-	-	-	☑	☑	☑
Divulgação	-	-	-	-	☑	-	-	-	☑	☑	☑
Processamento	-	-	-	-	-	☑	☑	☑	☑	☑	☑
Reutilização	☑	☑	☑	☑	☑	-	-	-	☑	☑	☑
Representação	-	☑	-	☑	☑	-	-	-	☑	☑	☑
Descarte	-	-	-	-	☑	-	☑	☑	☑	☑	☑

1 – Consentimento e escolha
2 – Legitimidade e especificado do objetivo
3 – Limitação da Coleta
4 – Minimização dos Dados
5 – Limitação de Uso, Retenção e Divulgação
6 – Precisão e Qualidade
7 – Abertura, Transparência e Notificação
8 – Acesso e Participação Individual
9 – Responsabilização
10 – Segurança da Informação
11 – Conformidade com a Privacidade

Fonte: Elaborada pela autora (2022).

Caso haja fontes regulatórias adjacentes identificadas para o contexto de aplicação do modelo, os requisitos extraídos destas também devem ser adicionados à essa matriz e os mesmos devem ser relacionados às operações de tratamento dos dados, conforme elucida o Quadro 34.

Quadro 34 - Matriz de análise das operações de tratamento com os requisitos extraídos de fontes regulatórias adjacentes

Fonte: Elaborada pela autora (2022).

A elaboração da matriz deve comtemplar os requisitos de todas as fontes regulatórias adjacentes cabíveis ao contexto de aplicação, de forma que todos os requisitos sejam relacionados com as operações de tratamento do dado e assim apresente os pontos para identificação das evidências.

Para a identificação e coleta de evidências, essa matriz é utilizada como guia pois a mesma apresenta os pontos de necessidade de atuação e por consequência os prováveis pontos de existências de artefatos que possam ser utilizados como evidências. Juntamente com a matriz, utiliza-se também o quadro de pré-requisitos, apresentado no Quadro 30, para complementar o entendimento e considerar as ações implementadas em cada pré-requisito em busca de resposta ao seguinte questionamento:

Q.1 - Qual é(são) o(s) artefato(s) a ser(em) utilizado(s) como evidência para cada ponto de intersecção da matriz sinalizada com ☑?

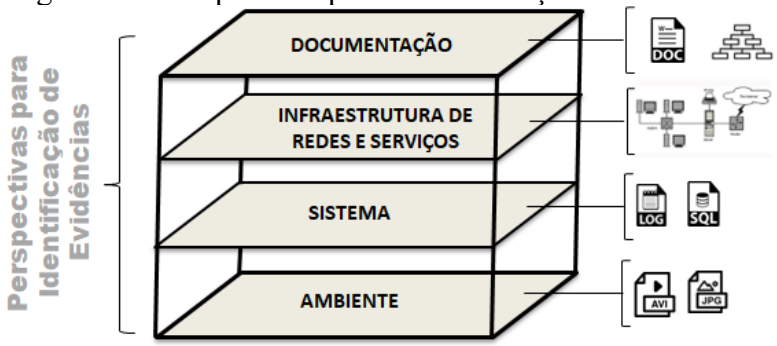
Para exemplificar, considerando a primeira coluna do Quadro 33: *Quais são os artefatos a serem utilizados para evidenciar que o requisito Consentimento e escolha foi atendido na etapa da coleta e reutilização dos dados?*

Essa pergunta deve ser repetida quantas vezes forem necessárias para abordar todos os requisitos de privacidade e demais requisitos, em todas as operações de tratamento dos dados. E a resposta para essa questão resulta nas possibilidades de extração de artefatos, proveniente dos controles implementados, no entanto, deve considerar todos os requisitos listados no Quadro 34, para cada requisito avaliado.

b) Abordagem em perspectivas

Para facilitar a identificação das evidências em resposta a Q.1, optou-se por segmentar a análise em perspectivas (segundo instrumento de apoio), conforme apresentado na Figura 22.

Figura 22 - Perspectivas para a identificação de evidências



Fonte: Elaborada pela autora (2022).

Os artefatos a serem utilizados como evidência podem ser obtidos sob a perspectiva de documentação, infraestrutura de rede e serviços, sistemas e ambiente, sendo esses pertinentes a qualquer cenário que lida com dados, independentemente de sua natureza ou ramo de atuação da organização.

Sendo assim, entende-se que o uso de perspectivas possibilita a avaliação para a identificação de evidências de forma segmentada e direcionada a cada domínio em uma abordagem sistêmica. Ou seja, para atender um determinado requisito, podem existir artefatos em todas as perspectivas sugeridas, em algumas ou apenas em uma delas.

Para auxiliar na identificação dos artefatos que podem ser utilizados como evidências em cada uma das perspectivas, uma lista de possíveis artefatos foi criada com apoio das informações fornecidas pelos especialistas que participaram da pesquisa apresentada no APÊNDICE D. Esta lista é apresentada no Quadro 35.

Quadro 35 - Lista de possíveis artefatos por perspectivas

PERSPECTIVAS	POSSÍVEIS ARTEFATOS
DOCUMENTAÇÃO	Contratos com fornecedores; Termos de aceite/adesão; Código de Ética e Conduta, Política de Proteção e Privacidade de Dados; Política de Segurança da Informação; Termo de Responsabilidade no Uso de Informações; Relatórios de Auditoria; Procedimento de Gestão de Incidentes; Políticas e Procedimentos de maneira geral; Procedimento de Segurança Física; Desenhos de Processos.

INFRAESTRUTURA DE REDES E SERVIÇOS	Topologia de redes; Prints de tela de configurações; Hardening de servidores e estações; Inventário de ativos (hardware e software); Evidências de mudanças que aprovam as configurações (GMUD - Gestão de Mudanças); NDA com fornecedores; Logs de Active Directory, firewall, proxy, SIEM, DLP entre outros serviços; Prints de configurações de IDS/IPS/; Prints de GPOs Prints de atualização periódica de sistemas operacionais; Contratos com fornecedores; Termos de abertura de projetos; Políticas de acesso ao datacenter; Documentação de soluções em nuvem.
SISTEMA	Software Development Lifecycle; Metodologia de Desenvolvimento de Software; Guia de Segurança para o Desenvolvimento e Aquisição de Sistemas; Baseline de Segurança para Databases; Política de desenvolvimento seguro; Testes de vulnerabilidades em sistemas, logs de sistema; Políticas de desenvolvimento seguro com *Privacy by Design*; Arquiteturas de sistemas; Tabelas do banco de dados; Hardening de sistemas; Processos de atualização e validação de código; NDA com fornecedores; entre outros.
AMBIENTE	Sistemas de CFTV; Sistemas de Alarmes; Armários ou repositórios físicos que acomodam dados; Geradores; Nobreaks; entre outros.

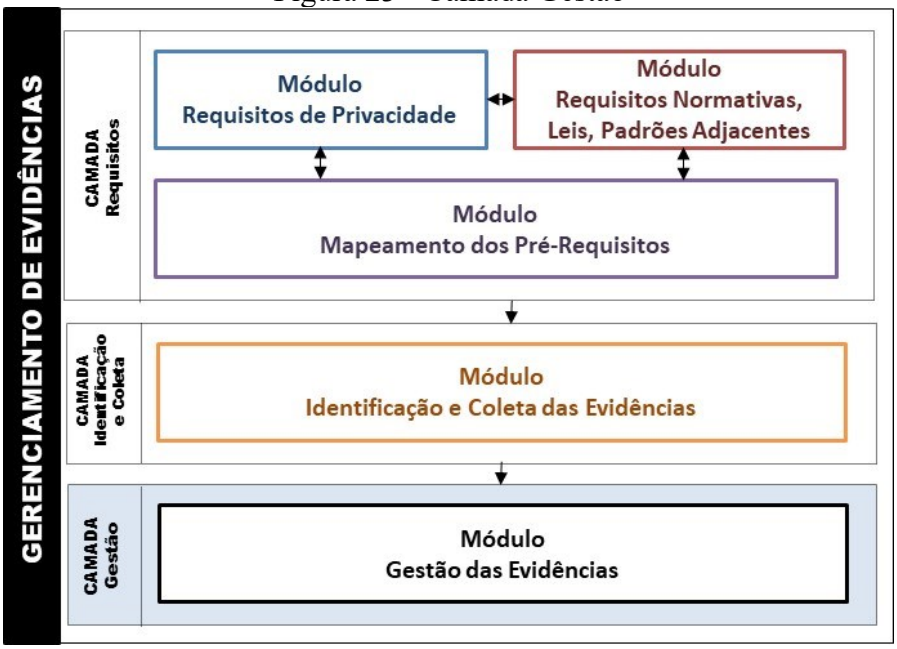
Fonte: Elaborada pela autora (2022).

O uso da abordagem em perspectivas na identificação dos artefatos sistematiza o processo ao incitar o entrevistado a localizar artefatos em diferentes ambientes. Como um guia facilitador para a identificação das evidências, a abordagem em perspectivas auxilia nas entrevistas e na completeza das respostas.

5.2.3 Camada gestão das evidências

Para representar a conformidade e gerir as evidências, optou-se por adotar como notação para representação gráfica, a modelagem de um caso de garantia de privacidade. Conforme abordado anteriormente na subseção 2.5.1, os casos de garantia são utilizados para comprovar a veracidade das alegações feitas a respeito de um determinado assunto, e para isso são utilizados artefatos como evidências.

Figura 23 - Camada Gestão



Fonte: Elaborada pela autora (2022).

Para este estudo, buscou-se ajustar a forma de modelagem e representação dos casos de garantia comumente aplicados para avaliar a segurança em sistemas e em outros contextos, para a comprovação da aderência aos requisitos de privacidade preconizados na normativa de referência ISO 29100.

Para este ajuste foram realizados estudos e análises das abordagens de uso dos casos de garantia já aplicados e publicados e observou-se que o GSN vem sendo utilizado em diferentes contextos.

Ge *et al.* (2012) investigam como uma decisão clínica pode ser argumentada e documentada utilizando o GSN. Esse trabalho apresenta um estudo de caso demonstrando o argumento de uma decisão clínica referente a uma criança diagnosticada com déficit de atenção e hiperatividade com o GSN.

Para Yamamoto e Morisaku (2016), o GSN também pode ser utilizado para representar o BSC (*Balanced Scorecard*). Para os autores, o GSN pode ser usado para decompor os objetivos de negócio de uma estrutura do tipo árvore e expressar as metas de negócio.

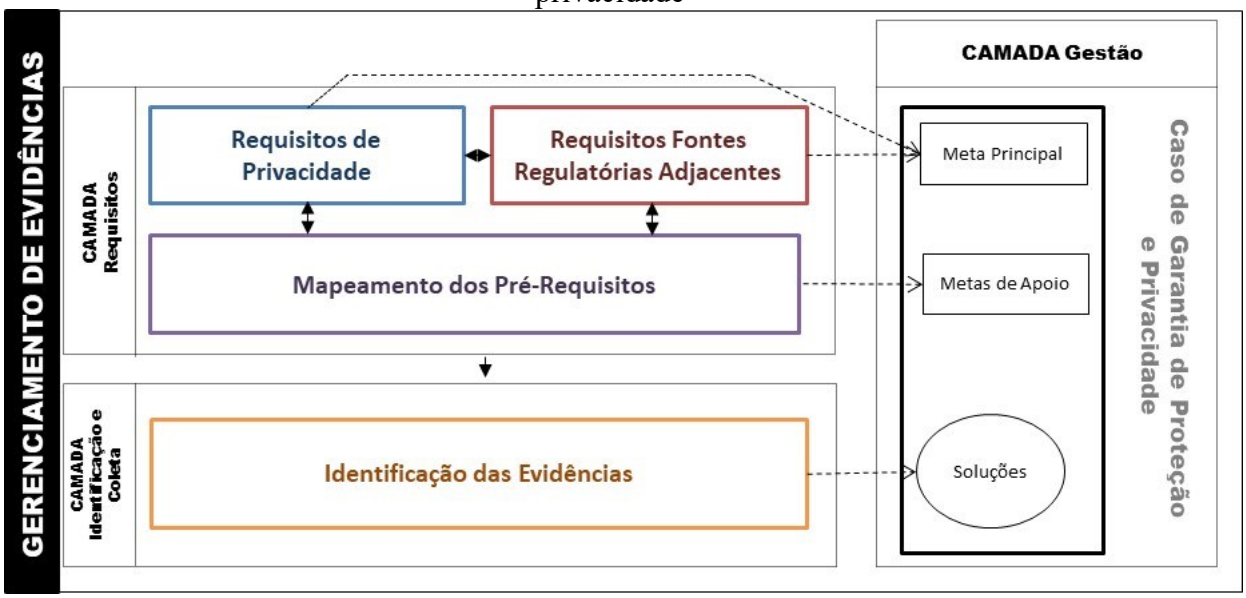
Por sua vez, Kobayashi *et al.* (2020) utilizam o GSN para observar a consistência das políticas de segurança da informação de uma empresa e sua subsidiária. O estudo estrutura a ISO 27001 utilizando o caso de garantia para entender a concordância e discordância entre as políticas de segurança de duas empresas e, utilizando o caso de garantia criado, demonstram como as duas empresas concluem mutualmente um acordo final para uso das políticas.

Considerando a base conceitual existente sobre o tema, foi possível definir a estrutura

do caso de garantia. De acordo com a visão de Kokaly (2017), entende-se que um caso de garantia pode ser modelado de diversas maneiras, desde que contemple os componentes principais: reivindicações, argumentos e evidências na essência de seu propósito, independente da nomenclatura utilizada.

Dada as características dos modelos de notações abordados na subseção 2.5.1, observou-se que a abordagem GSN é a mais adequada para ser utilizada como notação devido ao seu dinamismo, sentido de progressão (top-down de acordo com o modelo proposto) e possibilidade de migração para representações automatizadas em ferramentas. Sendo assim, para definir a estrutura do caso de garantia de privacidade, buscou-se correlacionar as camadas no modelo, com os elementos da GSN, conforme apresentado na Figura 24.

Figura 24 - Correlação das camadas do modelo para a formação do caso de garantia de privacidade



Fonte: Elaborada pela autora (2022).

Os módulos de Requisitos de Privacidade e Requisitos de Fontes Regulatórios Adjacentes pertencentes à Camada de Requisitos, irão compor as Metas Principais do caso de garantia. As saídas do módulo de Mapeamento de Pré-Requisitos irão compor as Metas de Apoio e as saídas da camada de Identificação das Evidências, constituirão as Soluções. Com isso, uma estrutura do caso de garantia de privacidade pode ser construída a partir das duas primeiras camadas do modelo.

Outro fator que pôde ser observado ao se analisar a notação textual registrada nos formulários e a estrutura gráfica apresentada, é que mesmo se considerando somente os dois elementos principais do GSN (Metas e Soluções) para a estrutura dos casos de garantia, a representação gráfica fica extensa e de difícil visualização se modelada em um único diagrama.

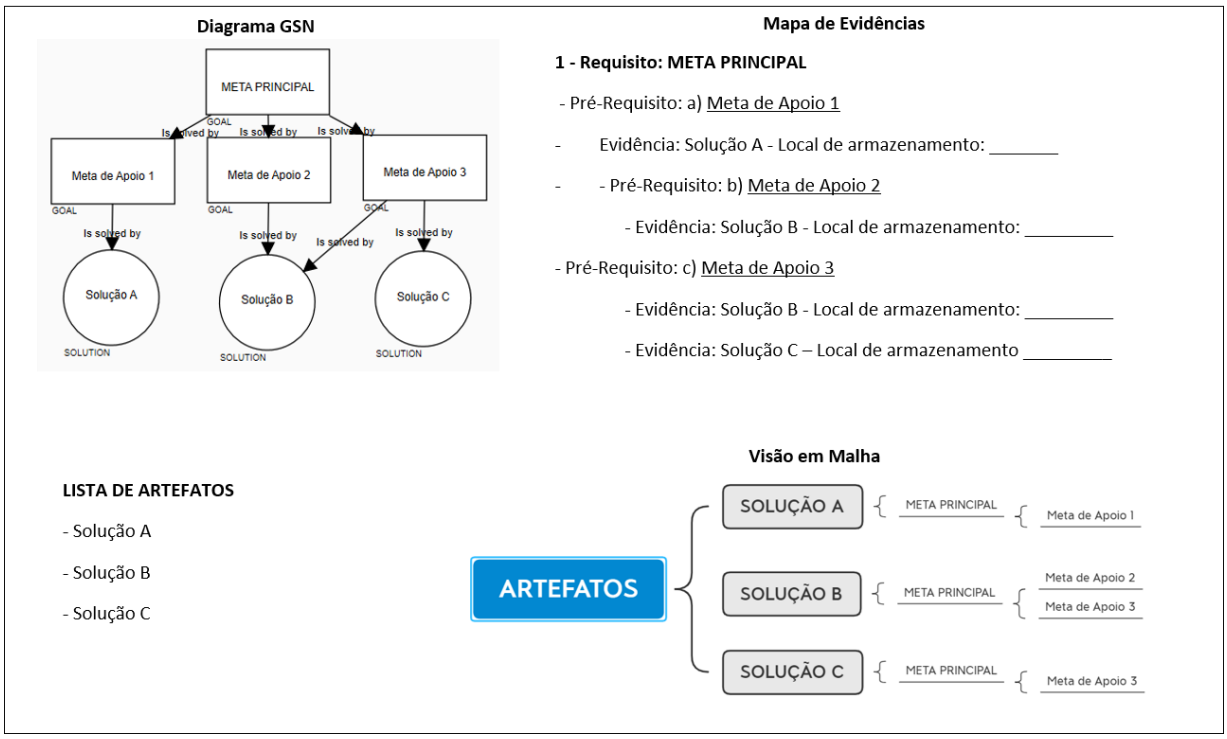
Devido à quantidade de Metas Principais que possam existir em um cenário de aplicação, observou-se a necessidade de serem apresentadas em casos de garantia separadamente.

Verificou-se que, mesmo se considerando somente os requisitos de privacidade apresentados na subseção 5.2.1.1, os quais totalizam 11 Metas, é necessário segmentar o caso de garantia para facilitar a sua visualização. Para isso, propõe-se que sejam desenvolvidos grupos de casos de garantia por Meta e que cada grupo seja apresentado também de forma textual contemplando a localização da evidência (mapa de evidências).

O modelo também contempla uma lista de artefatos identificados e uma visão sob a perspectiva dos artefatos utilizados como evidência, denominada como visão em malha, propiciando uma visão da relação das evidências com diferentes grupos de requisitos, visto a importância desses mapeamentos para se manter a coerência no momento das atualizações dos artefatos.

A Figura 25 elucida as visões contempladas pelo modelo.

Figura 25 - Visões do caso de garantia de privacidade

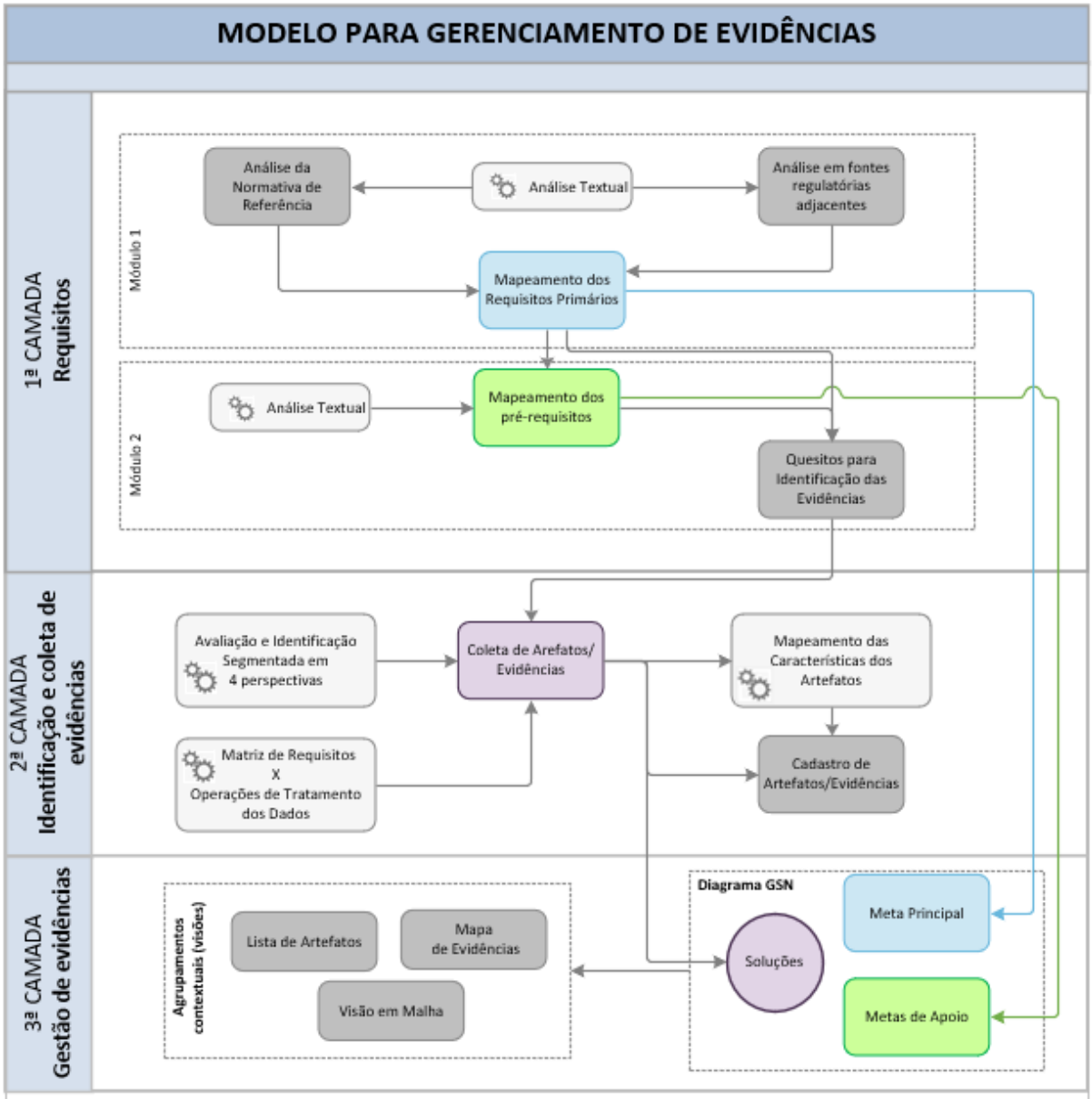


Fonte: Elaborada pela autora (2022).

Para promover a visão sistêmica pretendida para as evidências, propõe-se que os mapas sejam desenvolvidos de forma unitária, por cenário de aplicação do modelo.

A estrutura proposta para o COM.PRIVACY pode ser observada na Figura 26.

Figura 26 - Estrutura proposta para o modelo



Fonte: Elaborado pela autora (2022).

Vale ressaltar que a periodicidade recomendada para aplicação do modelo é anual para os requisitos já implementados. Para os requisitos e pré-requisitos faltantes, o modelo deve ser aplicado na finalização de cada implementação.

5.3 APLICAÇÃO DO MODELO

Esta subseção apresenta as atividades relacionadas à aplicação do modelo a qual corresponde à etapa 4 – Demonstrar o Artefato do ciclo de DSR de Wieringa (2014).

5.3.1 Contextualização da empresa

Para que fosse possível a consolidação das etapas e dos produtos resultantes do COM.PRIVACY, foi estabelecido que o mesmo seria aplicado por completo, em um processo real de uma empresa. Para isso, iniciou-se uma série de contatos com empresas e instituições da Grande Florianópolis, Santa Catarina, solicitando apoio para a aplicação do presente estudo.

A busca foi por uma empresa que já estivesse com o processo de implementação de proteção e privacidade de dados em andamento, pois o modelo trata de evidências e para tê-las era necessário um certo nível de implementação completo. Outro ponto levado em consideração foi o volume e a criticidade dos dados manipulados por essa empresa. Entende-se que em maior ou menor proporção, a grande maioria das empresas manipulam dados pessoais, porém algumas delas em maior volume e essas teriam prioridade para a aplicação do modelo.

Das empresas consultadas, a CASACARESC se colocou à disposição para participar. Registrada na Agência Nacional de Saúde, na modalidade de Autogestão, a CASACARESC foi fundada no ano de 1970. É considerada uma Sociedade Civil, com personalidade jurídica de direito privado, de natureza assistencial, sem finalidades econômicas, sendo operadora de plano de saúde dos funcionários ligados às seguintes empresas: EPAGRI, CIASC, CIDASC, CASACARESC, totalizando atualmente 12.096 beneficiários.

Importante ressaltar que dados de saúde são considerados dados pessoais sensíveis os quais demandam tratativas especiais em relação à sua privacidade. Na tentativa de identificar qual dos processos da CASACARESC possuía maior volume de coleta e retenção de dados pessoais foi disponibilizado o processo de adesão de beneficiários, o qual retém todo o cadastro de beneficiários, assim como históricos de saúde dos titulares e de todos os seus dependentes.

Ficou acordado com a diretoria da instituição que toda documentação referente à experimentação, gerada a partir das entrevistas e produzidas na aplicação do modelo, seriam disponibilizados à equipe da CASACARESC e que poderia também ser utilizada como documentação desta pesquisa, visto que as atividades não contemplariam dados pessoais de beneficiários e sim o processo de adesão e as ações encaminhadas para o tratamento dos dados. O documento contendo a autorização da diretoria para a realização das atividades, acesso às informações e uso das informações obtidas na tese se encontra no APÊNDICE F desta tese.

Vale ressaltar que a CASACARESC, no período da aplicação do modelo estava sob a orientação de uma empresa de consultoria para a implantação de proteção e privacidade de dados, e a funcionária responsável por acompanhar essa consultoria foi designada para

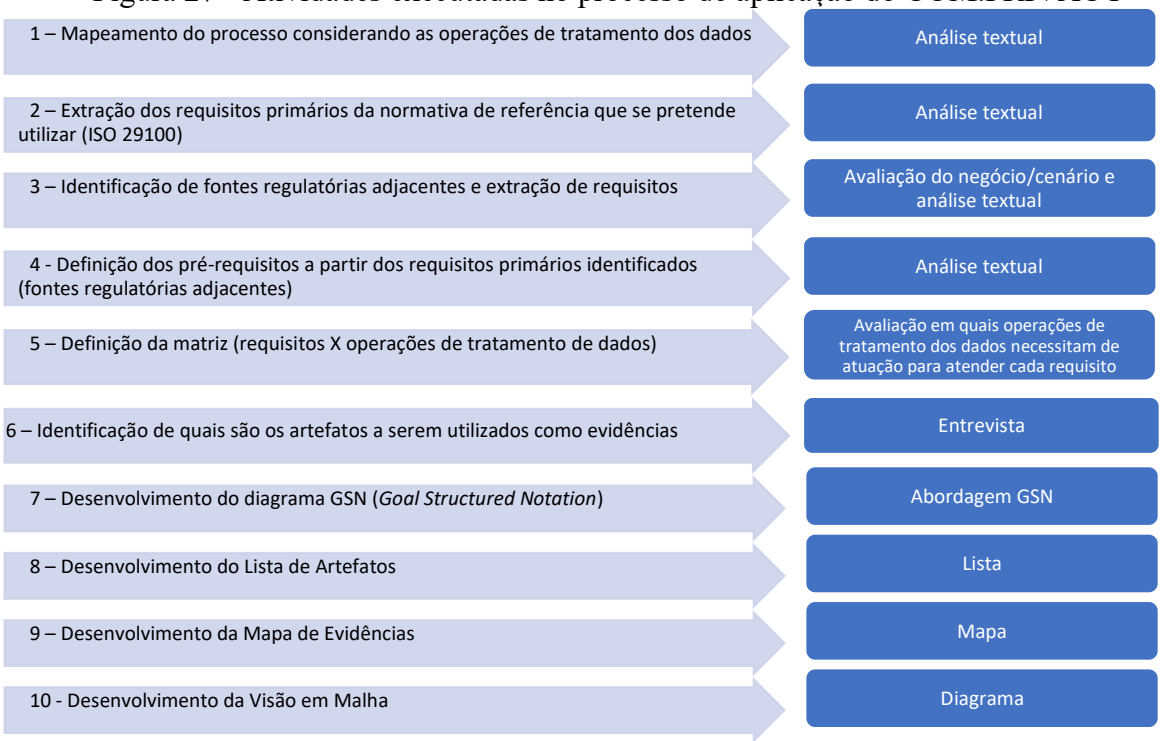
acompanhar o trabalho de aplicação do COM.PRIVACY, bem como participar das entrevistas, enviar os documentos e esclarecer dúvidas que surgiram durante as atividades.

5.3.2 Processo de aplicação do modelo

Ao iniciar os trabalhos com a CASACARESC, foi realizada uma reunião presencial com a presença da diretoria na qual foram apresentados o modelo desenvolvido, as atividades que seriam realizadas em sua aplicação e uma sugestão de periodicidade de interações para sua execução. Nesta reunião foi designada a representante da instituição que acompanharia o trabalho e foram realizados os ajustes no cronograma de interações de acordo com a disponibilidade da mesma.

A Figura 27 apresenta as atividades que foram executadas no processo de aplicação do modelo da instituição CASACARESC. A seguir as mesmas estão descritas de acordo com as camadas do modelo para facilitar o entendimento e correlação.

Figura 27 - Atividades executadas no processo de aplicação do COM.PRIVACY



Fonte: Elaborado pela autora (2022).

A primeira atividade realizada foi o mapeamento do processo de Adesão de Beneficiários, visto que até então não se tinha conhecimento de seu funcionamento. A empresa de consultoria que estava em atuação junto à CASACARESC já tinha iniciado o processo de

mapeamento, porém não em todas as operações de tratamento dos dados que foram adotadas para o modelo. Dessa forma, o processo foi mapeado junto à representante da instituição, considerando as seguintes operações de tratamento: Acesso, Transferência, Divulgação, Processamento e Reutilização do dado, tendo em vista que as operações de Coleta, Armazenamento, Compartilhamento e Eliminação já haviam sido mapeadas pela CASACARESC e pela consultoria.

Com o processo mapeado foi possível entender seu funcionamento assim como ter conhecimento sobre os dados que são tratados em cada etapa.

5.3.4 Camada de requisitos

Na segunda atividade, foi feita uma análise textual, em que os requisitos primários foram extraídos da normativa de referência de proteção e privacidade de dados que se pretendia utilizar, neste caso a ISO 29100. Conforme apresentado, foram adotados os 11 princípios preconizados pela normativa. Para essa atividade não houve a necessidade de interações com a representante da instituição CASACARESC, sendo realizada apenas pela pesquisadora, visto que se trata de uma atividade já prevista na estruturação do modelo.

A terceira atividade contemplou a obtenção das fontes regulatórias adjacentes, as quais tiveram como premissa serem obrigatórias e apresentar em seu conteúdo algum tipo de influência no tratamento dos dados. Para esta atividade, a representante da instituição buscou informações junto à assessoria jurídica para garantir a completude destas. Para esse cenário foi identificada apenas a Resolução Normativa nº 117 da Agência Nacional de Saúde (ANS), de 30 de novembro de 2005, que no Capítulo II – Da Identificação de Clientes e Manutenção de Registros, traz no artigo 4º que: “Os cadastros, registros e documentos mencionados nos arts. 2º e 3º devem ser mantidos organizados, à disposição da ANS, durante o período mínimo de cinco anos, a partir da emissão do(s) documento(s).”. Dessa forma, o tempo de retenção dos documentos definidos por essa resolução normativa, tornou-se parte dos requisitos primários a serem considerados na aplicação do COM.PRIVACY.

Na quarta atividade, com os requisitos primários identificados, as suas fontes regulatórias foram avaliadas textualmente para a identificação dos pré-requisitos necessários. Pré-requisitos são todas as condições necessárias para se alcançar os requisitos primários. Esta atividade foi realizada pela pesquisadora sem interação com a representante da instituição CASACARESC. Na Figura 28 pode-se observar os pré-requisitos do requisito Consentimento e Escolha, registrados no formulário.

Figura 28 - Pré-requisitos para o requisito consentimento e escolha

REQUISITO	PRÉ-REQUISITO
1. CONSENTIMENTO E ESCOLHA	**Permissão de escolha do tratamento de DP** a) Apresentar ao titular de DP a escolha de permitir ou não o tratamento de seus DP, exceto quando o titular de DP não puder livremente reter o consentimento ou onde a legislação aplicável permitir especificamente o tratamento de DP sem o consentimento da pessoa natural. A escolha do titular de DP deve ser dada livremente, específica e com conhecimento fornecendo mecanismos claros, acessíveis, inteligíveis e facilmente compreensíveis
	Obtenção formal do consentimento b) Obter o consentimento *opt-in* de aceitação do titular de DP para coletar ou processar os DP sensíveis, exceto onde a lei aplicável permitir o processamento de DP sensível sem o consentimento da pessoa natural.
	Informativo participação e acesso individual c) Informar aos titulares de DP, antes de obter o consentimento, sobre os seus direitos sob o princípio de participação e acesso individual;
	Informativo abertura, transparência e notificação d) Fornecer aos titulares de DP, antes da obtenção do consentimento, as informações indicadas pelo princípio da abertura, transparência e notificação
	Implicações da concessão e retenção do consentimento e) Explicar aos titulares de DP as implicações da concessão ou retenção do consentimento.
	Revogação do consentimento

Fonte: Elaborado pela autora (2022).

5.3.5 Camada de identificação e coleta de evidências

A atividade cinco, também realizada apenas pela pesquisadora, consistiu na construção da matriz que relaciona os requisitos primários com as operações de tratamento dos dados, sinalizando os pontos que necessitam de atuação para sua implementação. A matriz trata-se de um instrumento de apoio para a condução das entrevistas que buscam identificar os artefatos que podem ser utilizados como evidência. Sua construção ocorreu avaliando em quais operações de tratamento dos dados necessitam de atuação para atender cada requisito, com base nas respostas obtidas ao seguinte questionamento: Observada a definição do requisito <*requisito de privacidade a ser avaliado*> e os pré-requisitos relacionados a ele, em quais operações de tratamento dos dados necessitam de atuação para atendê-lo? A matriz foi construída na medida em que cada item questionado resultou em respostas positivas.

Na atividade seis o objetivo foi identificar os artefatos que poderiam ser utilizados como evidências, para isso foram realizadas entrevistas com a representante da instituição CASACARESC as quais ocorreram na modalidade presencial e por videoconferência.

Os instrumentos de apoio (abordagem em perspectivas e a matriz) foram utilizados para conduzir as entrevistas e as evidências identificadas para cada pré-requisito existente foram

registradas em formulário.

A Figura 29 apresenta o formulário complementado com as evidências identificadas.

Figura 29 - Formulário preenchido com as evidências

REQUISITO	PRÉ-REQUISITO	ARTEFATO
1. CONSENTIMENTO E ESCOLHA	**Permissão de escolha do tratamento de DP** a) Apresentar ao titular de DP a escolha de permitir ou não o tratamento de seus DP, exceto quando o titular de DP não puder livremente reter o consentimento ou onde a legislação aplicável permitir especificamente o tratamento de DP sem o consentimento da pessoa natural. A escolha do titular de DP deve ser dada livremente, específica e com conhecimento fornecendo mecanismos claros, acessíveis, inteligíveis e facilmente compreensíveis	**Formulário de Adesão**
	Obtenção formal do consentimento b) Obter o consentimento *opt-in*/de aceitação do titular de DP para coletar ou processar os DP sensíveis, exceto onde a lei aplicável permitir o processamento de DP sensível sem o consentimento da pessoa natural.	**Não se aplica para Coleta Dados (legitimo interesse)** **Formulário de Adesão**
	Informativo participação e acesso individual c) Informar aos titulares de DP, antes de obter o consentimento, sobre os seus direitos sob o princípio de participação e acesso individual;	**Política de Privacidade**
	Informativo abertura, transparência e notificação d) Fornecer aos titulares de DP, antes da obtenção do consentimento, as informações indicadas pelo princípio da abertura, transparência e notificação	**Política De Privacidade**
	Implicações da concessão e retenção do consentimento e) Explicar aos titulares de DP as implicações da concessão ou retenção do consentimento.	**Formulário de Adesão**
	Revogação do consentimento	**Formulário de Requisição de Direitos do Titular de Dados**

Fonte: Elaborado pela autora (2022).

Para esta atividade de identificação e coleta das evidências, ressalta-se que o uso dos instrumentos de apoio apresentou contribuição para os resultados obtidos visto que a identificação dos artefatos não ocorreu de forma imediata aos questionamentos e, na medida em que os instrumentos foram sendo abordados e a entrevistada induzida a pensar sob diversas perspectivas e em diferentes operações de tratamento dos dados, as identificações foram facilitadas. Todos os requisitos e pré-requisitos foram abordados de forma a concluir a identificação das evidências com êxito.

Durante a aplicação do modelo, uma situação foi observada e imediatamente tratada. Foi identificado que dados referentes às perspectivas pelas quais as evidências eram obtidas, não se tratava de um dado relevante para registro, ou seja, que a abordagem em perspectivas estava sendo útil apenas na condução das entrevistas com a finalidade de identificação das evidências. Com isso, os formulários já foram alterados e as informações deixaram de compor os formulários de registro. Após a adequação implementada, a nova versão foi utilizada para a continuidade da aplicação.

Para cada evidência identificada, foi gerado um cadastro com suas características para que possam ser geridas na camada seguinte. Para exemplificar, a Figura 30 apresenta o cadastro do artefato Política de Privacidade identificado na aplicação do COM.PRIVACY.

Figura 30 - Cadastro política de privacidade

Artefato: **20. Política de Privacidade**	
Fonte de Extração: **Site da CasaCaresc**	
Tipo: (x) Estática - Local de armazenamento do artefato (caminho): **Site da CasaCaresc** **https://www.casacaresc.org.br/privacidade/politica_de_privacidade.php** - Identificador do artefato (nome/código e extensão): **Política de Privacidade** - Data de extração: **20/01/2022** - Prazo de validade: **22/04/2022** ( ) Dinâmica - Como o artefato deve ser extraído da fonte?	Observação

Fonte: Elaborada pela autora (2022).

As informações obtidas até aqui oriundas da aplicação do modelo foram registradas nos formulários apresentados e em um sistema de cadastro desenvolvido para apoiar este experimento. Porém, esse sistema foi desenvolvido com o objetivo de facilitar o processo de aplicação do COM.PRIVACY, não sendo esse um produto desta pesquisa. O modelo pode ser aplicado com a utilização dos formulários apresentados neste trabalho sem a necessidade de nenhuma operação de automação, pois durante a experimentação os formulários sugeridos foram testados e apresentaram resultado satisfatório.

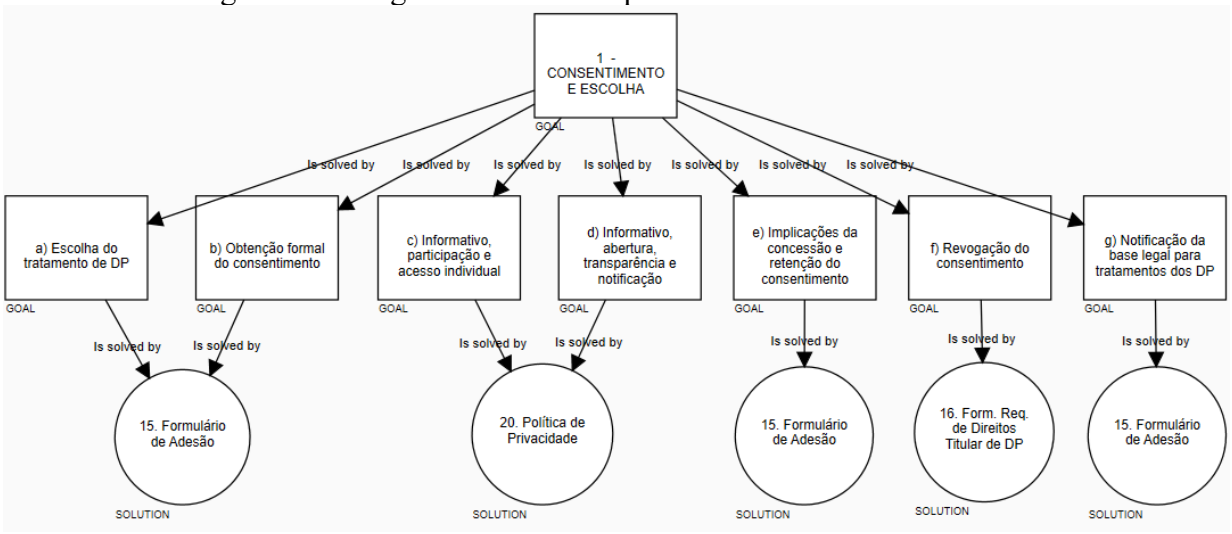
5.3.6 Camada de gestão de evidências

Na atividade sete, em posse das informações obtidas nas entrevistas, com o uso da abordagem GSN, o diagrama foi construído utilizando os componentes Meta e Soluções. Para essa atividade foi utilizada a ferramenta Assurance and Safety Case Environment (ASCE)[13] em uma licença acadêmica concedida pelo fornecedor à pesquisadora, para a realização desse trabalho.

A Figura 31 apresenta o diagrama GSN do requisito Consentimento e Escolha mapeado para o cenário de aplicação do modelo.

[13] Mais informações sobre a ferramenta Assurance and Safety Case Environment (ASCE) podem ser obtidas em https://www.adelard.com/asce/choosing-asce/index/

Figura 31 - Diagrama GSN do requisito consentimento e escolha



Fonte: Elaborada pela autora (2022).

A atividade oito abordou o desenvolvimento da Lista de Artefatos. Todos os artefatos identificados e registrados nos formulários foram listados, totalizando 29 artefatos, conforme apresentados parcialmente na Figura 32. Para a construção dessa lista, os artefatos foram organizados em ordem alfabética e numerados para facilitar sua localização.

Figura 32 - Lista de artefatos identificados

1	Análise de Riscos de Privacidade de Dados
2	Arquivo encaminhado por e-mail (Unimed e Uniodonto)
3	Autenticação por Usuário e Senha
4	Clausula Contratual com Fornecedores
5	Configuração Bloqueio de Sessão
6	Configurações de Acessos por Perfil
7	Controle de acesso físico (alarme)
8	Controle de acesso físico armários
9	Controle de Descarte
10	Cópia dos Documentos de Identificação

Fonte: Elaborada pela autora (2022).

Na atividade 9, em que foi desenvolvido o mapa de evidências, buscou-se formatar para modo textual as informações obtidas nas entrevistas referentes às evidências identificadas para cada pré-requisito, conforme apresentado na Figura 33.

Figura 33 - Exemplo de mapa de evidências

1 - Requisito: CONSENTIMENTO E ESCOLHA

- Pré-Requisito: a) Escolha do tratamento de DP

- Evidência: 15. Formulário de Adesão - Local de armazenamento: - Sistema Benner – Módulo Beneficiário e Armários

- Pré-Requisito: b) Obtenção formal do consentimento

- Evidência: 15. Formulário de Adesão - Local de armazenamento: - Sistema Benner – Módulo Beneficiário e Armários

- Pré-Requisito: c) Informativo, participação e acesso individual

- Evidência: 20. Política de Privacidade - Local de armazenamento: Site da CasaCaresc https://www.casacaresc.org.br/privacidade/politica_de_privacidade.php

- Pré-Requisito: d) Informativo abertura, transparência e notificação

- Evidência: 20. Política de Privacidade - Local de armazenamento: Site da CasaCaresc https://www.casacaresc.org.br/privacidade/politica_de_privacidade.php

- Pré-Requisito: e) Implicações da concessão e retenção do consentimento

- Evidência: 15. Formulário de Adesão - Local de armazenamento: - Sistema Benner – Módulo Beneficiário e Armários

- Pré-Requisito: f) Revogação do consentimento

- Evidência: 16. Formulário de Requisição de Direitos do Titular de DP - Local de armazenamento: https://docs.google.com/forms/d/11wn_zzlqH_j6ZQcSh6Jbim02NEyo_8jKVZxec7-_c7g/prefill

- Pré-Requisito: g) Notificação da base legal para tratamento dos DP

- Evidência: 15. Formulário de Adesão - Local de armazenamento: - Sistema Benner – Módulo Beneficiário e Armários

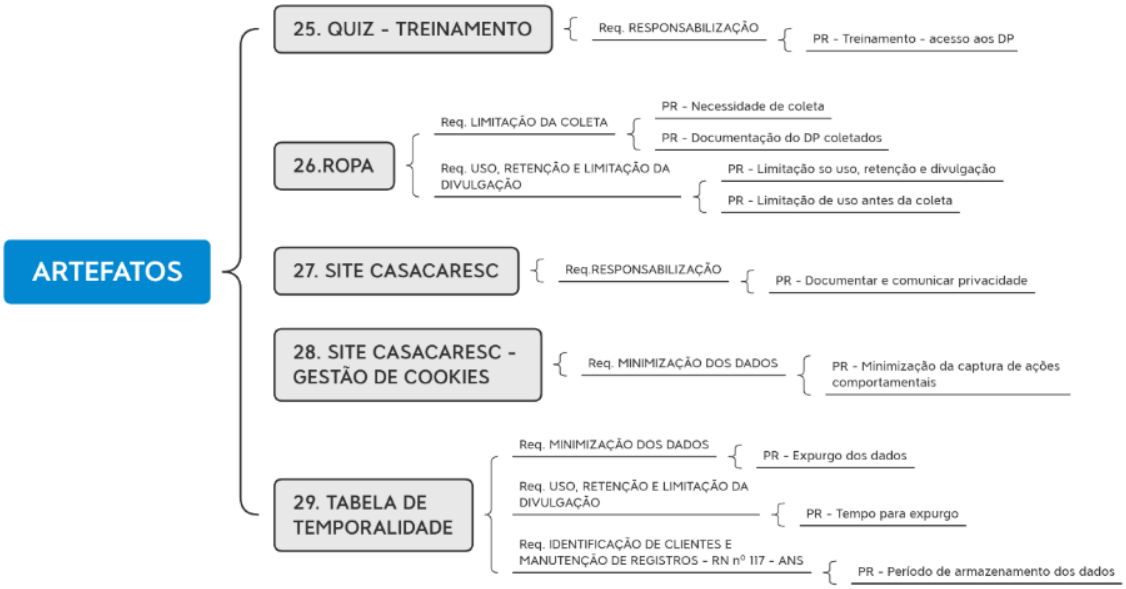
Fonte: Elaborada pela autora (2022).

Os mapas de evidências contemplam além do requisito e pré-requisito, o local de armazenamento das mesmas para facilitar a localização. Para possibilitar uma visão sob a perspectiva do artefato, o COM.PRIVACY previu a Visão em malha desenvolvido na atividade dez. O objetivo deste diagrama é dispor, a partir da evidência, quais requisitos e pré-requisitos são atendidos com ela. Importante ressaltar que essa visão proporciona visibilidade das dependências e assim viabiliza que, sempre que for necessário algum tipo de atualização nas evidências, estas sejam feitas com entendimento das relações existentes entre diferentes pré-requisitos e com o menor impacto possível.

Na Figura 34 é possível observar um exemplo do diagrama da visão em malha obtida na aplicação do modelo na instituição CASACARESC [14].

[14] Para a elaboração do diagrama de visão em malha foi utilizada a ferramenta XMind2020 em sua versão trial. Mais informações sobre a ferramenta XMind2020 podem ser obtidas em https://www.xmind.net/

Figura 34 - Exemplo de visão em malha



Fonte: Elaborada pela autora (2022).

As atividades 7 (Diagrama GSN), 8 (Lista de Artefatos), 9 (Mapa de Evidências) e 10 (Visão em Malha) foram realizadas pela pesquisadora sem interação direta com a representante da instituição CASACARESC. Durante a execução dessas atividades, algumas dúvidas e confirmações foram esclarecidas por e-mail.

Com isso, concluiu-se as atividades de aplicação do COM.PRIVACY e após a conclusão do desenvolvimento diagrama dos diagramas, listas e mapas de evidências, os mesmos foram apresentados em uma reunião presencial que envolveu a diretoria da CASACARESC, para validação e conclusão do trabalho.

5.5 CONSIDERAÇÕES SOBRE O COM.PRIVACY

Dada a complexidade e dinamismo do tema proteção e privacidade de dados, sempre foi uma das premissas desta pesquisa que o modelo proposto apresentasse facilidade em seu entendimento e aplicação e que o mesmo fosse entendido pelos profissionais da área, assim como pelos titulares dos dados, como útil e que fornecesse contribuições para ambos os papéis. Dessa forma, o modelo está estruturado em camadas para segmentar as atividades e apresenta em cada uma delas os métodos e os instrumentos de apoio que possam contribuir e facilitar sua utilização. O modelo proposto pode ser aplicado em empresas de qualquer porte, pois foi estruturado para que possa ser aplicado considerando escopos definidos, ou seja pode ser

aplicado em um processo, em uma área, em um produto. Nos casos de empresas maiores, o tempo de aplicação no contexto completo pode ser mais longo, porém seu objetivo é focar na segmentação dos escopos para que possam obter resultados em menor tempo.

Vale destacar que o modelo apresentado nesta pesquisa utiliza a abordagem GSN de forma simplificada utilizando apenas dois componentes: Meta principal e de apoio e soluções, podendo ser complementado com os demais componentes integrantes da abordagem original, de acordo com o que for identificado como necessário.

O modelo deve ser revisado anualmente para garantir a completeza e pertinência com o escopo de aplicação. Para isso, um agendamento prévio deve ser realizado logo após a aplicação do modelo para que depois de um ano o mesmo seja validado e analisado criticamente quanto à sua adequação. Em casos de mudanças no escopo, sendo elas em um processo, um sistema ou em um produto, o modelo deve ser reaplicado imediatamente para que permaneça coerente com o cenário do escopo.

Finaliza-se esta seção ressaltando que não foi objetivo desta tese aplicar o modelo em um contexto completo de uma empresa e sim em um escopo definido, neste caso em um processo, para testar suas funcionalidades. Com sua aplicação pode-se concluir que, da forma apresentada, o modelo possibilita sua utilização conforme se propõe e permite que o trabalho seja ampliado a novos escopos caso desejado.

6 AVALIAÇÃO DO COM.PRIVACY

Esta seção apresenta os resultados da pesquisa realizada com os especialistas para avaliar o modelo para gerenciamento de evidência de proteção e privacidade de dados proposto nessa tese. Para esta avaliação foram convidados especialistas da área de segurança da informação, proteção e privacidade de dados, os quais guiados por questões predefinidas declararam suas opiniões sobre o COM.PRIVACY.

Inicialmente são apresentados os objetivos da avaliação e em seguida são expostas as atividades de planejamento e preparação da avaliação (Seção 6.2). Na seção 6.3 expõe-se como a avaliação foi aplicada e a subseção 6.3.1 em diante aborda a análise e os resultados da mesma.

6.1 OBJETIVOS DA AVALIAÇÃO

A avaliação do COM.PRIVACY foi realizada utilizando o método Painel de Especialistas e contemplou os seguintes objetivos:

a) verificar se o universo/delimitação do campo de conhecimento utilizado é o necessário para cumprir o propósito do modelo (**Escopo**);

b) verificar se o nível de aprofundamento e decomposição do modelo está adequado (**Profundidade e Precisão**);

c) verificar se a amplitude de aplicação do modelo e a possibilidade de aplicação em cenários distintos com diferentes características foram observados pelos especialistas e estão de acordo (**Generalidade**);

d) verificar se na visão dos especialistas, o modelo apresenta a capacidade de *suportar* e contém todos os elementos necessários para cumprir eficientemente o seu propósito *(***Robustez e Completeza**);

e) verificar se o modelo pode ser entendido e aplicado com facilidade (**Clareza**);

f) verificar se na visão dos especialistas o modelo provê *consistência nas informações fornecidas (***Consistência**);

g) verificar se na visão dos especialistas entrevistados, o COM.PRIVACY contribui no contexto da proteção e privacidade de dados com sua abordagem em gerenciamento de evidências e se recomendariam o uso do modelo (**Contribuição/Recomendação**).

6.2 PLANEJAMENTO E PREPARAÇÃO DA AVALIAÇÃO

Ao se iniciar o processo de avaliação observou-se que a mesma envolveria a participação de seres humanos e com isso fez-se necessário submeter a pesquisa, bem como o processo de avaliação para a apreciação do Comitê de Ética em Pesquisas com Seres Humanos (CEPSH) da Universidade Federal de Santa Catarina (UFSC). O mesmo foi submetido e o parecer para a realização da avaliação foi favorável, emitido sob o processo de nº 55847922.5.0000.0121, conforme disponível do APÊNDICE G.

Em relação ao perfil dos especialistas que participaram da avaliação, não foram estabelecidas restrições em relação à sua formação, visto que nessa área atuam profissionais com formação diversas. Porém, foi adotado o critério de que os especialistas atuassem em projetos que envolvem a adequação aos preceitos de proteção e privacidade de dados.

Em relação à titulação mínima, foi definido que os participantes da avaliação teriam no mínimo pós-graduação *lato sensu*. Decidiu-se por essa titulação para possibilitar que tanto profissionais que atuassem em empresas, como na academia como docentes ou pesquisadores ou de forma autônoma, pudessem participar. Entendeu-se que devido a se tratar de uma área em constante desenvolvimento, a definição de alguma restrição com relação à titulação poderia impedir a participação de alguns convidados com relevância para a pesquisa.

Dada a natureza dos objetivos definidos para a avaliação do COM.PRIVACY, foi elaborado um questionário a ser preenchido pelos especialistas, o qual foi organizado em três etapas. A primeira etapa apresentou o Termo de Consentimento Livre e Esclarecido (TCLE) — disponível no Apêndice H; a segunda etapa teve como intuito identificar o perfil dos participantes; e a terceira consistiu na avaliação do modelo propriamente dito. A etapa 2 (perfil dos participantes) contou com sete questões e a etapa 3 (Avaliação do Modelo) com sete questões também, conforme disponível no APÊNDICE I desta tese[15].

Cada objetivo apresentado na seção anterior originou uma questão sobre o modelo, conforme apresentado no Quadro 36, e o especialista entrevistado teve a oportunidade de qualificar sua resposta de acordo com a escala Likert: 1 – Discordo, 2 – Nem discordo, nem concordo e 3 – Concordo. Além disso, cada questão disponibilizou um campo de observações para possibilitar uma argumentação, complementação ou sugestões e oportunidades de melhoria.

[15] Disponível em: https://docs.google.com/forms/d/e/1FAIpQLScPWvjS3GQ_E2fbPdczn2ITC-k6PXfnIciFDBBOERnpu_F8dg/viewform

Quadro 36 - Objetivos e questões avaliadas

ITEM AVALIADO	OBJETIVO DA QUESTÃO	QUESTÕES AVALIADAS
ESCOPO	Verificar se o universo/delimitação do campo de conhecimento utilizado é o necessário para cumprir o propósito do modelo.	**Q1.** O modelo abrange o campo de conhecimento necessário para estruturar o processo de gerenciamento de evidências no âmbito da segurança e privacidade de dados.
PROFUNDIDADE E PRECISÃO	Verificar se o nível de aprofundamento e decomposição do modelo está adequado.	**Q2.** O nível de detalhamento do modelo (etapas, atividades e tarefas) é adequado e suficiente para comprovar uma alegação de segurança e privacidade com o gerenciamento de evidências.
GENERALIDADE	Verificar se a amplitude de aplicação do modelo e a possibilidade de aplicação em cenários distintos com diferentes características foram observados pelos especialistas e estão de acordo.	**Q3.** O modelo, da forma em que foi estruturado, possibilita sua aplicação em diferentes setores e negócios, considerando as especificidades de cada segmento.
ROBUSTEZ E COMPLETEZA	Verificar se na visão dos especialistas, o modelo apresenta a capacidade de suportar e contém todos os elementos necessários para cumprir eficientemente o seu propósito**.**	**Q4.** O modelo é abrangente o suficiente e apresenta os componentes necessários para sustentar uma alegação de segurança e privacidade de dados.
CLAREZA	Verificar se o modelo pode ser entendido e aplicado com facilidade.	**Q5.** O modelo é facilmente entendido e fácil de ser aplicado.
CONSISTÊNCIA	Verificar se na visão dos especialistas o modelo provê consistência nas informações fornecidas.	**Q6.** O modelo apresenta coerência nas bases estruturantes adotadas (*Privacy by Design*, ISO 29100 e operações de tratamento de dados) e em suas etapas, provendo informações consistentes que apoiam a comprovação de alegações de segurança e privacidade de dados.
CONTRIBUIÇÃO/ RECOMENDAÇÃO	Verificar se na visão dos especialistas entrevistados, o COM.PRIVACY contribui no contexto da proteção e privacidade de dados com sua abordagem em gerenciamento de evidências e se recomendariam o uso do modelo.	**Q7.** Considerando as opções de modelos/métodos/metodologias existentes, recomendo a adoção do modelo de gerenciamento de evidências apresentado, pois o mesmo apresenta grande contribuição na comprovação de requisitos e alegações de segurança e privacidade de dados.

Fonte: Elaborado pela autora (2022).

Para a avaliação do COM.PRIVACY foram convidados oito especialistas e desses, seis concordaram em participar da pesquisa. Para o convite foram realizados contatos telefônicos com os mesmos e nestes foi explanada a forma de condução e o tempo que seria necessário para finalizar as avaliações.

O tempo necessário para a realização do processo de avaliação foi de 1 hora e 15 minutos, sendo 1 hora para a apresentação e quinze minutos para preenchimento da avaliação. No período de tempo definido para a apresentação, foram expostos os conteúdos referentes ao modelo e sua aplicação. E os 15 minutos destinados ao preenchimento da avaliação foram designados aos participantes para responderem os questionamentos de avaliação e exporem suas opiniões.

6.3 APLICAÇÃO DA AVALIAÇÃO

A avaliação foi realizada de forma individual e na apresentação foram contemplados os seguintes assuntos: (i) o modelo e seu funcionamento, (ii) a apresentação do sistema utilizado em sua aplicação, e (iii) uma breve explanação das questões que seriam respondidas por eles na avaliação.

Os agendamentos foram realizados de acordo com a disponibilidade de cada participante e as apresentações aconteceram pelo Google Meet, guiadas por uma apresentação contendo 15 slides[16]. Foram apresentados o modelo e seu funcionamento e as etapas de aplicação, assim como um exemplo dos diagramas, listas e mapas que são produtos do modelo. Esse momento também foi utilizado para esclarecer as dúvidas dos participantes e complementar a explicação conforme a necessidade de cada um deles. Após o término, um link do Google Forms[17] foi encaminhado para que o especialista pudesse responder a avaliação e incluir em cada item uma observação/sugestão.

6.4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

Conforme já mencionado, a primeira etapa da avaliação foi a apresentação do TCLE com todas as especificações e riscos inerentes a participação da avaliação e neste quesito todos

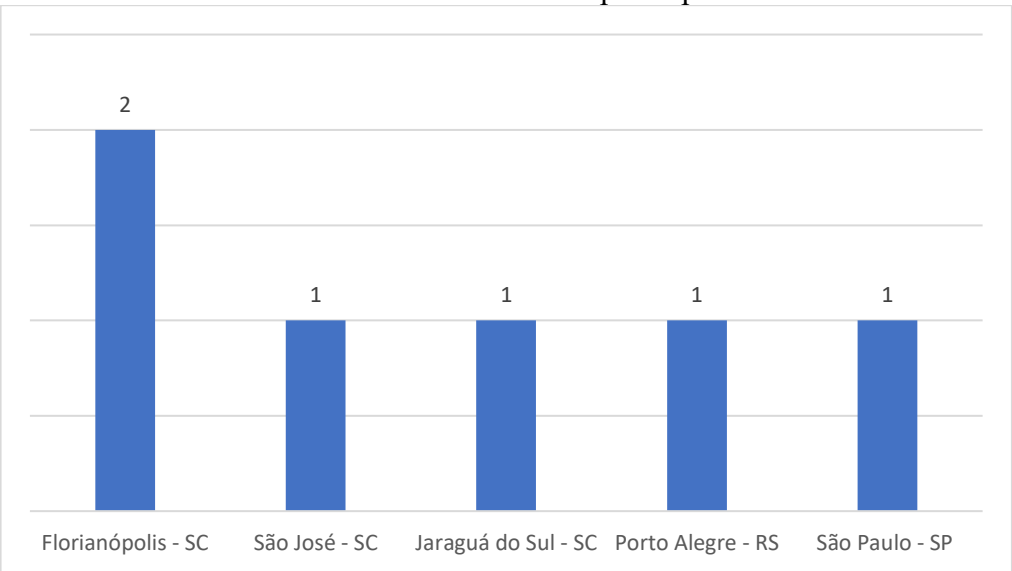
[16] Disponível em: http://www.gislainepfreund.com.br/comprivacy/avaliacao.htm
[17] https://docs.google.com/forms/d/e/1FAIpQLScPWvjS3GQ_E2fbPdczn2ITC-k6PXfnIciFDBBOERnpu_F8dg/viewform

os participantes declararam ter lido e aceitar os termos descritos.

Na segunda etapa da avaliação foram coletadas informações referentes ao perfil dos participantes, as quais foram relevantes para confirmar a competência técnicas e a experiências dos especialistas que participaram da pesquisa. Em relação à idade dos participantes, três deles possuem entre 31 e 40 anos, dois deles possuem entre 41 e 50 anos e 1 (um) deles entre 51 e 60 anos.

A cidade e o estado em que residem é apresentado no Gráfico 1.

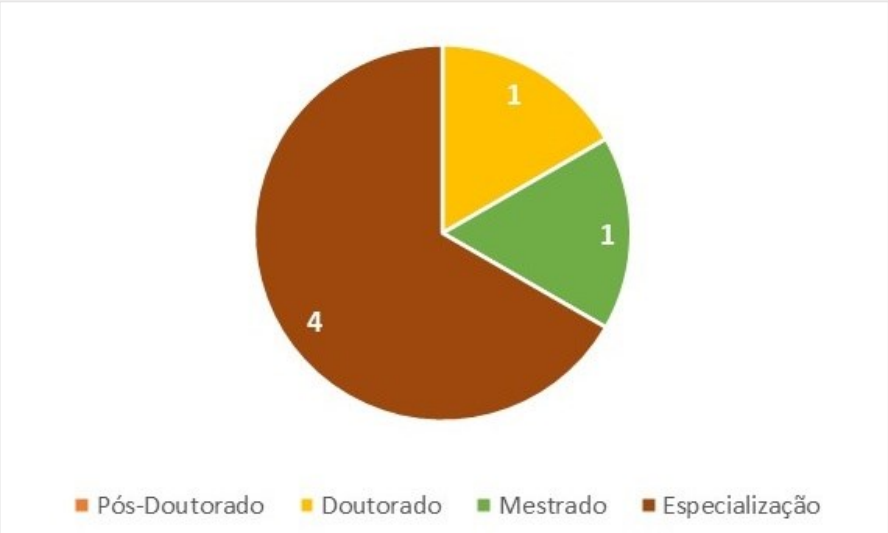
Gráfico 1 - Localidade dos participantes



Fonte: Elaborado pela autora (2022).

Em relação à formação acadêmica, a maioria dos participantes possui pós-graduação *lato sensu*, conforme apresentado no Gráfico 2.

Gráfico 2 - Formação dos especialistas



Fonte: Elaborado pela autora (2022).

Referente à função profissional que os participantes desempenham atualmente configuram um cenário multidisciplinar, visto que apresentaram as seguintes funções:

a) Participante 1: Analista de Sistemas;
b) Participante 2: Professor e empreendedor;
c) Participante 3: Coordenador setor Administrativo, Financeiro e Contábil;
d) Participante 4: CISO (Chief Information Security Officer);
e) Participante 5: Especialista em Proteção e Privacidade de Dados;
f) Participante 6: Superintendente Jurídico e Encarregado de Dados.

Os dados coletados quanto ao tempo de atuação na atual função na carreira profissional e também referente à quantidade de projetos que já participaram na área de segurança da informação e/ou privacidade de dados, apresentam um grau de maturidade quanto à experiência em suas áreas, conforme elucidado nos Gráficos 3 e 4.

Gráfico 3 - Tempo de atuação profissional

Fonte: Elaborado pela autora (2022).

Gráfico 4 - Quantidade de projetos

Fonte: Elaborado pela autora (2022).

A terceira etapa da avaliação teve como objetivo verificar se a percepção dos especialistas participantes está alinhada com os objetivos do COM.PRIVACY, tanto no que se refere ao seu funcionamento quanto à sua contribuição para a área.

Com relação ao escopo do modelo, no qual se procurou verificar se o universo/delimitação do campo de conhecimento é suficiente para cumprir o seu propósito, todos os participantes concordaram com essa afirmação. O Quadro 37 apresenta as observações inseridas pelos mesmos nessa questão.

Quadro 37 - Observações sobre a questão 1 da avaliação do COM.PRIVACY

Participante	Observações
Especialista 2	O1 - "O modelo compreende desde o levantamento de requisitos, baseados em normas ISO e regulações setoriais, até o apontamento de onde é possível encontrar as evidências relacionadas com as etapas de tratamento de dados".
Especialista 3	O2 - "O modelo ajuda a organizar as ideias e visualizar as evidências que temos para proteção de dados de forma bem clara e útil para a organização. Durante as entrevistas sobre o processo mapeado também muitas dúvidas que tinha sobre essas evidências foram esclarecidas".
Especialista 4	O3 - "O modelo não só abrange como abre espaço para estendê-lo, na medida em que direciona e abre espaço para o acolhimento de outros dispositivos pertinentes".
Especialista 5	O4 - "Ao basear-se na ISO/IEC 29100, o modelo apresentou coesão com o seu propósito e margem para englobar os requisitos necessários".

Fonte: Elaborado pela autora (2022).

Em análise aos comentários inseridos, verificou-se destaque na atuação dos princípios norteadores oriundos da abordagem *Privacy by Design* os quais apresentam:

a) Segurança e privacidade de ponta a ponta, atuante em todas as operações de tratamento dos dados;
b) Segurança e Privacidade da concepção do produto/serviço/processo à comprovação de uma alegação.

Observou-se que a materialização desses princípios foi percebida pelos especialistas 2, 3 e 4. Já o especialista 5 apresentou uma consolidação referente à limitação do escopo deste trabalho, visto que sua estrutura basilar é uma normativa de referência e as demais fontes regulatórias devem ser utilizadas em complemento a ela, quando aplicável.

Ao avaliar a profundidade e precisão do modelo, procurou-se identificar na percepção dos participantes quantos especialistas concordariam com a afirmação: O nível de detalhamento do modelo (etapas, atividades e tarefas) é adequado e suficiente para o gerenciamento de evidências. Ou seja, o nível de aprofundamento e decomposição do modelo é suficiente e adequado ao seu propósito.

Todos os participantes concordaram com essa afirmação e as respostas foram complementadas com as observações apresentadas no Quadro 38.

Quadro 38 - Observações sobre a questão 2 da avaliação do COM.PRIVACY

Participante	Observações
Especialista 2	O1 - "O modelo possui granularidade adequada para a gestão de evidências. Neste ponto, eu destaco a possibilidade de gestão de evidências de cada uma das etapas de tratamento de dados. Além disso, o modelo suporta a gestão de evidências considerando o arcabouço normativo relacionado com cada processo corporativo. O modelo também abrange diversos tipos de evidências, flexibilidade necessária para a aplicação no mundo real. Por fim, o uso do padrão GSN possibilita ótima visibilidade sobre as evidências associadas a cada item da matriz, além de oferecer subsídios para a organização identificar quais itens não possuem evidências relacionadas."
Especialista 6	O2 - "Observação à oportunidade de estabelecimento de regras de recorrência da aplicação do modelo/revisão dos artefatos, principalmente em relação àqueles que não possuem prazo de validade."

Fonte: Elaborado pela autora (2022).

O especialista 2 consolida os objetivos do modelo e menciona a facilidade de se obter a visão da situação representada no diagrama GSN. Vale ressaltar que, além de observar o que o cenário possui com a identificação das evidências, o modelo possibilita também a identificação

das lacunas dos itens que ainda não estão implantados ou implantados parcialmente. Mesmo não sendo seu objetivo principal, na medida em que não são localizadas as evidências de implementação, as lacunas são identificadas e podem nortear as próximas atividades de implementação.

Com relação à observação do especialista 6, ao compreender seu apontamento, observa-se que a preocupação do mesmo está relacionada com a periodicidade de aplicação do modelo visto que nos casos de evidências do tipo dinâmica, estas não possuem prazo de validade e podem se perder com o tempo. Esta sugestão foi acatada e está disposta na subseção 5.2.3 Camada Gestão das Evidências, a qual prevê a aplicação anualmente e nos casos dos requisitos e pré-requisitos que ainda não tenham sido implementados, logo após sua implementação.

Sobre a generalidade do COM.PRIVACY, o questionamento teve como objetivo verificar se na opinião dos participantes o modelo possibilita a sua aplicação em diferentes setores e negócios. Ou seja, a amplitude de aplicação do modelo oferece possibilidade de aplicá-lo em cenários distintos com diferentes características. O resultado apresentou que todos os especialistas participantes concordam com essa afirmação e as observações sobre este item são apresentadas do Quadro 39.

Quadro 39 - Observações sobre a questão 3 da avaliação do COM.PRIVACY

Participante	Observações
Especialista 2	O1 - "A adaptabilidade do sistema às diversas normatizações setoriais e o uso das etapas de tratamento de dados oferecem a flexibilidade necessária para que o modelo seja utilizado por diferentes setores."
Especialista 5	O2 - "A opção pela normativa em prevalência à legislação cumpre este propósito, sem ser excludente, na medida que abre espaço para qualquer outra regulamentação pertinente ao caso em análise."

Fonte: Elaborado pela autora (2022).

Assim como na questão 1 que trata sobre o escopo, as observações obtidas na questão 3 reafirmam a limitação do escopo deste trabalho, sendo ele baseado em uma normativa de referência aplicável a qualquer tipo de negócio e as demais fontes regulatórias utilizadas de forma complementar e de acordo com o cenário de aplicação do COM.PRIVACY tornando-o adaptável a diferentes cenários.

Referente à questão 4, a qual verifica a percepção dos participantes em relação à robustez e completeza do modelo, também todos os participantes concordaram com a afirmação exposta que objetivou verificar se o modelo apresenta componentes suficientes, possuindo assim capacidade de suportar e conter todos os elementos necessários para cumprir

eficientemente o seu propósito.

Para esta questão foram feitas as observações apresentadas no Quadro 40.

Quadro 40 - Observações sobre a questão 4 da avaliação do COM.PRIVACY

Participante	Observações
Especialista 2	O1 - "Na minha percepção, a divisão do modelo em três camadas, assim como os componentes de cada camada, é adequada para realizar uma gestão de evidências. Além disso, o modelo oferece uma base para que novos componentes sejam agregados, se necessário. Acredito que eventuais componentes possam ser adicionados, a partir da implantação do modelo em organizações de grande porte."
Especialista 6	O2 - "Observação à oportunidade de elaboração de um catálogo de artefatos, de forma a dar mais aderência ao modelo, evitando análises subjetivas das evidências apresentadas."

Fonte: Elaborado pela autora (2022).

Com relação à observação do especialista 2, percebe-se que a segmentação do modelo em camadas permitiu a percepção que o mesmo seja aplicado em empresas de pequeno e grande porte e que a aplicação deve ser realizada por processo, sistema ou departamento de forma granular. Quanto à observação do especialista 6, em conversa com o mesmo, observou-se que essa sugestão trata do uso de um catálogo de "possíveis artefatos" que possam ser utilizadas como evidência para cada pré-requisito apresentado. O catálogo pode ser utilizado como instrumento nas entrevistas para apoiar na identificação das evidências. Considerando que este catálogo, para que seja genérico o suficiente para ser aplicado, poderá ser gerado após a aplicação do modelo em diferentes contextos. Essa sugestão foi acatada como sugestão para trabalhos futuros, apresentada na subseção 7.1 desta tese.

Ao observar a percepção dos especialistas participantes em relação à clareza do modelo para verificar se o modelo é facilmente entendido e fácil de ser aplicado, todos concordaram com essa afirmação. A questão foi complementada com as observações apresentadas no Quadro 41.

Quadro 41 - Observações sobre a questão 5 da avaliação do COM.PRIVACY

Participante	Observações
Especialista 2	O1 - "Certamente, o modelo é de fácil compreensão. Já em relação a sua aplicação, eu penso que dependerá do porte da empresa e, consequentemente, do nível de processo existentes. Outro ponto que impactará na facilidade de aplicação é a maturidade corporativa, pois se a empresa não tiver realizado o mapeamento dos processos previamente, ela necessitará fazê-lo para aplicar o

	modelo. Por fim, penso que a facilidade na gestão do modelo também dependerá da organização, pois é necessário que diversas áreas corporativas estejam muito bem alinhadas com o responsável pelo modelo para que o mesmo permaneça atualizado.”
Especialista 5	O2 - “A possibilidade de realizar a entrega em diferentes formatos facilita muito o entendimento por parte de quem recebe os resultados, e a aplicação do modelo também é bastante facilitada na medida em que apresenta diversos mecanismos de apoio ao profissional.”

Fonte: Elaborado pela autora (2022).

A partir da observação do especialista 2, entende-se que a satisfação dos resultados obtidos da aplicação do modelo, depende do nível de maturidade da organização a qual se pretende aplicá-lo. Se a organização está com seus processos mapeados e os requisitos implantados, seu resultado será mais satisfatório e obtido com mais agilidade. Em organizações que estão iniciando, o processo de implementação, por exemplo, terá que reaplicar o modelo na medida em que os requisitos forem sendo implementados, o que pode dificultar a obtenção de um resultado satisfatório e finalizado.

Em relação à consistência do modelo, foi observado a concordância dos especialistas com a afirmação: “O modelo apresenta coerência nas bases estruturantes adotadas (*Privacy by Design*, ISO 29100 e operações de tratamento de dados) e em suas etapas, provendo informações consistentes para o gerenciamento de evidências de proteção e privacidade de dados”.

Para esta afirmação as respostas também foram unânimes em relação à concordância dos participantes, tendo em vista que todos concordaram com a afirmação e as respostas foram complementadas com as observações apresentadas no Quadro 42.

Quadro 42 - Observações sobre a questão 6 da avaliação do COM.PRIVACY

Participante	Observações
Especialista 2	O1 - “As três bases estruturantes para o modelo parecem adequadas para que o mesmo apresente a solidez e flexibilidade necessária para aplicação no mundo real.”
Especialista 3	O2 - “O modelo oferece, numa abordagem processual, ferramentas e métodos muito bem relacionados com as bases mais amplamente adotadas pelo mercado.”
Especialista 4	O3 - “Escopo normativo bem definido.”
Especialista 6	O4 - “Observação à necessidade de direcionamento das fontes para os normativos adjacentes, a fim de evitar a desconsideração de norma relevante, por desconhecimento do entrevistado.”

Fonte: Elaborado pela autora (2022).

Verifica-se que as os especialistas 2, 3 e 4 ratificam o objetivo deste estudo de apresentar um modelo consistente com bases estruturantes consolidadas de forma a tornar o COM.PRIVACY sólido e estável. No que se refere à observação do especialista 6, apresentada em conversa com o participante, identificou-se a preocupação de que alguma fonte regulatória adjacente importante não fosse identificada pelo entrevistado, deixando de fora itens relevantes para o processo de evidência. Dessa forma, a sugestão foi acatada e incluída na subseção 5.2.1 Módulo Requisitos de Fontes Regulatórias Adjacentes, a qual recomenda que entidades de classe referentes ao cenário de aplicação do modelo sejam consultadas, além do departamento jurídico e demais departamentos internos da empresa.

Na última questão da avaliação, foi verificada a percepção dos especialistas participantes em relação à contribuição/recomendação a qual buscou obter o nível de concordância com seguinte questão: Considerando as opções de modelos e métodos existentes, recomendo a adoção do modelo de gerenciamento de evidências apresentado, pois o mesmo apresenta contribuição na validação de requisitos e alegações de proteção e privacidade de dados. Para esta questão também todos os participantes foram favoráveis e as respostas foram complementadas com as observações apresentadas no Quadro 43.

Quadro 43 - Observações sobre a questão 7 da avaliação do COM.PRIVACY

Participante	Observações
Especialista 2	O1 - "Eu acredito que a estrutura proposta no modelo apresentado agrega valor às áreas de segurança e privacidade. Além disso, penso que a elaboração de um modelo sistematizado para gestão de evidências oferece grande contribuição, pois eu não possuo conhecimento de outros *frameworks* para apoiar esta atividade."
Especialista 4	O2 - "Fiquei realmente muito interessado. Pretendo desdobrar internamente na companhia."
Especialista 5	O3 - "O caráter modular e receptivo a diferentes artefatos para gerenciamento de evidências do modelo, favorece a adoção do mercado corporativo à sistemática apresentada pela pesquisadora."

Fonte: Elaborado pela autora (2022).

Analisada a concordância dos especialistas participantes com a afirmação de contribuição e indicação do COM.PRIVACY, juntamente com as observações obtidas na questão 7, conclui-se que o modelo atende seu propósito.

Vale ressaltar que em todas as apresentações com os especialistas procurou-se reforçar sobre a importância do preenchimento do campo observações, e que as sugestões eram muito bem-vindas considerando que este é o momento destinado a obter sob a visão dos especialistas, as sugestões de melhorias identificadas. Durante a apresentação algumas dúvidas de

entendimento sobre o funcionamento do COM.PRIVACY foram sendo sanadas e foram apresentados os itens que deveriam ser preenchidos no fechamento da avaliação.

Ressalta-se também que todos os especialistas que participaram da avaliação estavam motivados e interessados em contribuir com o trabalho. Durante a apresentação houve momentos de discussões sobre os conteúdos apresentados e as dúvidas que surgiram foram esclarecidas.

A avaliação foi preenchida pelos especialistas no momento mais propício para os mesmos, sem a presença desta pesquisadora, para que eles pudessem dispor de todas as suas percepções e sugestões sem nenhuma interferência.

As sugestões apontadas pelos participantes foram pertinentes, acatadas, e incluídas no modelo. Fizeram parte das sugestões apresentadas: a definição da periodicidade de aplicação do modelo, a consulta a entidades de classe, departamento jurídico e demais áreas da empresa para a identificação de fontes regulatórias adjacentes e o desenvolvimento de um catálogo de evidências para apoiar na identificação das evidências. As duas primeiras sugestões foram inseridas no modelo e a última incluída na seção de trabalhos futuros.

Diante do exposto, conclui-se que a avaliação realizada pelos especialistas foi considerada satisfatória e atingiu os objetivos definidos. Com ela pode-se observar a percepção dos especialistas quanto ao: escopo, profundidade e precisão, generalidade, robustez e completeza, clareza, consistência do modelo, bem como quais as contribuições/recomendações foram sugeridas para o modelo.

Considerando o perfil, o envolvimento dos participantes e os resultados obtidos constata-se que os propósitos do COM. PRIVACY estão alinhados com a percepção dos especialistas, e que o modelo pode contribuir com o gerenciamento de evidências de proteção e privacidade de dados. O COM.PRIVACY auxilia na validação de requisitos e controles relacionados à proteção e privacidade de dados proporcionando transparência para organizações e titulares, orquestrado por normativas e fontes regulatórias.

7 CONCLUSÕES E TRABALHOS FUTUROS

Esta tese apresentou o COM.PRIVACY, um modelo para auxiliar na validação de requisitos e controles relacionados à proteção e privacidade de dados com uma abordagem em evidências para demonstrar conformidade com os requisitos de "Responsabilização" e "Conformidade com a Privacidade" previsto na normativa de referência ISO 29100.

Para esta pesquisa foram definidos os seguintes objetivos específicos: a) identificar os componentes que constituirão o modelo, estabelecendo os elementos essenciais e a estrutura; b) elaborar o modelo para gerenciar evidências de proteção e privacidade de dados e o método de aplicação, empregando os componentes e a abordagem definida; c) aplicar o modelo identificando as melhorias a serem ajustadas; e d) validar o modelo, submetendo à apreciação de especialistas.

Para o alcance do objetivo específico "a" — identificar os componentes que constituirão o modelo, estabelecendo os elementos essenciais e a estrutura — foram analisados alguns trabalhos apresentando na literatura que apresentavam a abordagem de casos de garantia com GSN em diferentes cenários. Os estudos mostraram que é possível adaptar o GSN, porém a base dos diagramas são os requisitos, ou seja, as metas que se deseja alcançar. Com isso, apresentou-se a necessidade de extrair da fonte de referência, neste caso da ISO 29100, as metas a serem alcançadas.

As normas de referência ISO/IEC 29100, ISO/IEC 29101 e ISO/IEC 27701 e as Leis GDPR e LGPD também foram estudadas e com isso, adotou-se uma abordagem completa em relação às operações de tratamento dos dados. O conceito *Privacy by Design,* seus princípios e objetivo também foram observados nesses estudos como relevantes para embasar o propósito do modelo. Com essas análises foi possível identificar os componentes e estabelecer os elementos essenciais do COM.PRIVACY, sendo eles: as bases estruturantes e a estruturação do modelo, constituída pela normativa ISO/IEC 29100 que compõe os requisitos e pré-requisitos, o conceito de *Privacy by Design* que fundamenta o propósito do modelo, os instrumentos de apoio na coleta das evidências e o diagrama e as visões para representar as evidências identificadas.

Buscando alcançar o objetivo "b" — elaborar o modelo para gerenciar evidências de proteção e privacidade de dados e o método de aplicação, empregando os componentes e a abordagem definida —, e considerando os elementos essenciais e a estrutura estabelecida na etapa anterior, o modelo foi elaborado segmentado em três camadas. Na camada um, os requisitos e pré-requisitos devem ser extraídos da normativa de referência a qual se pretende

alcançar. Na camada dois, as evidências devem ser identificadas utilizando os instrumentos de apoio: abordagem em perspectivas e matriz que relaciona os requisitos com as operações de tratamento dos dados e na camada três são desenvolvidos o diagrama GSN, lista de artefatos, mapa de evidências e visão em malha.

Para atingir o objetivo "c" — aplicar o modelo identificando as melhorias a serem ajustadas —, o COM.PRIVACY foi aplicado na organização CASACARESC. Durante a sua aplicação observou-se uma melhoria a ser realizada nos registros das evidências. Esta melhoria refere-se aos registros previstos das abordagens por perspectivas, os quais não eram relevantes e foram imediatamente alterados. Nenhum outro ponto de ajuste foi observado durante a experimentação do modelo e a aplicação do COM.PRIVACY seguiu com sucesso.

Para o alcance do objetivo "d" — validar o modelo, submetendo à apreciação de especialistas — os objetivos da avaliação foram definidos e com isso, o instrumento de avaliação foi elaborado. Participaram da avaliação 6 especialistas os quais forneceram sua opinião em relação ao escopo, profundidade e precisão, generalidade, robustez e completeza, clareza, consistência e contribuição. Considerando a opinião dos especialistas, observa-se que o COM.PRIVACY contribui e pode auxiliar na validação de requisitos e controles relacionados com a proteção e privacidade de dados. Algumas sugestões foram apontadas pelos participantes e as consideradas pertinentes e possíveis de serem implementadas neste estágio do modelo foram acatadas, porém nenhum ajuste significativo fez-se necessário.

No que se refere à questão definida para nortear esta tese — Como sistematizar o gerenciamento de evidências de conformidade de proteção e privacidade de dados em um modelo que apoie os requisitos de "Responsabilização" e "Conformidade com a Privacidade" previstos nas normativas? — esta é respondida, ao considerar a obrigatoriedade de proteção e privacidade de dados por força de leis sancionadas em âmbito mundial e o desafio de estar em conformidade com normativas de referência e ser capaz de demonstrá-la. O COM.PRIVACY sistematiza e apoia na comprovação de conformidade dos requisitos "Responsabilização" e "Conformidade com a Privacidade", demonstrando como e em quais evidências os requisitos são validados.

Ainda, concernente às hipóteses definidas para esta pesquisa, sendo elas – H1: As abordagens utilizadas para o gerenciamento de evidência em casos de garantia de padrões de segurança aplicados em sistemas críticos podem ser ajustadas para o contexto de proteção e privacidade de dados e contribuir também com essa temática; e – H2: Considerando que, além de implementar controle, mecanismos e processos de proteção e privacidade de dados orientados pelos requisitos das normativas de referência é necessário ser capaz de comprová-

los, é possível afirmar que um modelo para gerenciar as evidências de proteção e privacidade de dados pode contribuir para demonstrar a conformidade com as normativas. Com o desenvolvimento do COM.PRIVACY conclui-se que as mesmas formam confirmadas, visto que o modelo foi proposto com a uso de casos de garantia e contribui na comprovação de conformidade com as normativas para a tutela de um direito fundamental do cidadão: a proteção e privacidade de seus dados pessoais.

Ademais, espera-se que esse estudo possa contribuir com:

– a comunidade acadêmico-científica, visto que apresentou uma análise de abordagens propostas na literatura e a proposição de um modelo com base em pesquisas realizadas anteriormente, permitindo que pesquisadores o utilizem para a realização de testes e ajustes em suas pesquisas bem como deem continuidade aos estudos aqui propostos;

– os cidadãos, uma vez que propõem uma abordagem que pode ser utilizada na validação e comprovação de seus direitos de privacidade como titulares dos dados;

– as organizações, pois o modelo proposto pode apoiá-las na adequação e aderência à normativas de proteção e privacidade de dados e ser adotado como referência para o gerenciamento de evidências;

– os órgãos reguladores/certificadores e auditores por proporcionar a padronização nas comprovações sobre o tratamento de dados pessoais;

– os profissionais da área de proteção e privacidade de dados, quanto à oportunidade de adotar um modelo que objetiva garantir a qualidade e aceitação das evidências; e

– os profissionais da área da Ciência da Informação e áreas relacionadas, como uma oportunidade de atuação profissional na área de proteção e privacidade de dados.

Como limitação desta pesquisa, identifica-se a aplicação do modelo em apenas um processo da CASACARESC. Isso se deu devido ao escopo definido para este estudo, bem como, ao tempo que se teve para sua aplicação. Dessa forma, justifica-se que não foi possível aplicá-lo em outros processos e em empresas de outros segmentos de atuação. Além disso, a avaliação do modelo realizada por seis especialista também é considerada uma limitação da pesquisa, ao considerar que uma quantidade maior de avaliações poderia resultar em novas sugestões. Porém, devido ao alto nível de experiência dos especialistas selecionados, ao perfil multidisciplinar dos mesmos e sua atuação em empresa de segmentos distintos, justifica-se essa quantidade de especialistas participantes da avaliação do COM.PRIVACY.

Referente as limitações do modelo apresentado, identifica-se a ausência de abordagens que contemplem padrões para avaliação da pertinência e adequação das evidências identificadas. O escopo do COM.PRIVACY limita-se a identificar, registrar, visualizar e

localizar os artefatos utilizados para comprovar conformidade com as normativas de proteção e privacidade de dados e não aborda essa temática. Ademais, o COM.PRIVACY apresenta modelos de formulários digitais, porém não automatizados a serem adotados para os registros das evidências identificadas. E os diagramas, listas e mapas de apresentação são desenvolvidos manualmente, de acordo com as informações registradas nos formulários. Desta forma, outra limitação do modelo é a ausência de automação dos registros de forma a facilitar a geração dos artefatos e a localização das evidências de forma automatizada e interativa.

E por fim, ressalta-se que o COM.PRIVACY foi aplicado em uma organização que já estava com o projeto de implantação dos requisitos de proteção e privacidade em andamento e este fato contribuiu para a demonstração dos resultados apresentados aqui, porém, o mesmo também pode ser aplicado em cenários que estejam em estágios iniciais de implantação, pois não apresentará perdas de resultado e apoiará também na identificação dos itens de implementação faltantes.

7.1 TRABALHOS FUTUROS

Entende-se que esta investigação inicia uma discussão sobre mecanismos para auxiliar na validação de requisitos e controles relacionados à proteção e privacidade de dados com abordagem em evidências.

Dessa forma, sugere-se que uma das propostas de trabalhos futuros envolvam modelos e metodologias que possam ser utilizadas na avaliação da qualidade e pertinência das evidências apresentadas. Este trabalho procurou identificá-las e apresentá-las de forma sistemática. Entende-se que avaliar se as mesmas são suficientes e apropriadas para seu propósito é de extrema relevância para se obter um processo com ciclo completo.

Para contextualizar esse trabalho na área do Direito, sugere-se que pesquisas sejam desenvolvidas para que o COM.PRIVACY seja adaptado aos conceitos da teoria da prova com uma perspectiva voltada a proposta de uma estrutura de evidências probatórias.

No que se refere à continuidade do COM.PRIVACY, sugere-se como trabalhos futuros a automação completa do modelo de forma que os preenchimentos, elaboração do diagrama GSN e demais artefatos gerados por ele, assim como a localização das informações registradas e vínculos com as evidências ocorram de forma interativa em sistema.

Para a continuidade do modelo propõe-se também que o mesmo seja aplicado em diferentes contextos, com o intuito de comprovar o quesito generalidade e que com essas aplicações seja desenvolvido um catálogo de evidências para apoiar futuras aplicações.

Finalmente, em relação a estruturação do COM.PRIVACY sugere-se que novos componentes sejam adicionados ao modelo de forma a facilitar a visualização e possibilite o controle de versões e informações mais claras das fontes de extração das evidências.

7.2 ARTIGOS PUBLICADOS

Durante o período de desenvolvimento desta tese (2018–2022) foram elaborados e publicados artigos científicos relacionados aos temas que contribuíram no desenvolvimento da pesquisa. A seguir é apresentada uma listagem desses artigos.

O trabalho Freund, Fagundes e Macedo (2020) apresenta uma análise dos princípios propostos pela GDPR e em quais fases do ciclo de vida dos dados proposto por esses princípios precisam ser observadas.

- FREUND, G. P.; FAGUNDES, P. B.; MACEDO, D. D. J. An analysis of blockchain and GDPR under the data lifecycle perspective. **Mobile Networks & Applications**, 2020.

O trabalho Fagundes *et al.* (2020) apresenta os resultados de uma análise sobre os SOCs, taxonomias, tesauros e ontologias utilizados pela Ciência da Informação, a fim de verificar se os mesmos são passíveis de serem utilizados durante as atividades do processo de Engenharia de Requisitos.

- FAGUNDES, P. B., FREUND, G. P., VITAL, L. P., DE BARROS, C. M., MACEDO, D. D. J Taxonomias, ontologias e tesauros: possibilidades de contribuição para o processo de Engenharia de Requisitos. **Em Questão**, v. 26, n. 1, p. 237-254, 2020.

O trabalho Freund *et al* (2019) realiza uma análise com foco na característica veracidade em Big Data, apresentando as relações deste aspecto com os mecanismos tecnológicos de segurança da informação.

- FREUND, G. P., FAGUNDES, P. B., MACEDO, D. D. J., DUTRA, M. L. Mecanismos tecnológicos de segurança da informação no tratamento da veracidade dos dados em ambientes Big Data. **Perspectivas em Ciência da Informação**, v. 24, p. 124-142, 2019.

O trabalho Freund, Sembay e Macedo (2019) analisa e identifica os aspectos interdisciplinares existentes entre os tipos, níveis e benefícios da proveniência de dados com as propriedades de segurança da informação, contribuindo para o debate das relações no âmbito da Ciência da Informação.

- FREUND, G. P.; SEMBAY, M. J.; MACEDO, D. D. J. Proveniência de dados e segurança da informação: relações interdisciplinares no domínio da ciência da informação. **Revista Ibero-Americana de Ciência da Informação**, v. 12, n. 3, p. 807-825, 2019.

O trabalho Freund, Fagundes e Macedo (2017) apresenta o conjunto de requisitos de segurança da informação prescritos na norma ISO 27017:2016, para atender as demandas de segurança específicas oriundas da utilização de serviços em nuvem, destinados aos provedores dos serviços.

- FREUND, G. P.; FAGUNDES, P. B.; MACEDO, D. D. J. Requisitos para análise de segurança da informação em provedores de serviços em nuvem. **Informação & Tecnologia**, v. 4, p. 89-109, 2017.

Capítulos de livros:

- FREUND, G. P.; FAGUNDES, P. B.; MACEDO, D. D. J. Identification of the relationships between the stages of the data lifecycle and the principles of the brazilian general data protection act. *In*: MUGNAINI, R. (org.). **Data and Information in Online Environments**. 1. ed. Springer International Publishing, 2020. v. 319. p. 79-88.

- FREUND, G. P.; MACEDO, D. D. J. Comportamento organizacional e segurança da informação: uma análise das correlações. *In*: **Gestão do capital humano em organizações empreendedoras**. Pandion, 2020. p. 135-162.

REFERÊNCIAS

ABDULLAH, N. S.; SADIQ, S.; INDULSKA, M. **Emerging challenges in information systems research for regulatory compliance management**. *In*: INTERNATIONAL CONFERENCE ON ADVANCED INFORMATION SYSTEMS ENGINEERING, 22., Scopus, Tunisia, Hammamet, 2010. p. 251- 265. Disponível em: https://link.springer.com/chapter/10.1007/978-3-642-13094-6_21. Acesso em: 10 fev. 2021.

ALVES, R. C. V. *et al.* Ciência da Informação, Ciência da Computação e Recuperação da Informação: algumas considerações sobre os métodos e tecnologias da informação utilizados ao longo do tempo. **Revista Eletrônica Informação e Cognição**, v. 6, n. 1, p. 28-40, 2007. Disponível em: https://revistas.marilia.unesp.br/index.php/reic/article/view/746. Acesso em: 05 fev. 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). ABNT NBR ISO/IEC 27701 – 2019 – Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes. 2019, 82 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). ABNT NBR ISO/IEC 29100: Tecnologia da informação — técnicas de segurança — estrutura de privacidade. Rio de Janeiro, 2020.

ASSURANCE CASE WORKING GROUP *et al.* **Goal structuring notation community standard (version 2).** 2018. Disponível em: https://scsc.uk/scsc-141B. Acesso em: 05 mar. 2021.

ALDEN, K. *et al.* Using argument notation to engineer biological simulations with increased confidence. **Journal of the Royal Society Interface**, v. 12, n. 104, p. 20141059, 2015. Disponívem em: https://royalsocietypublishing.org/doi/full/10.1098/rsif.2014.1059. Acesso em: 06.fev.2021.

ATHE, P.; DINH, N. A framework for assessment of predictive capability maturity and its application in nuclear thermal hydraulics. **Nuclear Engineering and Design**, v. 354, p. 110201, 2019. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0029549319302109. Acesso em: 16.jun.2021.

BAASE, S. **A gift of fire**: Social, legal, and ethical issues for computing and the Internet. Upper Saddle River, NJ: Pearson Prentice Hall, 2008.

BARBOSA, P. Y. S. *et al.* **Privacy by evidence: a software development methodology to provide privacy assurance**. 2018. 148 f. Tese (doutorado em Ciência da Computação) – Universidade Federal de Campina Grande, Centro de Engenharia Elétrica e Informática, Campina Grande, Paraíba, 2018. Disponível em: http://dspace.sti.ufcg.edu.br:8080/jspui/handle/riufcg/1613. Acesso em: 05 mar. 2021.

BLOOMFIELD, R. *et al.* **Using an assurance case framework to develop security strategy and policies**. *In*: INTERNATIONAL CONFERENCE ON COMPUTER SAFETY, RELIABILITY, AND SECURITY, Springer, Cham, 2017. p. 27-38. Disponível em:

https://link.springer.com/chapter/10.1007/978-3-319-66284-8_3. Acesso em: 03 mar. 2021.

BLOOMFIELD, R.; NETKACHOVA, K.; STROUD, R. **Security-informed safety**: if it's not secure, it's not safe. *In*: INTERNATIONAL WORKSHOP ON SOFTWARE ENGINEERING FOR RESILIENT SYSTEMS. Springer, Berlin, Heidelberg, 2013. p. 17-32. Disponível em: https://link.springer.com/chapter/10.1007/978-3-642-40894-6_2. Acesso em: 20 mar.2021.

BORKO, H. Information Science: what is it? **American Documentation**, v. 19, n. 1, p. 3-5, 1968. Disponível em: https://edisciplinas.usp.br/pluginfile.php/2532327/mod_resource/content/1/Oque%C3%A9CI.pdf. Acesso em: 10 fev. 2021.

BRAMAN, S. **Change of state**: Information, policy, and power. Mit Press, 2009.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 mar. 2021.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 23/03/2022

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 25 abr. 2020.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 25 abr. 2020.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 25 abr. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 jan. 2021.

BREAUX, T. D.; LOTRIONTE, C. B. **Towards a privacy management framework for distributed cybersecurity in the new data ecology**. *In*: 2011 IEEE INTERNATIONAL CONFERENCE ON TECHNOLOGIES FOR HOMELAND SECURITY (HST), IEEE, 2011. p. 6-12. Disponível em: https://ieeexplore.ieee.org/abstract/document/6107840. Acesso em: 03 mar. 2021.

CAE FRAMEWORKS. **Claims, Arguments, Evidence (CAE) framework**. CAE Concepts, 2021. Disponível em: https://claimsargumentsevidence.org/notations/claims-arguments-evidence-cae/. Acesso em: 03 mar. 2021.

CAFEZEIRO, I.; COSTA, L. C. da; KUBRUSLY, R. da S. Ciência da Computação, Ciência da Informação, Sistemas de Informação: uma reflexão sobre o papel da informação e da interdisciplinaridade na configuração das tecnologias e das ciências. **Perspectivas em Ciência da Informação**, v. 21, n. 3, p. 111-133, 2016. Disponível em: https://www.scielo.br/scielo.php?pid=S1413-99362016000300111&script=sci_abstract&tlng=pt. Acesso em: 10 mar. 2021.

CAPURRO, R.; HJORLAND, B. O conceito de informação. **Perspectivas em Ciência da Informação**, v. 12, n. 1, p. 148-207, 2007. Disponível em: https://www.scielo.br/j/pci/a/j7936SHkZJkpHGH5ZNYQXnC/abstract/?lang=pt. Acesso em: 20 abr. 2020.

CAVOUKIAN, Ann *et al.* Privacy by design: The 7 foundational principles. **Information and privacy commissioner of Ontario**, Canada, v. 5, 2009. Disponível em: http://jpaulgibson.synology.me/ETHICS4EU-Brick-SmartPills-TeacherWebSite/SecondaryMaterial/pdfs/CavoukianETAL09.pdf. Acesso em: 05 maio 2022.

COLOMBO, L. A.; FETZ, M. Contribuições do campo ciência, tecnologia e sociedade para a disseminação do conhecimento. **Revista Sinais**, v. 21, n. 1, 2017. Disponível em: https://www.periodicos.ufes.br/sinais/article/view/17439. Acesso em: 03 fev. 2021.

CRESWELL, J. **Projeto de pesquisa**: métodos qualitativo, quantitativo e misto. 3. ed. Porto Alegre: ARTMED, 2010.

DE HERT, P.; PAPAKONSTANTINOU, V. The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. **Computer Law & Security Review**, v. 28, n. 2, p. 130-142, 2012. Disponível em: https://www.sciencedirect.com/science/article/pii/S0267364912000295?casa_token=w1-zKYguw3EAAAAA:s8M9u_qgm11dRO3obLNoE1O72Sl5utfRJyD19DHmlnXN7NXilpoAQ47YRmVCY6RPaSZ3v2jllnU. Acesso em: 01 fev. 2021.

DESLANDES, S. E. A construção do projeto de pesquisa. *In*: MINAYO, M. C. S. (org.). **Pesquisa social**: teoria, método e criatividade. 18. ed. Petrópolis: Vozes, 1994. p. 31-50.

DIRECTIVE 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data. Disponível em: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046. Acesso em: 04 ago. 2020.

DLA PIPER. **Data Protection Laws of the world**: full handbook. 17 Apr. 2021. Disponível em: https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country=all. Acesso em: 20 fev. 2021.

EUROPEAN UNION. General data protection regulation. **Official Journal of the European Union**, 2018. [Online]. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1618398943851. Acesso em: 12 dez. 2020.

FACCHINI NETO, E.; DEMOLINER, K. S. Direito à privacidade e novas tecnologias: breves considerações acerca da Proteção de Dados Pessoais no Brasil e na Europa. **Revista Internacional Consinter de Direito**, ano IV, n. VII, v. 7, 2019. Disponível em: https://revistaconsinter.com/revistas/ano-iv-numero-vii/direitos-difusos-coletivos-e-individuais-homogeneos/direito-a-privacidade-e-novas-tecnologias-breves-consideracoes-acerca-da-protecao-de-dados-pessoais-no-brasil-e-na-europa/. Acesso em: 30 mar. 2021.

FAGUNDES, P. B; MACEDO, D. D. J.; FREUND, G. P. A produção científica sobre qualidade de dados em big data: um estudo na base de dados Web of Science. **RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação**, v. 16, n. 1, p. 194-210, 2018. Disponível em: https://periodicos.sbu.unicamp.br/ojs/index.php/rdbci/article/view/8650412. Acesso em: 05 mar. 2021.

FAGUNDES, P. B., FREUND, G. P., VITAL, L. P., DE BARROS, C. M., MACEDO, D. D. J. Taxonomias, ontologias e tesauros: possibilidades de contribuição para o processo de Engenharia de Requisitos. **Em Questão**, v. 26, n. 1, p. 237-254, 2020. Disponível em: https://www.seer.ufrgs.br/EmQuestao/article/view/90347. Acesso em 01 fev. 2022

FLORES, D. A. **An authentication and auditing architecture for enhancing security on egovernment services**. *In*: 2014 FIRST INTERNATIONAL CONFERENCE ON EDEMOCRACY & EGOVERNMENT (ICEDEG), IEEE, 2014. p. 73-76. Disponível em: https://ieeexplore.ieee.org/abstract/document/6819952. Acesso em: 03 mar. 2021.

FONSECA, J. J. S. **Metodologia da pesquisa científica**. Fortaleza: UEC, 2002. Apostila.

FORMOSO, S.; FELICI, M. **Evidence-based security and privacy assurance in cloud ecosystems**. *In*: IFIP INTERNATIONAL SUMMER SCHOOL ON PRIVACY AND IDENTITY MANAGEMENT, Springer, Cham, 2016. p. 205-219. Disponível em: https://link.springer.com/chapter/10.1007/978-3-319-41763-9_14. Acesso em: 04 mar. 2022.

FRAZÃO, A. **Nova LGPD**: principais repercussões para a atividade empresarial, 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-principais-repercussoes-para-a-atividade-empresarial-29082018. Acesso em: 03 abr. 2022.

FRAZÃO, A.; TEPEDINO, G.; OLIVA, M. D. **A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. Florianópolis: Revista dos Tribunais; Thomson Reuters Brasil, 2019.

FREUND, G. P.; FAGUNDES, P. B.; MACEDO, D. D. J. **Identification of the relationships between the stages of the Data Lifecycle and the principles of the brazilian general data protection act**. *In*: INTERNATIONAL CONFERENCE ON DATA AND INFORMATION IN ONLINE. Springer, Cham, 2020. p. 79-88. Disponível em https://link.springer.com/chapter/10.1007/978-3-030-50072-6_7. Acesso em: 12 dez. 2020.

FREUND, G. P.; FAGUNDES, P. B.; MACEDO, D. D. J. Requisitos para análise de segurança da informação em provedores de serviços em nuvem. **Informação & Tecnologia**, v. 4, p. 89-109, 2017. Disponível em: https://www.researchgate.net/profile/Douglas-Macedo-2/publication/334619959_Requisitos_para_analise_de_seguranca_da_informacao_em_proved

ores_de_servicos_em_nuvem/links/5d5a99d0a6fdcc55e8173ff7/Requisitos-para-analise-de-seguranca-da-informacao-em-provedores-de-servicos-em-nuvem.pdf. Acesso em 05 mai. 2022.

FREUND, G. P., FAGUNDES, P. B., MACEDO, D. D. J., DUTRA, M. L. Mecanismos tecnológicos de segurança da informação no tratamento da veracidade dos dados em ambientes Big Data. **Perspectivas em Ciência da Informação**, v. 24, p. 124-142, 2019. Disponível em: https://www.scielo.br/j/pci/a/RC6rLmbk4Jm6sCK7RkYryng/abstract/?lang=pt. Acesso em: 03 fev.2022.

FREUND, G. P.; MACEDO, D. D. J. Comportamento organizacional e segurança da informação: uma análise das correlações. In: **Gestão do capital humano em organizações empreendedoras**. Florianópolis: Pandion, 2020. p. 135-162.

FREUND, G. P.; SEMBAY, M. J.; MACEDO, D. D. J. Data Provenance and Security of Information: interdisciplinary relations in the field of Information Science. **Revista Ibero-Americana de Ciência da Informação**, v. 12, n. 3, p. 807-825, 2019. Disponível em: https://brapci.inf.br/index.php/res/v/121996. Acesso em: 15 abr. 2020.

GALVÃO, T. F.; PEREIRA, M. G. Revisões sistemáticas da literatura: passos para sua elaboração. **Epidemiologia e Serviços de Saúde**, v. 23, n. 1, p. 183–184, 2014. Disponível em: https://www.scielosp.org/scielo.php?pid=S2237-96222014000100183&script=sci_arttext&tlng=es. Acesso em: 03 mar. 2021.

GE, X. *et al.* Introducing goal structuring notation to explain decisions in clinical practice. **Procedia Technology**, v. 5, p. 686-695, 2012. DOI: 10.1016/j.protcy.2012.09.076

GEHANI, A.; CIOCARLIE, G. F.; SHANKAR, N. **Accountable clouds**. *In*: 2013 IEEE INTERNATIONAL CONFERENCE ON TECHNOLOGIES FOR HOMELAND SECURITY (HST). IEEE, 2013. p. 403-407. Disponível em: https://ieeexplore-ieee-org.ez46.periodicos.capes.gov.br/document/6699038. Acesso em: 03 mar. 2021.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2007.

GOODGER, A. C.; CALDWELL, N. H. M.; KNOWLES, J. T. **What does the Assurance case approach deliver for critical information infrastructure protection in cybersecurity?** *In*: *IET INTERNATIONAL CONFERENCE ON SYSTEM SAFETY, INCORPORATING THE CYBER SECURITY CONFERENCE 2012*, 7., Edinburgh, 2012. p. 1-6. DOI 10.1049/cp.2012.1501. Disponível em: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6458943. Acesso em: 04 mar. 2021.

GOLDENBERG, M. **A arte de pesquisar**. Rio de Janeiro: Record, 1997.

GROBLER, C. P.; LOUWRENS, C. P. **Digital evidence management plan**. *In*: 2010 INFORMATION SECURITY FOR SOUTH AFRICA, IEEE, 2010. p. 1-6. Disponível em: https://ieeexplore.ieee.org/abstract/document/5588661?casa_token=PUIviDe_jkQAAAAA:T

XjNdKZZe5YqEf88cPts8JObANSeElPd0F6fWUImjgg-Beul-04v9lJ0uP5QzqXxodfhlqk12V8. Acesso em: 27 dez. 2020.

HEVNER, A. *et al.* Design science in information systems research. **MIS Quarterly**, v. 28, n. 1, p. 75-105, mar. 2004. Disponível em: https://www.jstor.org/stable/25148625?seq=1. Acesso em: 03 jan. 2021.

HEVNER, A.; CHATTERJEE, S. **Design Research in Information Systems**: theory and practice. [*S. l.*]: Springer Science & Business Media, 2010.

HINDE, C.; OPHOFF, J. **Privacy**: A review of publication trends. *In*: 2014 INFORMATION SECURITY FOR SOUTH AFRICA, 2014. p. 1-7. Disponível em: https://ieeexplore.ieee.org/abstract/document/6950499. Acesso em: 03 mar. 2021.

HOLVAST, J. History of Privacy. *In*: MATYÁŠ, V. *et al.* (ed.). **The future of identity in the Information Society**: Privacy and Identity 2008. IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY, Springer, Berlin, Heidelberg, v. 298, 2009. Disponível em: https://link.springer.com/chapter/10.1007/978-3-642-03315-5_2. Acesso em: 23 mai.2021.

INGE, J. R. **The safety case, its development and use in the United Kingdom**. *In*: EQUIPMENT SAFETY ASSURANCE SYMPOSIUM. 2007. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=D14CC625161E7502EA190F7F72783B38?doi=10.1.1.170.106&rep=rep1&type=pdf. Acesso em: 10 mar. 2021.

ISAAK, J.; HANNA, M. J. User data privacy: Facebook, Cambridge Analytica, and privacy protection. **Computer**, v. 51, n. 8, p. 56-59, 2018. Disponível em: https://ieeexplore.ieee.org/abstract/document/8436400. Acesso em: 10 mar. 2021.

ISO/IEC. ISO/IEC 29100. International Standard – Information Technology – Security Techniques – Privacy Framework. 2011.

ISO/IEC. ISO/IEC 29101. International Standard – Information Technology – Security Techniques – Privacy Framework. 2013.

JABEEN, F. *et al.* Trust and reputation management in healthcare systems: taxonomy, requirements and open issues. **IEEE Access**, v. 6, p. 17246-17263, 2018. Disponível em: https://ieeexplore.ieee.org/abstract/document/8308716. Acesso em: 03 mar. 2021.

KANG, K. *et al.* An interactive trust model for application market of the internet of things. **IEEE Transactions on Industrial Informatics**, v. 10, n. 2, p. 1516-1526, 2014. Disponível em: https://ieeexplore.ieee.org/abstract/document/6742593. Acesso em: 02 mar. 2021.

KINOSHITA, S.; KINOSHITA, Y. **A thought experiment on evolution of assurance cases**. *In*: INTERNATIONAL CONFERENCE ON COMPUTER SAFETY, RELIABILITY, AND SECURITY, Springer, Cham, 2017. p. 17-26. Disponível em: https://link.springer.com/chapter/10.1007/978-3-319-66284-8_2. Acesso em: 02 mar. 2021.

KITCHENHAM, B. *et al*. Systematic literature reviews in software engineering: a systematic literature review. **Information and Software Technology**, v. 51, n. 1, p. 7-15, 2009.

Disponível em: http://dx.doi.org/10.1016/j.infsof.2008.09.009. Acesso em: 10 mar. 2021.

KNECHTEL, M. R. **Metodologia da pesquisa em educação**: uma abordagem teórico-prática dialogada. Curitiba: Intersaberes, 2014.

KNIGHT, J. The importance of security cases: Proof is good, but not enough. **IEEE Security & Privacy**, v. 13, n. 4, p. 73-75, 2015. Disponível em: https://www.computer.org/csdl/magazine/sp/2015/04/msp2015040073/13rRUxNW1XO. Acesso em: 02 mar. 2021.

KOBAYASHI, N. *et al.* Evaluation of assurance case description method using ISO 27001 for Merger and Acquisition. **International Journal of Service and Knowledge Management International Institute of Applied Informatics**, v. 4, n. 1, 61-75, 2020. Disponível em: https://www.researchgate.net/publication/341998828_Evaluation_of_Assurance_Case_Description_Method_using_ISO_27001_for_Merger_and_Acquisition. Acesso em: 03 mar. 2021.

KOKALY, S. **Managing assurance cases in model based software systems**. *In*: 2017 IEEE/ACM INTERNATIONAL CONFERENCE ON SOFTWARE ENGINEERING COMPANION (ICSE-C), 39., IEEE, 2017. p. 453-456. Disponível em: https://ieeexplore-ieee-org.ez46.periodicos.capes.gov.br/document/7965382. Acesso em: 03 mar. 2021.

KOKALY, S. *et al.* **Model management for regulatory compliance**: a position paper. *In*: 2016 IEEE/ACM INTERNATIONAL WORKSHOP ON MODELING IN SOFTWARE ENGINEERING (MiSE), 8., IEEE, 2016. p. 74-80. Disponível em: https://ieeexplore.ieee.org/abstract/document/7809790. Acesso em: 03 mar. 2021.

LAHBIB, A. *et al.* **Blockchain based trust management mechanism for IoT**. *In*: 2019 IEEE WIRELESS COMMUNICATIONS AND NETWORKING CONFERENCE (WCNC), Apr 2019, Marrakech, Morocco. p. 1-8. DOI: 10.1109/WCNC.2019.8885994. Disponível em: https://ieeexplore-ieee-org.ez46.periodicos.capes.gov.br/document/8885994. Acesso em: 03 mar. 2021.

LAKATOS, E. M.; MARCONI, M. de A. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas 2003.

LENHARD, J.; FRITSCH, L.; HEROLD, S. **A literature study on privacy patterns research**. *In*: 2017 EUROMICRO CONFERENCE ON SOFTWARE ENGINEERING AND ADVANCED APPLICATIONS (SEAA), 43., IEEE, 2017. p. 194-201. Disponível em: https://ieeexplore.ieee.org/abstract/document/8051348. Acesso em: 02 mar. 2021.

LINDE, K.; WILLICH, S. N. How objective are systematic reviews? Differences between reviews on complementary medicine**. J R Soc Med**., v. 96, p. 17-22, 2003. Disponível em: https://www.ncbi.nlm.nih.gov/pubmed/12519797. Acesso em: 11 jul. 2019.

LUKACS, A. What Is Privacy? The history and definition of privacy. **Tavaszi Szél 2016 Tanulmánykötet I**, p. 256-265, Apr. 2017. Disponível em: http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf. Acesso em: 15 dez. 2020.

MARCH, S. T.; SMITH, G. F. Design and natural science research on information technology. **Decision Support Systems,** v. 15, p. 251-266, 1995. Disponível em:

https://www.sciencedirect.com/science/article/pii/0167923694000412. Acesso em: 20 dez. 2020.

MASMOUDI, F. *et al.* **Optimal evidence collection for accountability in the cloud**. *In*: 2018 IEEE INTERNATIONAL CONFERENCE ON E-BUSINESS ENGINEERING (ICEBE), 15., IEEE, 2018. p. 78-85. Disponível em: https://ieeexplore-ieee-org.ez46.periodicos.capes.gov.br/document/8592633. Acesso em: 04 mar. 2021.

MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. 1. ed. São Paulo: Saraiva, 2014.

MOHAMMED, A. A. Digital Evidence and Best Evidence Rule. **SUST Journal of Engineering and Computer Science (JECS),** v. 19, n. 2, p. 1-9, 2018. Disponível em: https://core.ac.uk/download/pdf/323246026.pdf. Acesso em: 05 jan. 2021.

NAIR, S. *et al.* Evidence management for compliance of critical systems with safety standards: A survey on the state of practice. **Information and Software Technology**, v. 60, p. 1-15, 2015. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0950584914002560. Acesso em: 14 jan. 2021.

OMG GROUP *et al.* **Structured Assurance Case Metamodel (SACM)**. Version 2.1. Object Management Group, Apr. 2020. Disponível em: https://www.omg.org/spec/SACM/2.1/PDF. Acesso em: 25 fev. 2021.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 2013**. Disponível em: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Acesso em: 10 ago. 2020.

PANTAZOPOULOS, P. *et al.* **Towards a security assurance framework for connected vehicles**. *In*: 2018 IEEE INTERNATIONAL SYMPOSIUM ON "A WORLD OF WIRELESS, MOBILE AND MULTIMEDIA NETWORKS (WoWMoM)", 19., IEEE, 2018. p. 01-06. Disponível em: https://ieeexplore.ieee.org/abstract/document/8449811. Acesso em: 02 mar. 2021.

PEFFERS, K. *et al.* A Design Science Research Methodology for Information Systems Research. **Journal of Management Information Systems**, v. 24, n. 03, p. 4201-4204, 2007. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.535.7773&rep=rep1&type=pdf. Acesso em: 18 nov. 2019.

PETTICREW, M.; ROBERTS, H. **Systematic reviews in the social sciences**. Malden, MA: Blackwell Publishing, 2006.

PINHEIRO, P. P. **Proteção de Dados Pessoais**: Comentários à Lei n. 13.709/2018-LGPD. São Paulo: Saraiva Educação S.A., 2020.

PINHEIRO, J.; FARIAS, T.; ABE LIMA, J. Painel de especialistas e estratégia multimétodos: reflexões, exemplos, perspectivas. **Psico**, v. 44, n. 2, p. 4, 2013. Disponível em: https://revistaseletronicas.pucrs.br/index.php/revistapsico/article/view/11216. Acesso em: 20 mar. 2022.

QUEIROZ, D. G. de C.; MOURA, A. M. M. de. Ciência da Informação: história, conceitos e características. **Em Questão**, v. 21, n. 3, p. 25-42, 2015. Disponível em: https://seer.ufrgs.br/index.php/EmQuestao/article/view/57516. Acesso em: 03 jan. 2021.

RHODES, T. *et al.* Software assurance using structured assurance case models. **Journal of Research of the National Institute of Standards and Technology**, v. 115, n. 3, May/Jun. 2010. Disponível em: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4548534/. Acesso em: 06 jun.2021.

RICHARDSON, R. J. **Pesquisa social:** métodos e técnicas. 3. ed. São Paulo Atlas: 1999.

ROMANSKI, G. **Combined safety and security certification**. 2012. Disponível em: https://digital-library.theiet.org/content/conferences/10.1049/cp.2012.1511. Acesso em: 03 mar. 2021.

ROCHA, J. M.; HONORATO, M. J.; COSTA, E. Assessment of expert panels. **IEEE Latin America Transactions**, v. 14, n. 1, p. 303–308, 2016. Disponível em: https://ieeexplore.ieee.org/abstract/document/7430093. Acesso em: 05 jul.2021.

RODRÍGUEZ, A. S. M.; DEL PINO, J. C. Abordagem Ciência, Tecnologia e Sociedade (CTS): perspectivas teóricas sobre educação científica e desenvolvimento na América Latina. **Tear**: Revista de Educação, Ciência e Tecnologia, v. 6, n. 2, 2017. Disponível em: https://periodicos.ifrs.edu.br/index.php/tear/article/view/2490. Acesso em: 02 jan. 2021.

RUEBSAMEN, T.; REICH, C. **Supporting cloud accountability by collecting evidence using audit agents**. *In*: 2013 IEEE INTERNATIONAL CONFERENCE ON CLOUD COMPUTING TECHNOLOGY AND SCIENCE, 5., IEEE, 2013. p. 185-190. Disponível em: https://ieeexplore.ieee.org/abstract/document/6753796. Acesso em: 03 mar. 2021.

RUSHBY, J. The interpretation and evaluation of assurance cases. **SRI International,** Technical Report, SRI-CSL-15-01, jul. 2015. Disponível em: http://www.csl.sri.com/users/rushby/papers/sri-csl-15-1-assurance-cases.pdf. Acesso em: 27 fev. 2021.

SANTOS, A. R. **Metodologia científica**: a construção do conhecimento. Rio de Janeiro: DP&A, 1999.

SADIQ, S.; GOVERNATORI, G. Managing regulatory compliance in business processes. *In*: **Handbook on business process management 2**. Berlin, Heidelberg: Springer, 2015. p. 265-288. Disponível em: https://link.springer.com/chapter/10.1007/978-3-642-45103-4_11. Acesso em: 27 fev. 2021.

SARACEVIC, T. Ciência da informação: origem, evolução e relações. **Perspectivas em Ciência da Informação**, v. 1, n. 1, p. 41-62, 1996. Disponível em: https://periodicos.ufmg.br/index.php/pci/article/view/22308. Acesso em: 08 mar.2021.

SCHAAR, P. Privacy by design. **Identity in the Information Society**, v. 3, n. 2, p. 267-274, 2010.Disponível em: https://link.springer.com/article/10.1007/s12394-010-0055-x. Acesso em: 05 maio 2022.

SELVIANDRO, N.; HAWKINS, R.; HABLI, I. A Visual notation for the representation of assurance cases using SACM. *In*: INTERNATIONAL SYMPOSIUM ON MODEL-BASED SAFETY AND ASSESSMENT, Springer, Cham, 2020. p. 3-18. Disponível em: https://eprints.whiterose.ac.uk/165129/1/A_Visual_Notation_for_the_Representation_of_Assurance_Cases_using_SACM_2_.pdf. Acesso em: 05 mar. 2021.

SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS (SERPRO). Disponível em: https://www.serpro.gov.br/lgpd/menu/arquivos/linha-do-tempo-1/view. Acesso em: 10 fev. 2021.

SHEHABUDDEEN, N. *et al.* Representing and approaching complex management issues: Part 1-Role and definition. **Centre for Technology Management (CTM) Working Paper**, n. 2000/03, 1999. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1923155. Acesso em: 12 nov. 2020.

SILVA, E. L.; MENEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação**. 3. ed. rev. atual. Florianópolis: Laboratório de Ensino a Distância da UFSC, 2001

SIMON, H. **The Sciences of Artificial**. 3. ed. Cambridge, MA: MIT Press, 1996.

SIMMONDS, S.; COOK, S. C. **Use of the goal structuring notation to argue technical integrity**. *In*: INCOSE INTERNATIONAL SYMPOSIUM, 2017. p. 826-841.

SIRAGELDIN, A.; BAHARUDIN, B.; JUNG, L; T. **Hybrid scheme for trust management in pervasive computing**. *In*: 2012 INTERNATIONAL CONFERENCE ON INFORMATION RETRIEVAL & KNOWLEDGE MANAGEMENT, IEEE, 2012. p. 45-49. Disponível em: https://ieeexplore.ieee.org/abstract/document/6205031. Acesso em 02 mar. 2021.

SHAREEFUL, I. *et al.* Assurance of security and privacy requirements for cloud deployment models. **IEEE Transactions on Cloud Computing**, v. 6, n. 2, p. 387-400, 2018. Disponível em: https://ieeexplore-ieee-org.ez46.periodicos.capes.gov.br/document/7364243/. Acesso em: 03 mar. 2021.

SOLOVE, D. J. A Brief history of information privacy law. *In*: **Proskauer on Privacy, PLI**, 2006. Disponível em: https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications. Acesso em: 03 mar. 2021.

SPIEKERMANN, S. The challenges of privacy by design. **Communications of the ACM**, v. 55, n. 7, p. 38-40, 2012. Disponível em: https://dl.acm.org/doi/abs/10.1145/2209249.2209263?casa_token=Tb6jEo9S_fQAAAAA:8e07s7tj1Buw8PVfNJtaLwiebMEYNLHVQ1JQXzAVVc7xD1I0mbOrTRcKiV95Mb0b699dUGGGVX4. Acesso em: 04 maio 2022.

SPRIGGS, J. **GSN-the goal structuring notation**: a structured approach to presenting arguments. Springer Science & Business Media, 2012. DOI: 10.1007/978-1-4471-2312-5_13.

SKLYAR, V.; KHARCHENKO, V. **Assurance case driven design for computer systems**: graphical notations versus mathematical methods. *In*: 2016 THIRD INTERNATIONAL CONFERENCE ON MATHEMATICS AND COMPUTERS IN SCIENCES AND IN INDUSTRY (MCSI). IEEE, 2016. p. 308-312.

STARK, P. B.; WAGNER, D. Evidence-based elections. **IEEE Security & Privacy**, v. 10, n. 5, p. 33-41, 2012. Disponível em: https://ieeexplore.ieee.org/abstract/document/6203498. Acesso em: 02 mar. 2021.

TORRE, D. *et al.* **Using models to enable compliance checking against the GDPR**: an experience report. *In*: 2019 ACM/IEEE INTERNATIONAL CONFERENCE ON MODEL DRIVEN ENGINEERING LANGUAGES AND SYSTEMS (MODELS), 22. IEEE, nov. 2019. p. 1-11. Disponível em: https://ieeexplore.ieee.org/abstract/document/8906896?casa_token=ihC90jND56YAAAAA:tInlYulSAeV_GsZyO7nKyMMyxsDbBkRGAxoHK7H-TQmQ3tYj6-drNJTxQaHVgoARAmpDCkhURAM. Acesso em: 03 jan. 2021.

TRAVERSO, G. *et al.* **Evidence-based trust mechanism using clustering algorithms for distributed storage systems**. *In*: 2017 ANNUAL CONFERENCE ON PRIVACY, SECURITY AND TRUST (PST), 15., IEEE, 2017. p. 277-282. (Short Paper). Disponível em: https://ieeexplore.ieee.org/abstract/document/8476945. Acesso em: 03 mar. 2021.

TRIVINOS, A. N. S. **Introdução à pesquisa em Ciências Sociais**: a pesquisa qualitativa em Educação. São Paulo: Atlas, 1987.

UNIVERSIDADE FEDERAL DE SANTA CATARINA (UFSC). Programa de Pós-Graduação em Ciência da Informação. **Linhas de Pesquisa**: informação e tecnologia. Disponível em: https://pgcin.ufsc.br/linhas-de-pesquisa/. Acesso em: 05 fev. 2021.

VAISHNAVI, V.; KUECHLER, W; PETTER, S. **Design research in information systems**. 2004. 62 p. Disponível em: http://desrist.org/design-research-in-information-systems/. Acesso em: 10 out. 2021.

VAISHNAVI, V. K.; KUECHLER, W. **Design science research methods and patterns**. 2. ed. Boca Raton: CRC Press, 2015.

VAN AKEN, J. E. Management research as a design science: articulating the research products of mode 2 knowledge production in management. **British Journal of Management**, v. 16, n.01, p. 19-36, 2005. Disponível em: https://doi.org/10.1111/j.1467-8551.2005.00437.x. Acesso em: 18 nov. 2019.

VERGARA, S. C. **Projetos e relatório de pesquisa em administração**. 5. ed. São Paulo: Atlas, 2007.

VERGARA, S. C. **Métodos de coleta de dados no campo**. 2. ed. São Paulo: Atlas, 2012.

WARDZIŃSKI, A.; JONES, P. **Uniform model interface for assurance case integration**

with system models. *In*: INTERNATIONAL CONFERENCE ON COMPUTER SAFETY, RELIABILITY, AND SECURITY, Springer, Cham, 2017. p. 39-51. Disponível em: https://link.springer.com/chapter/10.1007/978-3-319-66284-8_4. Acesso em: 02 mar. 2021.

WARREN, S. D.; BRANDEIS, L. D. Direito à privacidade. *In*: BRECKENRIDGE, C. A. (ed.). **O direito à privacidade**. Universidade de Nebraska Press, Lincoln, 1970. p. 133-153.

WEI, R. *et al.* Model based system assurance using the structured assurance case metamodel. **Journal of Systems and Software**, v. 154, p. 211-233, 2019. Disponível em: https://www.sciencedirect.com/science/article/pii/S0164121219301062?casa_token=LsAiYCRzV1gAAAAA:L1glIBEETctZVT9OQjpJbv814TYNtaQLsydadBIGADB9k4z4rzt9guip16WcWPhdAkLfhyUamHQ Acesso em: 03 fev. 2021.

WESTIN, A. F. Social and political dimensions of privacy. **Journal of Social Issues**, v. 59, n. 2, p. 431-434, 2003. Disponível em: https://spssi.onlinelibrary.wiley.com/doi/abs/10.1111/1540-4560.00072?casa_token=Yw8eukGTVxUAAAAA:-Ma5jcOREUZfvWSSrHF4F_M-ou_hjWpS22pnPrtWa4ROMzhbLKixmyk5KBmy9buUeyu9qLXcEAT47Rw. Acesso em: 17 dez. 2020.

WIERINGA, R. Design science as nested problem solving. *In*: INTERNATIONAL CONFERENCE ON DESIGN SCIENCE RESEARCH IN INFORMATION SYSTEMS AND TECHNOLOGY, 4., ACM, 2009. **Proceedings** […]. ACM, 2009. p. 1-12. DOI: https://doi.org/10.1145/1555619.1555630

WIERINGA, R. J. **Design science methodology for information systems and software engineering**. [*S. l.*]: Springer Nature, 2014.

WIESE SCHARTUM, D. Making privacy by design operative. **International Journal of Law and Information Technology**, v. 24, n. 2, p. 151-175, 2016. Disponível em: https://academic.oup.com/ijlit/article-abstract/24/2/151/1750164?login=false. Acesso em: 06 maio 2022.

YAMAMOTO, S.; MORISAKI, S. **IT demand governance using business goal structuring notation**. *In*: INTERNATIONAL CONFERENCE ON IT CONVERGENCE AND SECURITY (ICITCS), 6., IEEE, 2016. p. 1-5. Disponível em: https://ieeexplore.ieee.org/abstract/document/7740346. Acesso em: 22 mar. 2022.

YAN, F. **Assurance case notations**: safer autonomous systems, 2020. Disponível em: https://etn-sas.eu/2020/06/26/assurance-case-notations/. Acesso em: 03 fev. 2021.

YIN, R. K. **Estudo de caso**: planejamento e métodos. 3. ed. Porto Alegre: Bookman, 2005.

ZHOU, J. *et al.* Secure and privacy preserving protocol for cloud-based vehicular DTNs. **IEEE Transactions on Information Forensics and Security**, v. 10, n. 6, p. 1299-1314, 2015. Disponível em: https://ieeexplore.ieee.org/abstract/document/7050342. Acesso em: 03 mar. 2021.

ZUCA, S. Audit evidence: necessity to qualify a pertinent opinion. **Procedia Economics and Finance**, v. 20, p. 700-704, 2015. Disponível em:

https://www.sciencedirect.com/science/article/pii/S2212567115001264?via%3Dihub. Acesso em: 03 jan. 2021.

APÊNDICE A – PARECER SUBSTANCIADO DO CEP – ESPECIALISTAS E AUDITOR

UNIVERSIDADE FEDERAL DE SANTA CATARINA - UFSC

PARECER CONSUBSTANCIADO DO CEP

DADOS DO PROJETO DE PESQUISA

Título da Pesquisa: PROPOSTA DE UM MODELO PARA ADEQUAÇÃO AOS REQUISITOS DE PROTEÇÃO E PRIVACIDADE DE DADOS

Pesquisador: DOUGLAS DYLLON JERONIMO DE MACEDO

Área Temática:

Versão: 2

CAAE: 44022921.5.0000.0121

Instituição Proponente: Universidade Federal de Santa Catarina

Patrocinador Principal: Universidade Federal de Santa Catarina

DADOS DO PARECER

Número do Parecer: 4.704.149

Apresentação do Projeto:

Segundo os pesquisadores: O universo digital proporcionou às organizações privadas e públicas, o uso massivo de dados pessoais e informações corporativas e com isso novos desafios surgiram quanto a proteção e privacidade de dados e legislações para tratar o tema foram adotadas em âmbito mundial. Diante do desafio de implementar os requisitos das legislações, observa-se que é necessário além de implementá-los, ser capaz de demonstrá-los adotando processos sistematizados que comprovem como e em quais evidências estes requisitos são validados. O objetivo desta tese é a proposição de um modelo de referência para gerenciar evidências probatórias de proteção e privacidade dos dados para demonstrar diligência e conformidade com as leis. Para alcançar seus objetivos, será realizada uma pesquisa aplicada e quanto à abordagem do problema, este estudo utilizará métodos mistos - quantitativo e qualitativo, com predominância na abordagem qualitativa. A natureza do objetivo é exploratória e descritiva por ter como parte do escopo proporcionar mais familiaridade com o problema e torná-lo mais explícito, descrevendo princípios, casos e abordagens relacionadas ao gerenciamento de evidências e proteção e privacidade de dados. Quanto aos procedimentos técnicos, esta pesquisa é classificada como bibliográfica, com survey e experimental. A pesquisa bibliográfica está presente na construção da revisão de literatura, bem como auxiliará nas análises e no desenvolvimento do modelo a ser proposto. A pesquisa com survey será aplicada em profissionais responsáveis na definição e na avaliação de evidências, com o objetivo de obter maior compreensão das práticas

Endereço: Universidade Federal de Santa Catarina, Prédio Reitoria II, R: Desembargador Vitor Lima, nº 222, sala 401
Bairro: Trindade **CEP:** 88.040-400
UF: SC **Município:** FLORIANOPOLIS
Telefone: (48)3721-6094 **E-mail:** cep.propesq@contato.ufsc.br

adotadas e desafios percebidos por estes para utilizar as respostas como contribuição para o modelo a ser proposto. Na etapa de validação do modelo será adotada a pesquisa experimental com a aplicação do modelo em um cenário real pela pesquisadora, que possibilitará a observação e identificação de melhorias durante sua utilização, além da submissão de um questionário a especialistas para avaliarem a adequação do modelo. Como método de pesquisa este trabalho utilizará o Design Science Research – DSR. O principal resultado esperado desta pesquisa é a proposição do modelo para gerenciamento de evidências composto por componentes e princípios de proteção e privacidade de dados que apoiem em todo o ciclo de vida das evidências probatórias e que este seja adotado como referência tanto na atividade de adequação e implementação das legislações e normativas como no processo de aferição e verificação de conformidade com as mesmas.

Objetivo da Pesquisa:

Objetivo Primário:

O objetivo geral desta pesquisa consiste em propor um modelo de referência para gerenciar evidências probatórias de proteção e privacidade dos dados para demonstrar diligência e conformidade com as leis.

Objetivo Secundário:

a) Identificar os componentes para constituir o modelo, estabelecendo os artefatos essenciais de evidências e a estrutura do modelo.

b)Identificar o processo a ser adotado para o gerenciamento das evidências, avaliando e ajustando as abordagens adotadas em casos de garantia de padrões de segurança em sistemas.

c)Elaborar o modelo empregando os componentes e o processo identificados, descrevendo os controles e estratégias recomendadas.

d)Estabelecer as orientações de implantação e uso do modelo, descrevendo a forma de aplicação do modelo.

e)Validar o modelo, aplicando em um cenário real, identificando melhorias junto a especialista e ajustando a versão para a entrega.

Avaliação dos Riscos e Benefícios:

Segundo os pesquisadores:

Riscos:

Pode-se citar como possíveis desconfortos e riscos decorrentes do preenchimento do questionário, o cansaço ou possíveis aborrecimento, a interferência na vida cotidiana ou na rotina de trabalho para o preenchimento do mesmo, sensação de coerção para participar da pesquisa ou algum constrangimento que possa ser causado decorrente da não compreensão de algumas das questões. Considera-se que os riscos apresentados são baixos pois o tempo necessário para o preenchimento não deve ultrapassar 15 minutos, o questionário será aplicados a profissionais atuantes em atividades de proteção e privacidade de dados que possuem conhecimento sobre o assunto e os contatos para esclarecimento de eventuais dúvidas estará disponível do documento de aceite de participação.

Benefícios:

Como benefícios de participação nesta pesquisa (questionário), pode-se citar a oportunidade de contribuir com a proposição de um modelo para apoiar os profissionais envolvidos na temática de proteção e privacidade de dados e a obtenção de conhecimentos com o recebimento da pesquisa completa logo após sua finalização.

Comentários e Considerações sobre a Pesquisa:

Trata-se de projeto de tese de doutorado de Gislaine Parra Freund, sob a orientação de Douglas Dyllon Jeronimo de Macedo, do Programa de Pós-Graduação em Ciência da Informação do Centro de Ciências da Educação da Universidade Federal de Santa Catarina.

Segundo os pesquisadores:

Para alcançar os objetivos deste trabalho de tese, quanto a sua natureza, será realizada uma pesquisa aplicada e quanto à abordagem do problema, este estudo utilizará métodos mistos quantitativo e qualitativo, com predominância na abordagem qualitativa. A natureza do objetivo é exploratória e descritiva por ter como parte do escopo proporcionar mais familiaridade com o problema e torná-lo mais explícito, descrevendo princípios, casos e abordagens relacionadas ao gerenciamento de evidências e proteção e privacidade de dados. Quanto aos procedimentos técnicos, esta pesquisa é classificada como bibliográfica, com survey e experimental. A pesquisa bibliográfica está presente na construção da revisão de literatura, bem como auxiliará nas análises e no desenvolvimento do modelo a ser proposto. A pesquisa com survey será aplicada em profissionais responsáveis na definição e na avaliação de evidências, com o objetivo de obter maior compreensão das práticas adotadas e desafios percebidos por estes e com isso, para utilizar

as respostas como contribuição para o modelo a ser proposto. Na etapa de validação do modelo será adotada a pesquisa experimental com a aplicação do modelo em um cenário real pela pesquisadora, que possibilitará a observação e identificação de melhorias durante sua utilização, além da submissão de um questionário a especialistas para avaliarem a adequação do modelo. Como método de pesquisa este trabalho utilizará o Design Science Research – DSR, seguindo as seguintes etapas: Identificar o problema e motivação; Definir o objetivo da solução; Projetar e desenvolver o artefato; Demonstrar o artefato; Avaliar o artefato e Comunicar os resultados.

Considerações sobre os Termos de apresentação obrigatória:

1) A redação dos Riscos e Benefícios está de acordo com as indicações do documento orientações para evitar pendências do CEPSH/UFSC.

2) Folha de Rosto assinada pelo orientador Douglas Dyllon Jeronimo de Macedo, e pelo coordenador do Programa de Pós-Graduação em Ciência da Informação do Centro de Ciências da Educação da Universidade Federal de Santa Catarina, Adilson Luiz Pinto, em 22 de fevereiro de 2021.

3) Carta de anuência: não há.

4) TCLE: apresenta um TCLE para o participante da pesquisa, que não contempla as exigências da resolução 510/2016.

5) Cronograma: Considerando o cronograma apresentado na Plataforma Brasil, a previsão de início do estudo é em 16/07/2021 com previsão de término em 26/07/2021.

6) Orçamento: informa não haver despesas.

Recomendações:

No trecho, do segundo parágrafo do TCLE, está faltando o verbo "ser" entre "devem" E "respondidas": "As perguntas apresentadas no questionário devem respondidas de acordo com as práticas adotadas por você em suas atividades profissionais e lhe será assegurado o acompanhamento e assistência durante todo o preenchimento do questionário".

No trecho seguinte, na segunda página do TCLE, o verbo está mal conjugado: Deveria ser "por se tratar", mas está assim: "Por trata de uma atividade a ser realizada de forma virtual, não estão previstas despesas financeiras (deslocamentos, alimentação, etc) para a participação nesta pesquisa porém, caso ocorram despesas imprevistas comprovadamente decorrentes de sua participação nesta pesquisa, as mesmas serão ressarcidas pelos pesquisadores.

Ainda recomenda-se a revisão do português, tanto do TCLE quanto dos questionários.

Conclusões ou Pendências e Lista de Inadequações:
Todas as pendências foram resolvidas, e o projeto está aprovado.

Lembramos aos senhores pesquisadores que, no cumprimento da Resolução 466/12, o Comitê de Ética em Pesquisa (CEP) deverá receber relatórios semestrais e/ou anuais sobre o andamento do estudo, bem como a qualquer tempo e a critério do pesquisador nos casos de relevância, além do envio dos relatos de eventos adversos, para conhecimento deste Comitê.

Este CEP aceita documentos assinados escaneados e documentos com assinatura digital sem questionar ou verificar a sua autenticidade. Isso pressupõe que o pesquisador responsável (ou seu delegado), que carregou o documento na Plataforma Brasil ao fazer o acesso com nome de usuário e senha, responsabiliza -se pela sua autenticidade e por eventuais consequências decorrentes dessa situação. Recomendamos aos pesquisadores que, para fins de eventual verificação, guardem em seus arquivos todos os documentos originais assinados manual ou digitalmente.

Esclarecemos que o CEPSH está sob fiscalização da CONEP e tem a obrigação de verificar se todos itens exigidos estão de acordo com a legislação, sob pena de sanções tais como suspensão ou descredenciamento, o que seria extremamente prejudicial a toda a comunidade acadêmica da UFSC e de outras instituições que utilizam seu serviço.

Considerações Finais a critério do CEP:

Este parecer foi elaborado baseado nos documentos abaixo relacionados:

UNIVERSIDADE FEDERAL DE SANTA CATARINA - UFSC

Continuação do Parecer: 4.704.149

Tipo Documento	Arquivo	Postagem	Autor	Situação
Informações Básicas do Projeto	PB_INFORMAÇÕES_BÁSICAS_DO_PROJETO_1703904.pdf	24/04/2021 23:26:30		Aceito
Outros	Questionario_Gislaine_Parra_Freund_24_04_2021.pdf	24/04/2021 23:24:01	GISLAINE PARRA FREUND	Aceito
Outros	Carta_Resposta_Parecer_4618918_24_04_2021.pdf	24/04/2021 23:22:55	GISLAINE PARRA FREUND	Aceito
Projeto Detalhado / Brochura Investigador	Projeto_Gislaine_Parra_Freund_24_04_2021.pdf	24/04/2021 23:18:47	GISLAINE PARRA FREUND	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	TCLE_Gislaine_Parra_Freund_24_04_2021.pdf	24/04/2021 23:18:17	GISLAINE PARRA FREUND	Aceito
Folha de Rosto	FolhaDeRosto_Gislaine_Parra_Freund.pdf	22/02/2021 21:54:26	GISLAINE PARRA FREUND	Aceito

Situação do Parecer:
Aprovado

Necessita Apreciação da CONEP:
Não

FLORIANOPOLIS, 11 de Maio de 2021

Assinado por:
Nelson Canzian da Silva
(Coordenador(a))

Endereço: Universidade Federal de Santa Catarina, Prédio Reitoria II, R: Desembargador Vitor Lima, nº 222, sala 401
Bairro: Trindade **CEP:** 88.040-400
UF: SC **Município:** FLORIANOPOLIS
Telefone: (48)3721-6094 **E-mail:** cep.propesq@contato.ufsc.br

APÊNDICE B – AVALIAÇÃO DA ADEQUAÇÃO DO MODELO - APLICAÇÃO

1 - Foi identificada a necessidade de algum ajuste nos princípios e nomenclaturas definidas para o modelo?

(**X**) Não.

( ) Sim Quais? Como foram tratadas?

2 - Foi identificada a necessidade de alguma adequação nas ações sugeridas em cada camada do modelo?

( ) Não.

(**X**) Sim.

Qual(is)?

Foi identificado que não era relevante registrar as perspectivas as quais estavam sendo utilizadas para apoiar a localização das evidências. O objetivo de uso deste instrumento é apenas para a condução da entrevista, para fins de identificação dos artefatos. Este campo não será utilizado posteriormente.

Como foi(ram) tratada(s)?

O campo de registro das perspectivas foi excluído do formulário e a aplicação seguiu sem o registro.

3 – A abordagem definida para gerenciar as evidências é pertinente e adequada?

( ) Não. Qual(is) ajuste(s) é/são necessário(s)? Como foi(ram) tratada(s)?

(**X**) Sim.

4 - Foram obtidas sugestões e/ou opiniões durante a aplicação do modelo?

(**X**) Não.

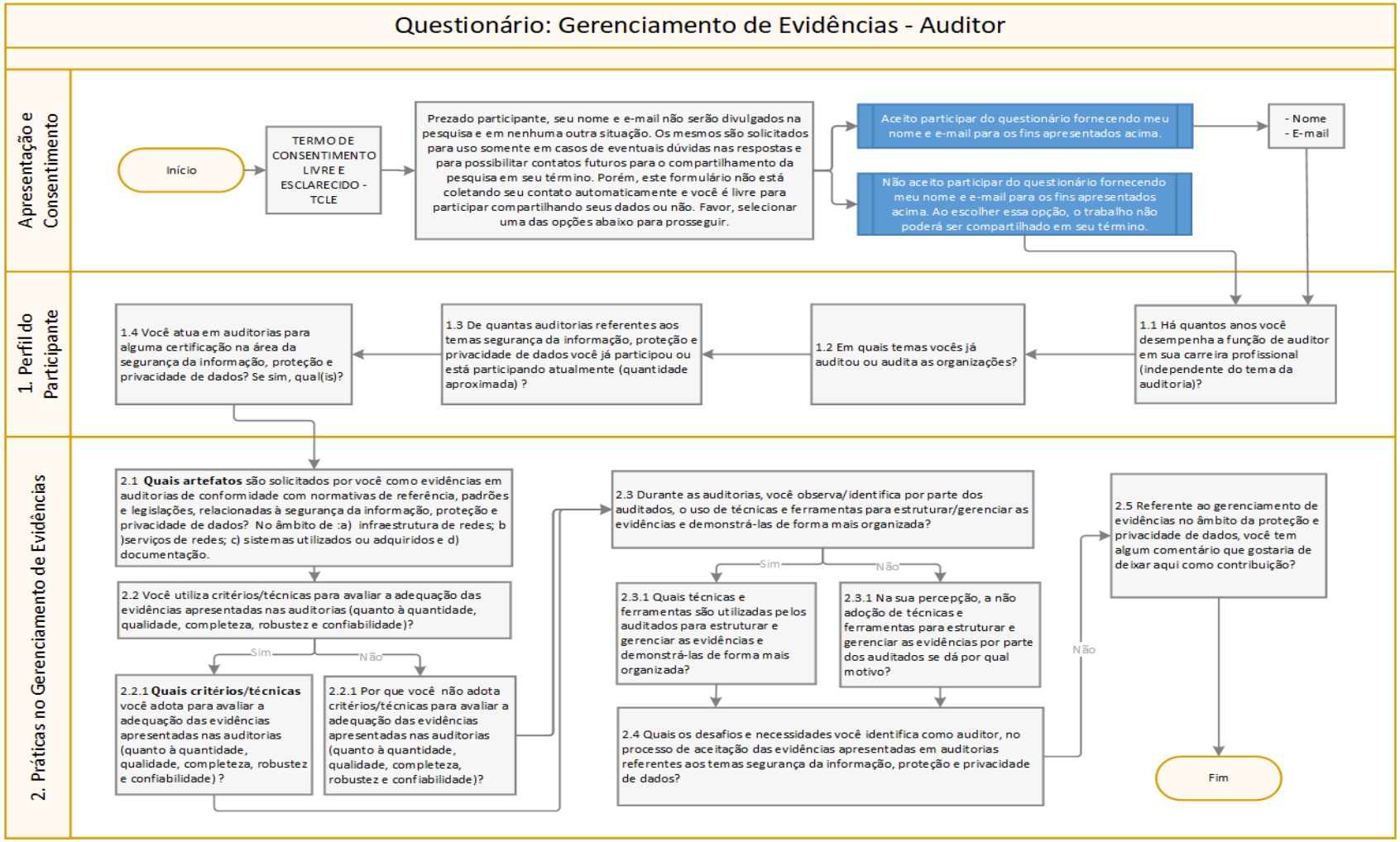
( ) Sim. Qual(is)? Como foi(ram) tratada(s)?

5 – Foram encontrados problemas ou dificuldades durante a aplicação do modelo?

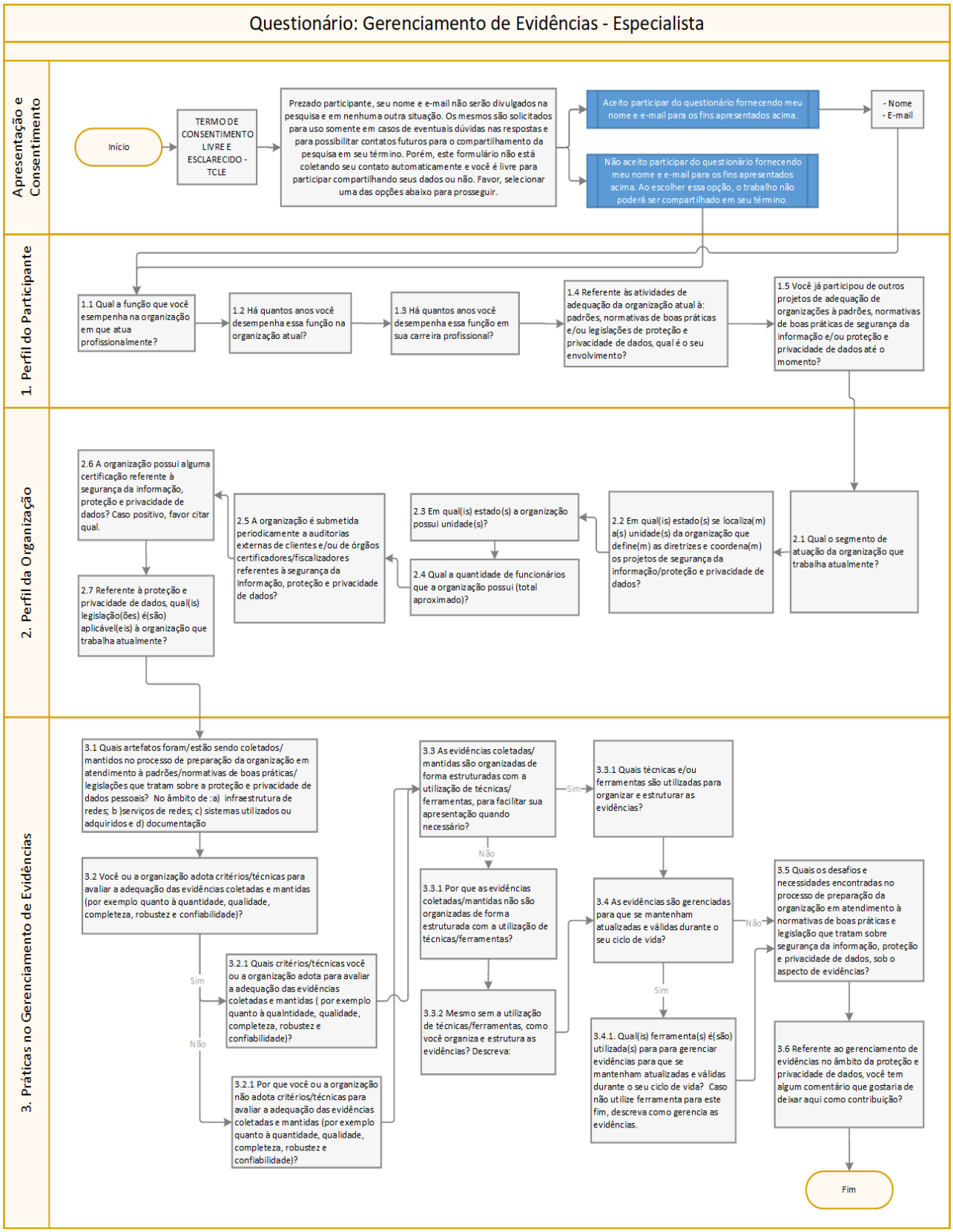
(**X**) Não.

( ) Sim Qual(is)? Como foi(ram) tratada(s)?

APÊNDICE C – QUESTIONÁRIO AUDITOR



APÊNDICE D – QUESTIONÁRIO ESPECIALISTA



APÊNDICE E – RESULTADO DA PESQUISA COM ESPECIALISTAS E AUDITOR

QUESTIONÁRIO PARA A OBTENÇÃO DA COMPREENSÃO SOBRE O PLANEJAMENTO E PRÁTICAS ADOTADAS PELAS ORGANIZAÇÕES E POR PROFISSIONAIS QUE AFEREM A ADERÊNCIA DAS ORGANIZAÇÕES A REQUISITOS DE PROTEÇÃO E PRIVACIDADE DE DADOS.

Este questionário é parte da pesquisa de Doutorado intitulada "PROPOSTA DE UM MODELO PARA GERENCIAMENTO DE EVIDÊNCIAS PROBATÓRIAS NO ÂMBITO DA PROTEÇÃO E PRIVACIDADE DE DADOS" e tem como objetivo obter insights e compreender: (i) como as organizações vem pensando e praticando o gerenciamento de evidências no âmbito da proteção e privacidade de dados, as técnicas e ferramenta utilizadas; (ii) como as evidências são avaliadas por profissionais responsáveis por aferir se um ambiente, sistema ou serviço está aderente a requisitos de proteção e privacidade de dados; e (iii) utilizar as respostas como contribuição para o modelo a ser proposto neste estudo.

Serão investigados nestes questionários: a) os tipos de informações e artefatos que estão sendo coletados, preservados e exigidos como evidências probatórias; b) as técnicas de estruturação e avaliação dessas evidências; c) as práticas que apoiam na gestão da evolução e mudanças ocorridas que possam afetar as evidências coletadas (gerenciamento); d) os critérios exigidos na avaliação e validação das evidências; e e) os desafios que os profissionais enfrentam atualmente no preparo e na validação das evidências.

Os questionários estão organizados em 3 etapas sendo elas: uma para identificar o perfil dos participantes, uma para identificar o perfil da organização e a outra para identificar as práticas no gerenciamento de evidências.

QUESTIONÁRIO 1 - Especialistas

Características dos participantes: profissionais que atuam em organizações de diferentes segmentos (Sistemas e Serviços; Financeira; Educação/Pesquisa e Saúde) responsáveis por preparar as organizações e torná-las aderente aos requisitos de proteção e privacidade de dados, deixando-as preparadas também para comprovar sua diligência e demonstrar que as alegações de proteção e privacidade são verdadeiras.

PERFIL DOS PARTICIPANTES

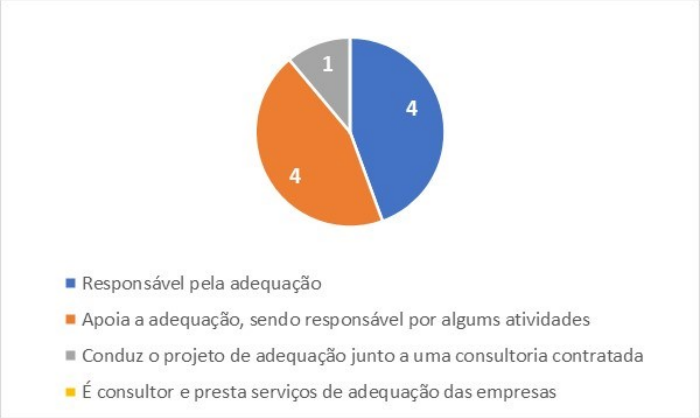
1.1 Qual a função que você desempenha na organização em que atua profissionalmente?

- CISO
- Analista de Segurança da Informação
- Gerente de TI
- Superintendente de TI
- Analista de segurança da informação
- Superintendente Jurídico
- COORDENAÇÃO ADMINISTRATIVA, FINANCEIRA E CONTÁBIL
- Gerente de TI/INFOSEC
- Gerente de Tecnologia

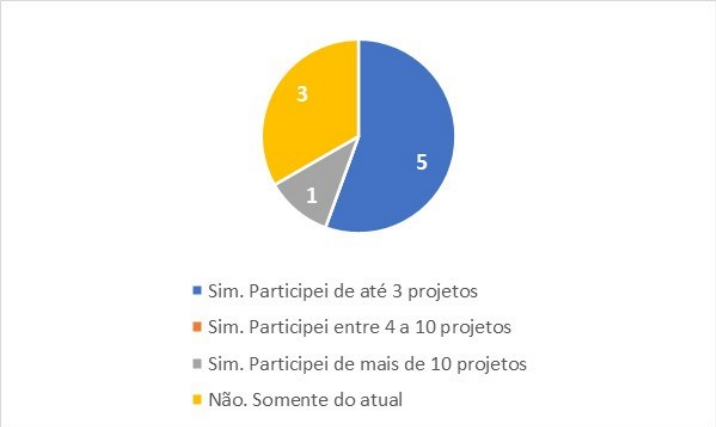
1.2 Há quantos anos você desempenha essa função na organização atual? (9 respostas)

1.3 Há quantos anos você desempenha essa função em sua carreira profissional? (9 respostas)

1.4 Referente às atividades de adequação da organização atua à padrões, normativas de boas práticas e/ou legislações de proteção e privacidade de dados, qual é o seu envolvimento? (9 respostas)



1.5 Você já participou de outros projetos de adequação de organizações à padrões, normativas de boas práticas de segurança da informação e/ou proteção e privacidade de dados até o momento? (9 respostas)



PERFIL DA ORGANIZAÇÃO

2.1 Qual o segmento de atuação da organização que trabalha atualmente?

- 44.4% - Call Center
- 33,3% - Desenvolvimento de sistemas/soluções
- 11,1% - Fabricação e comercialização de motores elétricos, transformadores e geradores.
- 11,1% - Operadora de Plano de Saúde na modalidade autogestão

2.2 Em qual(is) estado(s) se localiza(m) a(s) unidade(s) da organização que define(m) as diretrizes e coordena(m) os projetos de segurança da informação/proteção e privacidade de dados?

- 100% SC
- 33,3% SP

2.3 Em qual(is) estado(s) a organização possui unidade(s)?

- 100% - SC
- 77,8% - SP
- 44,4% - RS
- 11,1% - MG
- 11,1% - ES
- 11,1% - DF
- 11,1% AM

2.4 Qual a quantidade de funcionários que a organização possui (total aproximado)?

- 30000
- 11000
- 500
- 12000
- 11.000
- 12.000
- 22
- 300
- 80

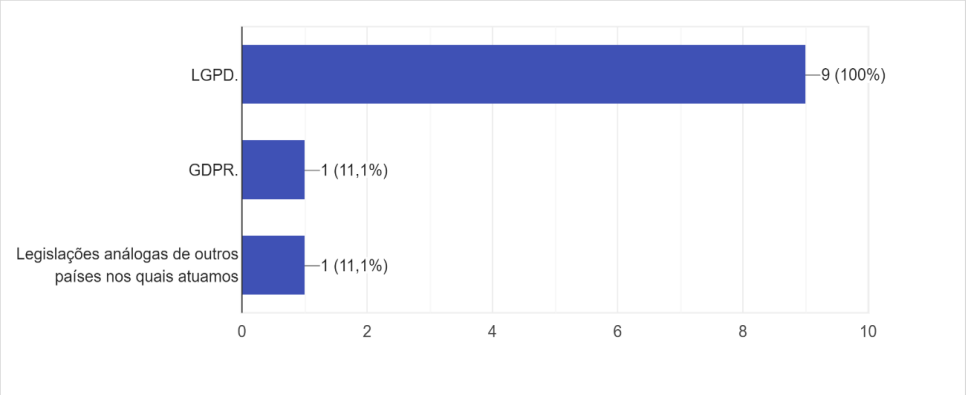
2.5 A organização é submetida periodicamente a auditorias externas de clientes e/ou de órgãos certificadores/fiscalizadores referentes à segurança da informação, proteção e privacidade de dados? (9 respostas)

2.6 A organização possui alguma certificação referente à segurança da informação, proteção e privacidade de dados? Caso positivo, favor citar qual.

NÃO – 8 respostas

SIM – 1 resposta – PCI-DSS

2.7 Referente à proteção e privacidade de dados, qual(is) legislação(ões) é(são) aplicável(eis) à organização que trabalha atualmente?



PRÁTICAS NO GERENCIMENTO DE EVIDÊNCIAS

3.1 a) Quais artefatos foram/estão sendo coletados/mantidos no processo de preparação da organização em atendimento à padrões/normativas de boas práticas/legislações que tratam sobre a proteção e privacidade de dados pessoais – no âmbito da insfraestrutura de redes (p.e: topologia, inventário de ativos, inventário de softwares etc.)?

- Diversos artefatos são coletados, desde aqueles relacionados à infraestrutura, como os citados no exemplo, quanto aqueles relacionados aos dados e informações em si, tais como classificação de informação, inventário de dados etc.
- Topologia de rede, inventário de ativos e softwares, evidência de implementação de soluções de segurança para redes (firewall, ids/ips, anti-ddos).
- Adequação de topologia, inventário de hardware e software, capacitação de colaboradores, revisão estrutura de usuários e acessos.
- Inventário de ativos, topologia datacenter, Topologia de Rede, procedimentos de gerenciamento de mudanças, políticas de acesso a Datacenter.
- Topologia, inventário de ativos, inventário de softwares, firewall, sistema de prevenção e detecção de intrusão.
- Não tenho conhecimento.
- No que diz respeito à infraestrutura de rede, a empresa de consultoria contratada nos solicitou os nomes dos sistemas utilizados e fez alguns questionamentos para

o analista técnico responsável pela TI da empresa. Enviamos em alguns momentos prints de tela para conhecerem a forma como o sistema funciona. Informações sobre armazenamentos, servidores e sistemas foram obtidas através de questionários mesmo, nenhuma outra comprovação além dos contratos com as empresas de software e com o DBA (hoje também função exercida por empresa terceirizada).

- Inventado de ativos, mapeamento de Fluxos.
- Topologias, documentação de IaaS, Inventário de hardware, inventário de software

3.1 b) Quais artefatos foram/estão sendo coletados/mantidos no processo de preparação da organização em atendimento à padrões/normativas de boas práticas/legislações que tratam sobre a proteção e privacidade de dados pessoais no âmbito dos serviços de redes (p.e: print de configurações, Listas, termos de abertura de projetos, contrato com fornecedores etc.)?

- CMDB, documentação de configurações, documentação de projetos, contratos e NDAs com fornecedores etc.
- Print de configurações, chamados de projetos, chamados de tratativa de correções, contrato com fornecedores.
- Contratos (Trabalho, Cliente, Fornecedor etc.), procedimentos operacionais, políticas institucionais, processos, manuais etc.
- Logs de *Active Directory*, firewall, Proxy, SIEM e DLP; print de tela com configurações em serviços de rede; Print de execução de comandos listando registros com Bloqueio do Sistema operacional.
- Print de configurações, Listas, termos de abertura de projetos, contrato com fornecedores, relatórios de auditoria, testes, políticas e normas internas.
- Não tenho conhecimento.
- A empresa de consultoria contratada nos solicitou contratos vigentes com prestadores, modelos de documentos preenchidos pelos colaboradores na contratação, nos questionou sobre políticas tais como código de ética, política de privacidade (nos auxiliou na construção de uma política preliminar no início do projeto), nos solicitou também modelos de documentos preenchidos por beneficiários, mapeou e fez entrevistas com os colaboradores sobre os principais processos e nos apresentou recentemente um Relatório da Etapa de preparação e ações prioritárias após analisar os documentos enviados, questionários preenchidos e entrevistas. Para explicar alguns processos foram enviados prints para melhor explicar e exemplificar o processo. O relatório apresentado traz a metodologia que adotaram, o nível de maturidade da organização em relação à privacidade da informação e apresentou os GAPs identificados e os tratamentos a serem realizados para adequação de forma geral, abrangendo toda a organização e inerentes a cada processo. Estamos na fase do projeto de definição das ações e prazos para iniciar a adequação com a finalidade de melhorar a maturidade da

organização em relação à privacidade da informação, avaliada no relatório apresentado como "Ad Hoc: procedimentos ou processos são geralmente informais incompletos e aplicados sem consistência. Os objetivos de controle não estão bem definidos, ou a sua percepção não é consistente em toda a organização".

- Revisão de contratos com fornecedores e clientes, termos de aceite/adesão.
- Contratos com fornecedores.

3.1 c) Quais artefatos foram/estão sendo coletados/mantidos no processo de preparação da organização em atendimento à padrões/normativas de boas práticas/legislações que tratam sobre a proteção e privacidade de dados pessoais no âmbito dos sistemas utilizados ou adquiridos (p.e: banco de dados, política de desenvolvimento seguro etc.)?

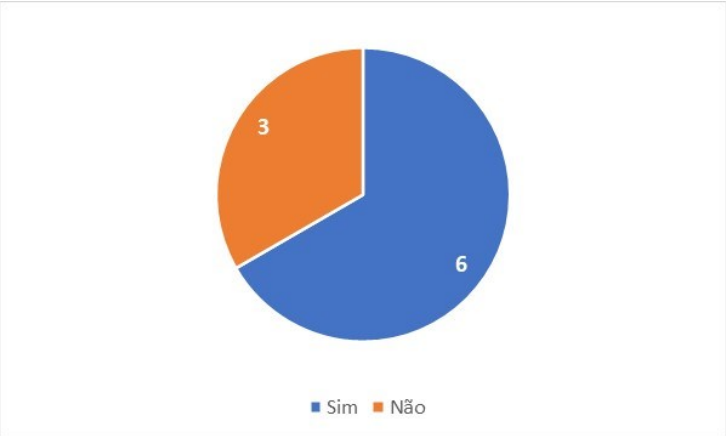
- Software Development Lifecycle, Metodologia de Desenvolvimento de Software, Guia de Segurança para o Desenvolvimento e Aquisição de Sistemas, Baseline de Segurança para Databases, e outros.
- Banco de dados, política de desenvolvimento seguro, testes de vulnerabilidades.
- Revisão da política de desenvolvimento de softwares internos, revisão e centralização dos sistemas de banco de dados, revisão da arquitetura e políticas de acesso.
- Log de acessos a funções dentro dos sistemas utilizados, Log de pessoas com acessos a execução de consultas nos bancos, documento com política de utilização de ambiente de teste/homologação, política da empresa de desenvolvimento detalhando a política de desenvolvimento seguro que utiliza, Comprovação de utilização das práticas de níveis de acesso dentro das funções do sistema.
- Banco de dados, política de desenvolvimento seguro, testes de boas práticas de desenvolvimento, exigências contratuais, prints de configurações.
- Norma de Uso dos Recursos de Tecnologia da Informação e Comunicação e Política de Desenvolvimento Seguro.
- Somente o contrato com a empresa de sistemas até o momento. Não foi solicitado nada que comprove o tratamento dado aos dados nessas empresas, somente analisadas as cláusulas dos contratos e fizemos uma reunião no início do projeto convidando os principais prestadores a participar para compor prova de que estamos buscando a adequação e divulgar a importância da adequação por todos os envolvidos. Porém na época não teve participação da maioria, então não sei se isso compõe prova.
- Políticas de retenção de dados e desenvolvimento seguro (*Privacy by Design*).
- Documento de governança de TI.

3.1 d) Quais artefatos foram/estão sendo coletados/mantidos no processo de preparação da organização em atendimento à padrões/normativas de boas

práticas/legislações que tratam sobre a proteção e privacidade de dados pessoais no âmbito da documentação (p.e: políticas, procedimentos, relatórios etc.)?

- Política de Segurança da Informação, Política de Privacidade, Termo de Responsabilidade no Uso das Informações da Empresa, e outros.
- Políticas, procedimentos, normas, relatórios de execução, evidências de implementação de controles.
- procedimentos operacionais, políticas institucionais, processos, manuais etc.
- Políticas de gerenciamento de acessos, política de privacidade de dados.
- políticas, procedimentos, relatórios, normas, códigos de conduta, termos.
- Política de Segurança da Informação, Política de Governança de Dados, Política de Gestão do Programa de Privacidade, Política de Gestão de Incidentes de Violação a Dados Pessoais, Política de Atendimento aos Direitos dos Titulares, Procedimento para Avaliação da Governança e Proteção de Dados Pessoais em Terceiros e Relatório de Impacto à Proteção de Dados Pessoais.
- Há o relatório da etapa de preparação e ações prioritárias realizado pela consultoria contratada. Todas as etapas do projeto até o momento tiveram reuniões gravadas pelo google Meet, inclusive as entrevistas com colaboradores e as apresentações dos resultados. Uma das ações propostas no relatório apresentado da etapa de preparação é incluir cláusulas nos contratos vigentes e implantar algumas políticas necessárias indicadas nesse relatório e estamos em fase de estipular os prazos para as adequações.
- Políticas e procedimentos de gestão de incidentes.
- Política de Segurança.

3.2 Você ou a organização adota critérios/técnicas para avaliar a adequação das evidências coletadas e mantidas (por exemplo quanto à quantidade, qualidade, completeza, robustez e confiabilidade)? (9 respostas)

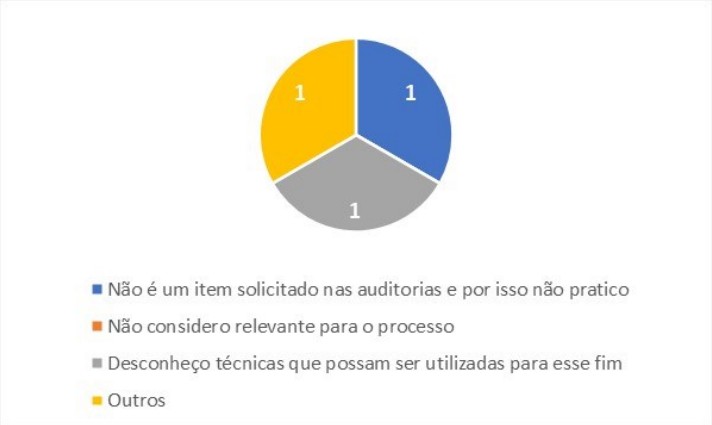


3.2.1 Quais critérios/técnicas você ou a organização adota para avaliar a adequação das evidências coletadas e mantidas (por exemplo quanto à quantidade,

qualidade, completeza, robustez e confiabilidade)?

- Os critérios e técnicas são gerenciados pela área de Controles e Tributário Internacional.
- Atualmente a organização não possui um processo formalizado quanto ao tema, mas no momento de abertura de solicitação de evidências é especificado exatamente o que é esperado da evidência a ser disponibilizada no que se refere à quantidade, qualidade, completeza, robustez e confiabilidade, sendo avaliado e caso não seja aderente ao esperado, ocorre a solicitação de melhoria da evidência, descrição e informações complementares.
- Revisões mediante a aprovação do Comitê de Proteção de Dados, necessário apresentação de evidências quando as correções realizadas.
- São definidos pontos a serem seguidos para a coleta e disponibilização de evidências, sendo que estas devem atender exatamente o que é esperado pelo solicitante.
- São avaliados os retornos recebidos dos contratantes a respeito das evidências encaminhadas. Além disso são realizadas auditorias internas e revisão de políticas e procedimentos em frequência e formato preestabelecidos.
- Política de retenção de dados/logs.

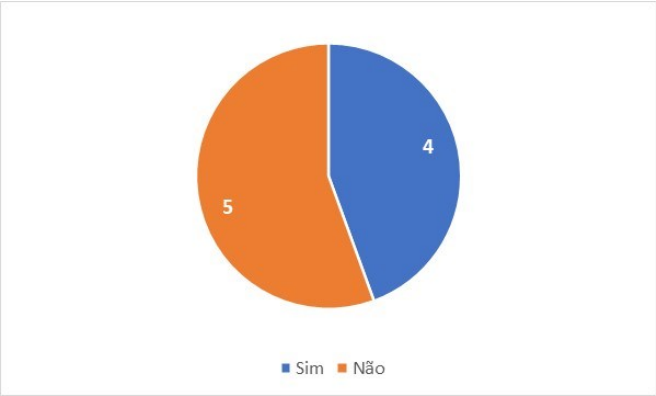
3.2.1 Por que você ou a organização não adota critérios/técnicas para avaliar a adequação das evidências coletadas e mantidas (por exemplo quanto à quantidade, qualidade, completeza, robustez e confiabilidade)? (3 respostas)



Outros: O nosso projeto de adequação ainda está em andamento. Até o momento não recebemos informações sobre a governança da adequação à LGPD ou técnicas para avaliar as evidências. A consultoria contratada apresentará técnicas para auxiliar na governança, mas não lembro de ter citado essa questão de avaliar a adequação das evidências.

3.3 As evidências coletadas/mantidas são organizadas de forma estruturada com

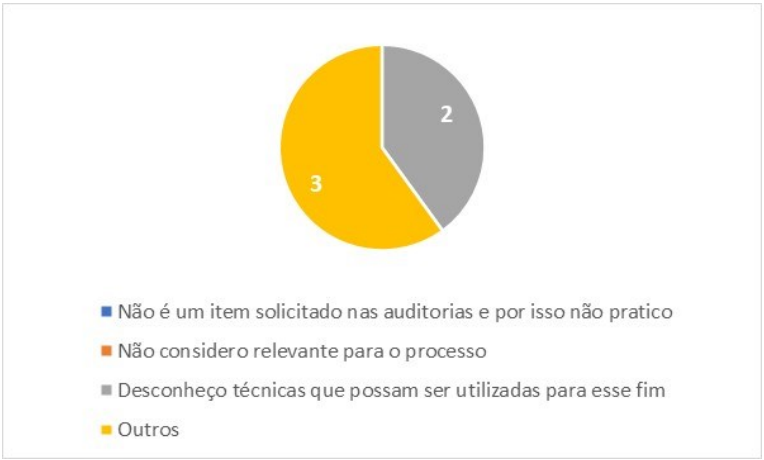
a utilização de técnicas/ferramentas para facilitar sua apresentação quando necessário? (9 respostas)



3.3.1 Quais técnicas e/ou ferramentas são utilizadas para organizar e estruturar as evidências?

- Evidências são organizadas e referenciadas de acordo com a solicitação que correspondem, em diretórios específicos para essa finalidade com acesso controlado.
- Confluence (Wi-ki corporativa) e Diretórios de Documentação da LGPD.
- Todas as evidências são solicitadas por chamados, organizadas e nomeadas conforme ao item que corresponde e são armazenadas em diretório para essa finalidade com controle de acesso restrito.
- Sharepoint.

3.3.1 Por que as evidências coletadas/mantidas não são organizadas de forma estruturada com a utilização de técnicas/ferramentas? (5 respostas)



Outros:

- Esta atividade está em desenvolvimento,

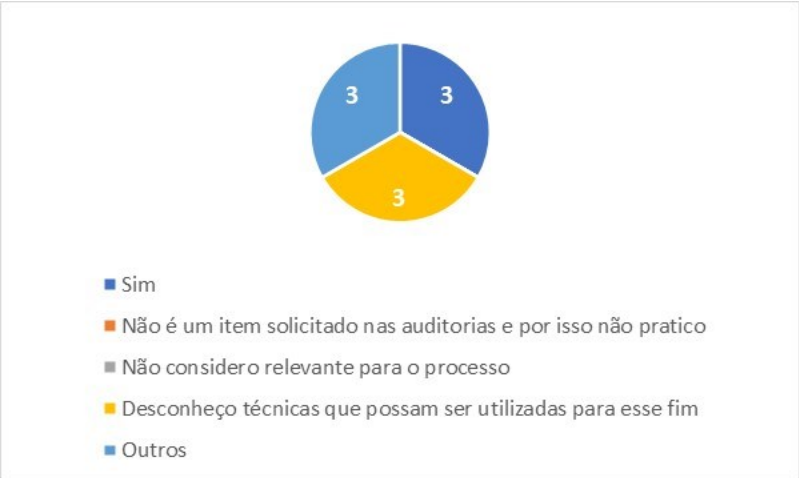
- Falta de braço,

- Não há ferramentas disponíveis para coleta e manutenção das evidências de forma organizada. Normalmente envolve custo e as empresas não estão dispostas a investir nesse quesito.

3.3.2 Mesmo sem a utilização de técnicas/ferramentas, como você organiza e estrutura as evidências? Descreva:

- Esta atividade está em desenvolvimento.
- Normalmente as solicitações já possuem um padrão a ser entregue pelos diversos clientes e com isto temos que seguir o que é solicitado.
- Elas são categorizadas em pastas, disponíveis em rede, de forma compartilhada, para consulta, na medida em que são solicitadas.
- Estamos sob orientação de uma consultoria contratada. As etapas até o momento para construir evidências sobre a adequação foram: adequações iniciais do site (política de privacidade, bandeira dos cookies e formulário para questionamentos para o DPO); reuniões e e-mails como prova de adequação aos fornecedores, clientes e colaboradores.
- Planilhas.

3.4 As evidências são gerenciadas para que se mantenham atualizadas e válidas durante o seu ciclo de vida? (9 respostas)

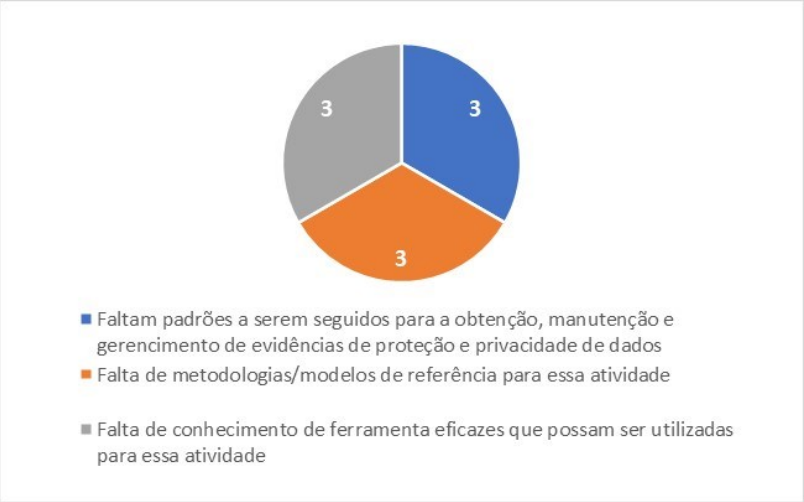


Outros:
- Esta atividade está em desenvolvimento.
- As evidências são levantadas conforme necessidade e não são reutilizadas, em caso de novas solicitações são retiradas novas evidências, até porque no caso da minha organização cada cliente pode ter uma particularidade e a evidência encaminhada para um, pode não servir para outro.
- Não, mas estamos trabalhando para tentar operacionalizar.

3.4.1. Qual(is) ferramenta(s) é(são) utilizada(s) para gerenciar evidências para que se mantenham atualizadas e válidas durante o seu ciclo de vida? Caso não utilize ferramenta para este fim, descreva como gerencia as evidências.

- Esta atividade está em desenvolvimento.
- O gerenciamento de evidências é realizado de forma manual, sendo a solicitação por chamado, envio de forma segura e armazenamento em diretório específico com controle de aceso.
- Ainda estamos operacionalizando.
- Todas as evidências são solicitadas por chamados, organizadas e nomeadas conforme ao item que corresponde e são armazenadas em diretório para essa finalidade com controle de acesso restrito. Evidências não são reutilizadas devido a particularidades do ambiente de cada cliente que temos em nossa estrutura.
- Não são utilizadas ferramentas. Existe um controle, em Excel, com um cronograma para atualização e revisão das evidências.
- Sharepoint.

3.5 Quais os desafios e necessidades encontradas no processo de preparação da organização em atendimento à normativas e boas práticas e legislações de proteção e privacidade de dados, sob o aspecto de evidências? (9 respostas)



3.6 Referente ao gerenciamento de evidências no âmbito da proteção e privacidade de dados, você tem algum comentário que gostaria de deixar aqui como contribuição?

- Apesar de ser um tema que afeta todas as organizações, o mercado ainda carece de conhecimento, pessoas, metodologias e ferramentas, principalmente quando o contexto envolve diversos contextos jurídicos.

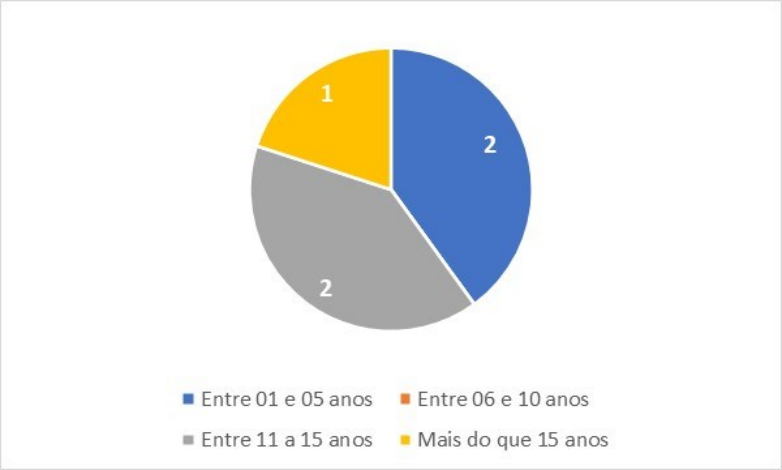
- É fundamental que a organização tenha uma metodologia definida para o gerenciamento de evidências, para garantir assertividade nas entregas e segurança com as informações contidas em cada uma.
- Ainda temos muitas dificuldades para trazer a responsabilidade do tema aos dirigentes da empresa.
- Não.
- Acredito que as empresas devem investir em controles e gerenciamento de evidências para assim manter a integridade e privacidade das mesmas.
- Esse é um tema pouco explorado em todas as rodas de discussão dos quais eu participo em proteção e privacidade de dados. Relevante a iniciativa de desenvolver-se estudos, padrões e metodologias nesse sentido, a fim de possibilitar uma melhor preparação dos profissionais para lidarem com o tema.
- Estamos ainda em processo de adequação, conhecendo ainda as ações necessárias para adequar a empresa e em processo de decisão sobre quais serão abordadas de forma prioritária. Ainda não temos a maturidade e conhecimento para essa etapa de governança da LGPD e gerenciamento das evidências no âmbito da proteção de dados, mas há a intenção de chegar em um momento de maturidade e conhecimento para isso.
- Plataforma for dummies.
- Os questionários de *compliance* das empresas geralmente se preocupam com detalhes desnecessários referentes à LGPD, apenas para passar pela etapa de preenchimento obrigatória nas empresas. Poucas empresas fazem due diligences sérias e capazes de elevar o nível da privacidade de dados, como por exemplo, solicitar o gerenciamento eficaz dos artefatos e processos que atendem à proteção dos dados. Isso inevitavelmente leva as empresas a investir onde for auxiliar mais aos negócios.

QUESTIONÁRIO 2 - Auditores

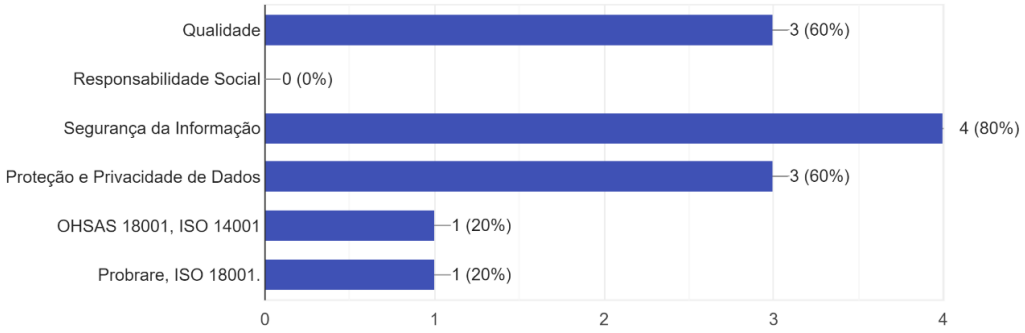
Características dos participantes: profissionais responsáveis por avaliar e aferir (auditores) se um processo, produto, serviço, sistema ou ambiente estão aderentes aos padrões e/ou normativas de proteção e privacidade de dados.

PERFIL DOS PARTICIPANTES

1.1 Há quantos anos você desempenha a função de auditor em sua carreira profissional (independente do tema da auditoria)? (5 respostas)



1.2 Em quais temas você já auditou ou audita as organizações? (5 respostas – múltipla escolha)



1.3 De quantas auditorias referentes aos temas segurança da informação, proteção e privacidade de dados você já participou ou está participando atualmente (quantidade aproximada)?

- 10.
- Participando de 1 atualmente. Já participei de muitas, não sei precisar a quantidade, mas com certeza mais de 30 auditorias externas e centenas de internas.
- +10.
- Participei de mais 300. E atualmente 35.
- 02 Eventos, apenas como Auditor de Acompanhamento LGPD.

1.4 Você atua em auditorias para alguma certificação na área da segurança da informação, proteção e privacidade de dados? Se sim, qual(is)?

- Não.
- Sim, ISO 27001.
- PCI e ISO27000.

- Sim. ISO 27001.
- Sim, LGPD. Entretanto, até o presente momento, somente acompanhamento em 02 Eventos.

PRÁTICAS NO GERENCIAMENTO DE EVIDÊNCIAS

2.1 a) Quais artefatos são solicitados por você como evidências em auditorias de conformidade com normativas de referência, padrões e legislações, relacionadas à segurança da informação, proteção e privacidade de dados – no âmbito da infraestrutura de redes (p.e: topologia, inventário de ativos, inventário de softwares etc.)?

- Topologia de rede, inventário de ativos, políticas, prints de tela.
- De acordo com o escopo de avaliação, diagrama de rede, inventário geral (ativos, softwares), localização dos ativos.
- Topologia da rede envolvida na auditoria, e das redes com autorizações/comunicações com esta rede, evidência de configurações de equipamentos que fazem validação e bloqueio de comunicações entre as redes, dependendo do que estiver autorizado e risco, evidências das requisições de mudanças que aprovaram a configuração, com justificativas e avaliações de riscos, testes e autorizações da liberação. Avaliação também da atualização do documento, se está dentro da definição das políticas internas ou se é posterior a última alteração significativa na arquitetura.
- Evidências de Dados, GPO, CFTV, Inventários de Máquinas e acessos, geradores, nobreak.
- Não se aplica, atualmente no contexto da minha atuação, uma vez que não Auditor de Segurança da Informação.

2.1 b) Quais artefatos são solicitados por você como evidências em auditorias de conformidade com normativas de referência, padrões e legislações, relacionadas à segurança da informação, proteção e privacidade de dados – no âmbito de serviços de redes (p.e: print de configurações, listas, termos de abertura de projetos, contrato com fornecedores etc.)?

- Topologia, documentos de processo, prints de tela
- De acordo com o escopo avaliado, quais são os serviços necessários para o escopo definido, *hardening* de servidores e estações (para configurações sistêmicas). Escopo de trabalho de fornecedores, resultados obtidos, melhorias, acompanhamento para serviços prestados por terceiros.

- Controle dos ativos relacionados aos serviços, com atualização dentro do prazo da política ou posterior a última alteração significativa, com detalhamento de obsolescência de equipamentos e serviços em execução, suporte, responsáveis.
- Avaliação das funções exercidas pelos serviços, avaliações de riscos, acessos, uso de contas genéricas ou compartilhadas na gestão dos serviços. São solicitadas evidências que comprovem as configurações informadas.
- LGPD e Segurança física e logica
- Não se aplica, atualmente no contexto da minha atuação, uma vez que não Auditor de Segurança da Informação.

2.1 c) Quais artefatos são solicitados por você como evidências em auditorias de conformidade com normativas de referência, padrões e legislações, relacionadas à segurança da informação, proteção e privacidade de dados – no âmbito dos sistemas utilizados ou adquiridos (p.e: banco de dados, política de desenvolvimento seguro etc.)?

- Políticas, tabelas do banco, documentos padrão, arquitetura de sistema
- Critérios de aquisição/contratação, análises de risco, *hardening* de sistemas.
- São avaliadas questões relacionadas ao tipo de informação armazenada e criticidade para a operação do negócio, para orientação do rigor da avaliação e recomendações, quanto maior o risco e exposição, mais evidências solicitadas. As coletadas de evidências (prints de telas, relatórios, configurações, documentos) que comprovem itens como requisitos como vigência de suporte, uso de versões suportadas e estáveis, arquitetura e gestão dos componentes (ativos, serviços, responsabilidades, etc.), volume de integrações e como são feitas as proteções e controles de sistemas que se conectam, exposição da internet e meios de proteção, acessos administrativos versus uso destes para acesso a dados reais, uso de logins genéricos ou compartilhadas, opções de perfis por função, autenticação, uso de relatórios e extrações de dados (como exportação para Excel ou semelhantes), gestão do ambiente como atualizações de patches, antivírus, *hardening*, backups, processos de atualização e validação de código (qualidade e código).
- Evidências remotamente e com evidências por e-mail do processo auditado
- Não se aplica, atualmente no contexto da minha atuação, uma vez que não Auditor de Segurança da Informação.

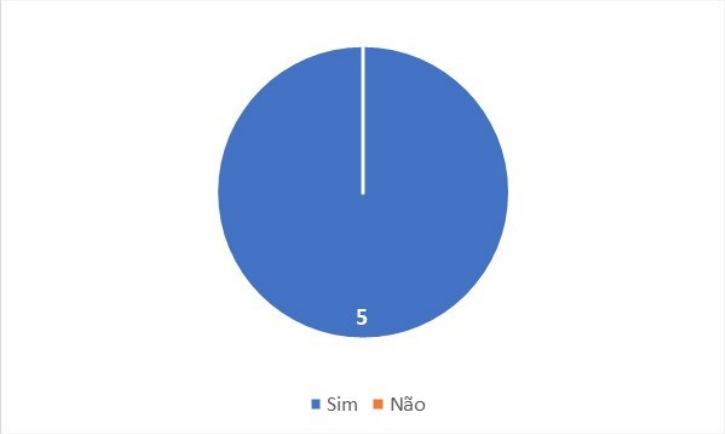
2.1 d) Quais artefatos são solicitados por você como evidências em auditorias de conformidade com normativas de referência, padrões e legislações, relacionadas à segurança da informação, proteção e privacidade de dados – no âmbito da documentação utilizados ou adquiridos (p.e: políticas, procedimentos, relatórios etc.)?

- Políticas, desenhos de processo, inventários.
- Procedimentos obrigatórios documentados, registros obrigatórios documentados.
- Políticas e normas, com as revisões dentro dos prazos estabelecidos, refletindo as responsabilidades e controles compatíveis com a estrutura corporativa, existência de indicadores de acompanhamento gerais (vulnerabilidades, obsolescência,

acessos, vazamentos, exceções, incidentes, treinamentos e conscientização, etc), registro e acompanhamento de riscos.

- Existe a classificado risco das empresas auditadas onde é gerado o relatório com a graduação e planos de ações.
- Apenas considerando o tema de LGPD, requisito os seguintes documentos, mas não se limitando a: Política de Privacidade, Avaliação de Impacto na Privacidade (AIP), Termo de Uso, Política de Cookies, Termos de consentimento, Política de retenção de dados, Levantamento e atendimento aos requisitos legais aplicáveis ao setor, Gestão de mudanças no caso de alterações que possam a impactar no tratamento de dados pessoais, Gestão do tratamento de dados perante terceiros.

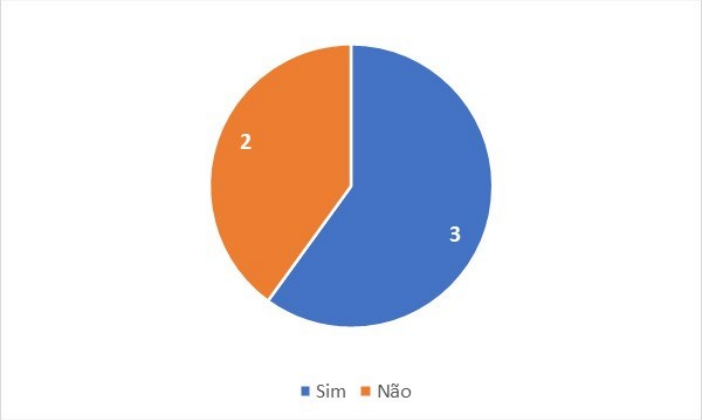
2.2 Você utiliza critérios/técnicas para avaliar a adequação das evidências apresentadas nas auditorias (quanto à quantidade, qualidade, completeza, robustez e confiabilidade)? (5 respostas)



2.2.1 Quais critérios/técnicas você adota para avaliar a adequação das evidências apresentadas nas auditorias (quanto à quantidade, qualidade, completeza, robustez e confiabilidade)?

- Tempo de vida do documento, completude do temos, abrangência, sentido e organização do documento
- Padronização de evidências, linha do tempo constante, forma de controle (planilhas manuais, relatórios automáticos etc.).
- Documentos e evidências claras, sem a omissão de trechos de telas ou relatórios, recentes, legíveis, com identificação da empresa e responsáveis, sem manipulação de dados (dados brutos da extração), protegido quanto a manipulação por terceiros, histórico de versões.
- Regras do *compliance*, controles internos. Método Ágil, Score S.I.
- Durante o processo de Auditoria a amostragem é realizada de forma a evidenciar o atendimento aos princípios, leis e normas, dando prioridade aos maiores riscos identificados pela Organização, avaliando a coerência da documentação dentro do contexto e efetiva implementação do programa da LGPD.

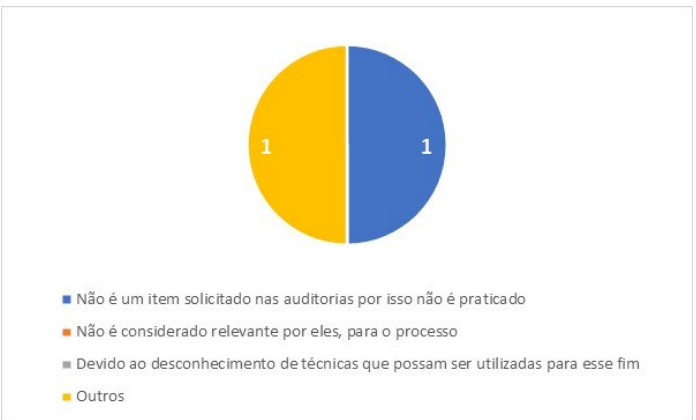
2.3 Durante as auditorias você observa/identifica por parte dos auditados. O uso de técnicas e ferramentas para estruturar/gerenciar as evidências e demonstrá-las de forma mais organizada? (5 respostas)



2.3.1 Quais técnicas e ferramentas são utilizadas pelos auditados para estruturar e gerenciar as evidências e demonstrá-las de forma mais organizada?

- Para aqueles que tiverem a disponibilidade, documentos padronizados, especificando o objetivo das amostras e as informações apresentadas de maneira organizada. Garantindo a integridade da amostra. Repositórios organizados por temas e períodos.
- MSA - Measurement System Analysis, Box Plot
- Normalmente são apresentadas planilhas de gestão, softwares específicos, demonstração da revisão de contratos, capacitação da equipe, inventário e fluxo de dados pessoais, incluindo os sensíveis.

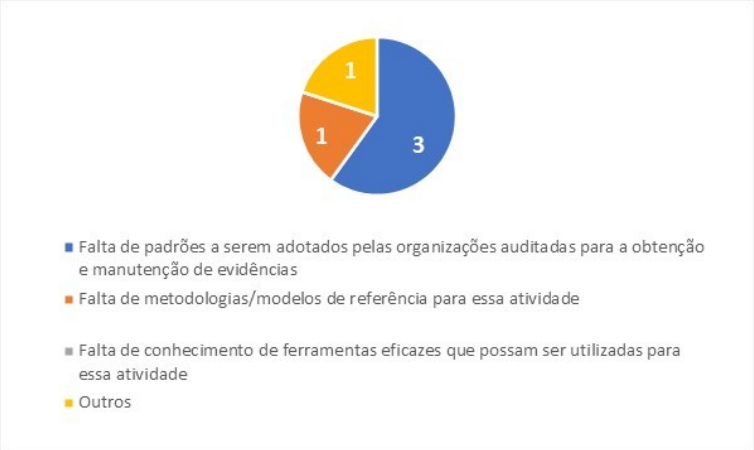
2.3.1 Na sua percepção, a não adoção de técnicas e ferramentas para estruturar e gerenciar as evidências por parte dos auditados se dá por qual motivo? (2 respostas)



Outros:

- Na grande maioria dos casos, os auditados não organizam as evidências pois as atividades do dia a dia são alocadas a diferentes equipes e cada equipe possui o próprio modo de organização. Não vale a pena sistematicamente organizar métodos diferenciados de organização de evidências somente para serem apresentadas em auditoria

2.4 Quais os desafios e necessidades você identifica como auditor, no processo de aceitação das evidências apresentadas em auditorias referentes à segurança da informação, proteção e privacidade de dados? (5 respostas)



Outros:

- Além da falta de padrões na geração dos artefatos, evidências com trechos parciais ou com omissões importantes de datas, identificações, objetivo da informação, ambientes (ex.: ambiente atualizado, mas nome que identifica se é homologação ou produção são extraídos da amostra).

2.5 Referente ao gerenciamento de evidências no âmbito da segurança da informação, proteção e privacidade de dados, você tem algum comentário que gostaria de deixar aqui como contribuição?

- Criar métodos exclusivos de manutenção de evidências pode gerar duplicidade de informação e consequentemente um problema de controle. Os processos devem ser estruturados de forma padronizada para que os resultados sejam produzidos sempre da forma mais padronizada possível, onde durante uma auditoria, o levantamento de resultados de uma tarefa ou evidências de execução seja conhecido e rapidamente encontrado, independente de qual área esteja executando as atividades.
- As evidências precisam ter a integridade garantida, clareza no objetivo (o que se pretende evidenciar), considerar que nem sempre o auditor domina todas as

tecnologias disponíveis, prints de telas ou relatórios parciais podem não gerar o entendimento necessário. Além disso, resultados de linhas de comandos e relatórios não devem ser manipulados nem tratados (ex.: extração de usuários ativos não devem passar por filtros prévios antes da entrega que alterem a amostra).

- Aprimoramento da gestão de terceiros relacionados ao tratamento de dados pessoais.

APÊNDICE F – AUTORIZAÇÃO

CASACARESC

ANS – nº 32755-7

AUTORIZAÇÃO

AUTORIZO que **GISLAINE PARRA FREUND**, na qualidade de pesquisadora de doutorado do projeto intitulado "Modelo para Gestão de Evidências de Privacidade de Dados", desenvolvido sob a orientação do Prof. Dr. Douglas Dyllon Jeronimo de Macedo do Programa de Pós-Graduação em Ciência da Informação da Universidade Federal de Santa Catarina, a:

- Ter acesso às informações relacionadas ao processo de "Adesão de Beneficiários" para o desenvolvimento de sua pesquisa de doutorado;
- Mapear o processo e identificar evidências de proteção e privacidade de dados junto a equipe da CasaCaresc, interagindo sempre que necessário, para tratar de assuntos relacionados ao desenvolvimento do projeto; e
- Divulgar os resultados obtidos e os artefatos elaborados provenientes da aplicação do modelo proposto em sua tese e/ou em publicações científicas resultantes da pesquisa desenvolvida.

Por fim, declaro que os artefatos contendo dados do processo de "Adesão de Beneficiários" disponibilizados e utilizados foram analisados por mim e atendem o que preconiza a Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – "LGPD") e o Decreto Estadual mº 1.184/2021.

Florianópolis, 20 de janeiro de 2021.

Claudio Cesar Reiter
Presidente - CASACARESC

CLAUDIO CESAR REITER
Presidente

Endereço: Rodovia Admar Gonzaga, 1.347, Itacorubi, CEP 88034-901 Florianópolis, Santa Catarina, Brasil
Fone (0xx48) 3665-5470 / 99637-0024 (Cadastro) - email: cadastro@casacaresc.org.br

APÊNDICE G – PARECER SUBSTANCIADO DO CEP – AVALIAÇÃO DO MODELO

UNIVERSIDADE FEDERAL DE SANTA CATARINA - UFSC

PARECER CONSUBSTANCIADO DO CEP

DADOS DO PROJETO DE PESQUISA

Título da Pesquisa: MODELO DE GERENCIAMENTO DE EVIDÊNCIAS PARA COMPROVAÇÃO DE ALEGAÇÕES DE SEGURANÇA E PRIVACIDADE DE DADOS

Pesquisador: DOUGLAS DYLLON JERONIMO DE MACEDO

Área Temática:

Versão: 3

CAAE: 55847922.5.0000.0121

Instituição Proponente: Universidade Federal de Santa Catarina

Patrocinador Principal: Financiamento Próprio

DADOS DO PARECER

Número do Parecer: 5.330.479

Apresentação do Projeto:

Projeto de doutorado de Gislaine Parra Freund no Programa de Pós-Graduação em Ciência da Informação do Centro de Ciências da Educação da Universidade Federal de Santa Catarina, orientada por Douglas Dyllon Jeronimo de Macedo.

Segundo os pesquisadores, no formulário de informações básicas da PB:

Resumo:

O universo digital proporcionou às organizações privadas e públicas, o uso massivo de dados pessoais e informações corporativas e com isso novos desafios surgiram quanto a proteção e privacidade de dados e legislações para tratar o tema foram adotadas em âmbito mundial. Diante do desafio de implementar os requisitos de privacidade de dados, observa-se que é necessário além de implementá-los, ser capaz de demonstrá-los adotando processos sistematizados que comprovem como e em quais evidências estes requisitos são validados. O objetivo desta tese é a proposição de um modelo de referência para gerenciar evidências de proteção e privacidade dos dados e assim demonstrar diligência e conformidade com normativas de referência. Para alcançar seus objetivos, será realizada uma pesquisa aplicada e quanto à abordagem do problema e este estudo utilizará métodos mistos - quantitativo e qualitativo, com predominância na abordagem qualitativa. A natureza do objetivo é exploratória e descritiva por ter como parte do escopo

Endereço: Universidade Federal de Santa Catarina, Prédio Reitoria II, R: Desembargador Vitor Lima, nº 222, sala 401
Bairro: Trindade **CEP:** 88.040-400
UF: SC **Município:** FLORIANOPOLIS
Telefone: (48)3721-6094 **E-mail:** cep.propesq@contato.ufsc.br

proporcionar mais familiaridade com o problema e torná-lo mais explícito, descrevendo princípios, casos e abordagens relacionadas ao gerenciamento de evidências e proteção e privacidade de dados. Quanto aos procedimentos técnicos, esta pesquisa é classificada como bibliográfica, com survey e experimental. Na etapa de validação do modelo será adotada a pesquisa experimental com a aplicação do modelo em um cenário real pela pesquisadora, que possibilitará a observação e identificação de melhorias durante sua utilização, além da condução de entrevistas guiadas por perguntas pré-definidas a especialistas, para avaliarem a adequação e contribuição do modelo. Como método de pesquisa este trabalho utilizará o Design Science Research – DSR. O principal resultado esperado desta pesquisa é a proposição do modelo para gerenciamento de evidências composto por componentes e princípios de proteção e privacidade de dados que apoiem em todo as operações de tratamento dos dados e que este seja adotado como referência tanto na atividade de adequação e implementação das normativas como no processo de aferição e verificação de conformidade com as mesmas.

Hipótese:

H1: As abordagens utilizadas para o gerenciamento de evidência em casos de garantia de padrões de segurança em sistemas críticos podem ser ajustadas para o contexto de proteção e privacidade de dados e contribuir também com essa temática.

H2: Considerando que, além de modelar e implementar estratégias de proteção e privacidade de dados orientadas por normativas de boas práticas, é necessário ser capaz de comprová-las, é possível afirmar que um modelo de referência para gerenciar as evidências de proteção e privacidade de dados contribui para demonstrar diligência e conformidade.

Metodologia Proposta:

A caracterização da pesquisa pode ser classificada quanto a sua: natureza, abordagem, objetivos e procedimentos. Esta pesquisa é classificada como pesquisa aplicada quanto à sua natureza e quanto à abordagem do problema, este estudo utiliza métodos mistos, sendo classificado como quantitativa e qualitativa. Do ponto de vista dos objetivos, esta pesquisa é exploratória e descritiva e quanto aos procedimentos técnicos, esta pesquisa é classificada como bibliográfica, com Survey, experimental e utilizará a observação sistemática.

Metodologia de Análise de Dados:

A avaliação do modelo será realizada por especialistas com a execução de entrevistas conduzidas pela pesquisadora. Os profissionais participantes da avaliação serão contatados por telefone e e-mail sendo estes convidados a participar da avaliação. Mediante aceitação de participação, um material contendo os conceitos necessário para o entendimento do modelo serão enviado aos participantes e o modelo será apresentado aos especialistas em reuniões virtuais individuais. Em seguida, será realizada uma entrevista semiestruturada que utilizará como instrumento de avaliação um questionário composto por 7 perguntas para a identificação do perfil do participante e 7 perguntas destinadas a avaliação do modelo. O questionário foi estruturado com perguntas fechadas, devendo em cada uma delas serem complementadas com observações e/ou sugestões proferidas pelo avaliador. As dimensões para a avaliação contemplam os seguintes critérios: escopo, profundidade e precisão, generalidade, robustez e completeza, clareza e consistência, sendo elas avaliadas com base na escala Likert de 1 a 5. Os dados resultantes da avaliação serão compilados, analisados e os ajustes das melhorias identificadas serão aplicados para a versão final do modelo para a entrega.

Estão previstos 10 participantes, que serão entrevistados.

Objetivo da Pesquisa:
Segundo os pesquisadores, no formulário de informações básicas da PB:

Objetivo Primário:

O objetivo geral desta pesquisa consiste em propor um modelo para gerenciamento de evidências de proteção e privacidade dos dados para demonstrar conformidade com normativas de referência.

Objetivo Secundário:

a) Identificar os componentes para constituir o modelo, estabelecendo os artefatos essenciais de evidências e a estrutura do modelo.

b) Analisar as abordagens utilizadas para gerenciar evidências em outras temáticas, definindo a que será adotada para o gerenciamento das evidências de proteção e privacidade de dados.
c) Elaborar o modelo para gerenciar evidências de proteção e privacidade de dados e o método de aplicação, empregando os componentes e a abordagem definida.
d) Aplicar o modelo em um estudo de caso, identificando as melhorias a serem ajustadas.
e) Validar o modelo, submetendo à apreciação de especialistas.

Avaliação dos Riscos e Benefícios:
Segundo os pesquisadores, no formulário de informações básicas da PB:

Riscos:

Pode-se citar como possíveis desconfortos e riscos decorrentes da participação, o cansaço ou aborrecimento enquanto estiver respondendo ao questionário, a interferência na sua vida cotidiana ou na sua rotina de trabalho devido a sua participação, possibilidade de sensação de coerção para participar da pesquisa ou algum constrangimento que possa ser causado decorrente da não compreensão de algumas das questões. Considera-se que os riscos apresentados são baixos pois o tempo necessário para sua participação é de uma hora e trinta minutos e a entrevista ocorrerá com profissionais atuantes em atividades de proteção e privacidade de dados que possuem conhecimento sobre o assunto. Além do que, você é livre para recusar-se a participar, retirar seu consentimento ou interromper a participação a qualquer momento, sua participação é voluntária e a recusa em participar não irá acarretar qualquer penalidade.

Benefícios:

Como benefícios pode-se citar a oportunidade de contribuir com a proposição de um modelo para apoiar os profissionais envolvidos na temática de proteção e privacidade de dados e a obtenção de conhecimentos com o recebimento da pesquisa completa logo após sua finalização.

Comentários e Considerações sobre a Pesquisa:
V. campo de conclusões.

UNIVERSIDADE FEDERAL DE SANTA CATARINA - UFSC

Continuação do Parecer: 5.330.479

Considerações sobre os Termos de apresentação obrigatória:

Folha de rosto está assinada pelo pesquisador responsável e pela coordenação do PPG ao qual a acadêmica está vinculada.

O cronograma prevê que a "avaliação do modelo com especialistas" ocorrerá a partir de 04/04/2022.

O orçamento informa que a pesquisa não terá custos (R$ 0,00).

Consta do protocolo o roteiro das entrevistas.

O TCLE está bem redigido e contempla essencialmente todas as exigências das resoluções sobre pesquisas com seres humanas.

Conclusões ou Pendências e Lista de Inadequações:

Sem pendências ou inadequações.

Considerações Finais a critério do CEP:

Este parecer foi elaborado baseado nos documentos abaixo relacionados:

Tipo Documento	Arquivo	Postagem	Autor	Situação
Informações Básicas do Projeto	PB_INFORMAÇÕES_BÁSICAS_DO_PROJETO_1874247.pdf	23/03/2022 19:47:53		Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	TCLE_Gislaine_Parra_Freund_ajustado_23_03_22.pdf	23/03/2022 19:47:11	GISLAINE PARRA FREUND	Aceito
Outros	Roteiro_Entrevista_Gislaine_Parra_Freund.pdf	03/03/2022 08:47:32	GISLAINE PARRA FREUND	Aceito
Folha de Rosto	folhaDeRosto_ajustado_assinado_03_03_22.pdf	03/03/2022 08:38:07	GISLAINE PARRA FREUND	Aceito
Projeto Detalhado / Brochura Investigador	Projeto_Gislaine_Parra_Freund.pdf	18/01/2022 10:47:35	GISLAINE PARRA FREUND	Aceito

Situação do Parecer:
Aprovado

Necessita Apreciação da CONEP:
Não

Endereço: Universidade Federal de Santa Catarina, Prédio Reitoria II, R: Desembargador Vitor Lima, nº 222, sala 401
Bairro: Trindade **CEP:** 88.040-400
UF: SC **Município:** FLORIANOPOLIS
Telefone: (48)3721-6094 **E-mail:** cep.propesq@contato.ufsc.br

UNIVERSIDADE FEDERAL DE SANTA CATARINA - UFSC

Continuação do Parecer: 5.330.479

FLORIANOPOLIS, 04 de Abril de 2022

Assinado por:
Luciana C Antunes
(Coordenador(a))

Endereço: Universidade Federal de Santa Catarina, Prédio Reitoria II, R: Desembargador Vitor Lima, nº 222, sala 401
Bairro: Trindade **CEP:** 88.040-400
UF: SC **Município:** FLORIANOPOLIS
Telefone: (48)3721-6094 **E-mail:** cep.propesq@contato.ufsc.br

APÊNDICE H – TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO (TCLE)

Universidade Federal de Santa Catarina
Programa de Pós-Graduação em Ciência da Informação
Campus Professor João David Ferreira Lima – Trindade – Florianópolis – Santa Catarina – Brasil – CEP: 88.040-900

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Você está sendo convidado(a) como voluntário(a) a participar de uma das etapas da pesquisa entitulada **"MODELO DE GERENCIAMENTO DE EVIDÊNCIAS PARA COMPROVAR ALEGAÇÕES DE SEGURANÇA E PRIVACIDADE DE DADOS"**. Esta pesquisa está associada à tese de doutorado de Gislaine Parra Freund, aluna do Programa de Pós-graduação em Ciência da Informação da Universidade Federal de Santa Catarina sob a orientação do Prof. Dr. Douglas Dyllon Jeronimo de Macedo.

O objetivo do estudo que está sendo desenvolvido é propor um modelo para gerenciar evidências e auxiliar na validação de requisitos e controles relacionados à proteção e privacidade de dados.

A etapa que você está sendo convidado(a) a participar faz parte da avaliação do modelo que está sendo proposto, a qual pretende verificar se o mesmo, sob a ótica de especialistas na área de proteção e privacidade de dados, é passível de ser utilizado para gerenciamento de evidências e se pode contribuir para a melhoria do processo de comprovação de conformidade com requisitos de proteção e privacidade de dados.

A avaliação do modelo será realizada por meio de entrevista guiada por questões estabelecidas pela pesquisadora, a serem respondidas com base nas práticas adotadas por esses profissionais especialistas. Desta forma, a sua participação consistirá em responder perguntas de um roteiro de entrevista/questionário à pesquisadora do projeto. Será assegurado à você todo o acompanhamento e assistência, caso tenha alguma dúvida no entendimento das questões, sobre os procedimentos ou sobre a pesquisa. A entrevista poderá ocorrer presencial em local a combinar com o entrevistado ou por vídeo conferência, sendo em ambos os casos gravada, para posterior análise da pesquisadora. A gravação é parte condicionante para participação da entrevista e deverá estar explicitamente autorizada no final deste documento. A entrevista será transcrita para o trabalho e permanecerá armazenada em arquivos digitais em local seguro, sendo acessada única e exclusivamente pelo pesquisador e pelo seu professor orientador para fins de análise dos resultados.

Como benefícios de sua participação nesta pesquisa, pode-se citar a oportunidade de contribuir com a proposição de um modelo para apoiar os profissionais envolvidos na temática de proteção e privacidade de dados e a obtenção de conhecimentos com o recebimento da pesquisa completa logo após sua finalização.

Por outro lado, pode-se citar como possíveis desconfortos e riscos decorrentes da sua participação, o cansaço ou aborrecimento enquanto estiver respondendo ao questionário, a interferência na sua vida cotidiana ou na sua rotina de trabalho devido a sua participação, possibilidade de sensação de coerção para participar da pesquisa ou algum constrangimento que possa ser causado decorrente da não compreensão de algumas das questões. Considera-se que os riscos apresentados são baixos pois o tempo necessário para sua participação é de uma hora e trinta minutos e a entrevista ocorrerá com profissionais atuantes em atividades de proteção e privacidade de dados que possuem conhecimento sobre o assunto. Além do que, você é livre para recusar-se a participar, retirar seu consentimento ou interromper a participação a qualquer momento, sua participação é voluntária e a recusa em participar não irá acarretar qualquer penalidade.

Em atenção aos requisitos do Código de Ética da pesquisa científica, lhe é assegurado que não será revelado o seu nome ou qualquer informação relacionada à sua privacidade. Os resultados deste trabalho poderão ser apresentados em congressos ou submetidos à revistas científicas, ressaltando-se que serão apresentados somente os resultados obtidos, sem revelar qualquer informação que venha a comprometer o sigilo aos seus dados.

Ressalta-se que após a conclusão dos estudos e a finalização do projeto será enviada para você uma cópia da tese contendo o modelo proposto, bem como as diretrizes para a sua aplicação.

O pesquisador responsável, compromete-se a conduzir a pesquisa de acordo com o que preconiza a Resolução 466/12 de 12/06/2012, que trata dos preceitos éticos e da proteção aos participantes da pesquisa.

Declaro que fui informado(a) dos objetivos da pesquisa acima de maneira clara e detalhada e esclareci minhas dúvidas. Sei que em qualquer momento poderei solicitar novas informações ou declinar da minha decisão em participar, se assim o desejar. A pesquisadora Me. Gislaine Parra Freund e o professor orientador Prof. Dr. Douglas Dyllon Jeronimo de Macedo certificaram-me de que todos os dados desta pesquisa serão confidenciais.

Em caso de dúvidas poderei contatar a pesquisadora Me. Gislaine Parra Freund no telefone (48) 99967-5454 ou pelo e-mail gislaineparraf@gmail.com, o professor orientador Prof. Dr. Douglas Dyllon Jeronimo de Macedo no telefone (48) 3721 - 3548 ou pelo e-mail douglas.macedo@ufsc.br, ou o Comitê de Ética em Pesquisa com Seres Humanos (CEPSH) da Universidade Federal de Santa Catarina (UFSC), sito à Rua Desembargador Vitor Lima, nº 222, sala 401, Trindade – Florianópolis, SC. Telefone (48)3721-6094 ou e-mail cep.propesq@contato.ufsc.br. O CEPSH é um órgão colegiado interdisciplinar, deliberativo, consultivo e educativo, vinculado à Universidade Federal de Santa Catarina, mas independente na tomada de decisões, criado para defender os

interesses dos participantes da pesquisa em sua integridade e dignidade e para contribuir no desenvolvimento da pesquisa dentro de padrões éticos.

[ ] Declaro que concordo em participar deste estudo. Recebi uma cópia deste termo de consentimento livre e esclarecido e me foi dada a oportunidade de ler e esclarecer as minhas dúvidas.

[ ] Declaro que concordo em gravar a entrevista realizada comigo e estou de acordo com as condições de uso das mesmas, descritas neste documento

APÊNDICE I – QUESTIONÁRIO DE AVALIAÇÃO DO COM.PRIVACY

Etapa 1 – Perfil dos Participantes	
Qual é a sua idade?	( ) entre 20 e 30 anos ( ) entre 31 e 40 anos ( ) entre 41 e 50 anos ( ) entre 51 e 60 anos ( ) mais do que 61 anos
Em que cidade e estado você reside:	
Qual a sua maior formação acadêmica?	( ) Pós-Doutorado ( ) Doutorado ( ) Mestrado ( ) Especialização
Qual a função profissional que desempenha atualmente?	
Qual o tempo que desempenha a atual função na carreira profissional?	( ) entre 01 e 05 anos ( ) entre 06 e 10 anos ( ) entre 11 e 15 anos ( ) entre 16 e 20 anos ( ) mais do que 21 anos
Quantos projetos você já participou na área de segurança e privacidade de dados.	( ) menos do que 3 projetos ( ) entre 4 e 10 projetos ( ) mais do que 10 projetos

Etapa 2 – Avaliação do Modelo				
Critérios	Questões	1	2	3
Escopo	**Q1.** O modelo abrange o campo de conhecimento necessário para estruturar o processo de gerenciamento de evidências no âmbito da segurança e privacidade de dados.			
OBS:				
Profundidade e Precisão	**Q2.** O nível de detalhamento do modelo (etapas, atividades e tarefas) é adequado e suficiente para comprovar uma alegação de segurança e privacidade com o gerenciamento de evidências.			
OBS:				
Generalidade	**Q3.** O modelo, da forma em que foi estruturado, possibilita sua aplicação em diferentes setores e negócios, considerando as especificidades de cada segmento.			
OBS:				
Robustez e Completeza	**Q4.** O modelo é abrangente o suficiente e apresenta os componentes necessários para sustentar uma alegação de segurança e privacidade de dados.			
OBS:				
Clareza	**Q5.** O modelo é facilmente entendido e fácil de ser aplicado.			
OBS:				

Consistência	**Q6.** O modelo apresenta coerência nas bases estruturantes adotadas (*Privacy by Design*, ISO 29100 e operações de tratamento de dados) e em suas etapas, provendo informações consistentes que apoiam a comprovação de alegações de segurança e privacidade de dados.			
OBS:				
Contribuição/ Recomendação	**Q7.** Considerando as opções de modelos/métodos/metodologias existentes, recomendo a adoção do modelo de gerenciamento de evidências apresentado, pois o mesmo apresenta grande contribuição na comprovação de requisitos e alegações de segurança e privacidade de dados.			
OBS:				