em questão
E-ISSN 1808-5245

Proteção e privacidade de dados: um modelo para o gerenciamento de evidências

Gislaine Parra Freund[1]

[1]Universidade Federal de Santa Catarina, Florianópolis, SC, Brasil;
gislaineparraf@gmail.com; ORCID https://orcid.org/0000-0002-2402-124X

Douglas Dyllon Jeronimo de Macedo[1]

[1]Universidade Federal de Santa Catarina, Florianópolis, SC, Brasil;
douglas.macedo@ufsc.br; ORCID https://orcid.org/0000-0002-3237-4168

Priscila Basto Fagundes[1]

[1]Universidade Federal de Santa Catarina, Florianópolis, SC, Brasil;
priscila.bfagundes@gmail.com; ORCID https://orcid.org/0000-0002-9461-311X

Resumo: As legislações e as normativas relacionadas à proteção e à privacidade de dados apresentam os requisitos a que organizações, processos, produtos e ambientes precisam atender para serem considerados seguros. Dentre os requisitos preconizados, destacam-se os de "Responsabilização" e "Conformidade com a privacidade", os quais definem que as organizações devem ser responsáveis e capazes de demonstrar conformidade com as leis e as normas vigentes. Além do desafio de implementar tais requisitos, é necessário adotar processos sistematizados que comprovem como e em quais evidências esses requisitos são validados. Este artigo apresenta um modelo denominado COM.PRIVACY para gerenciar evidências de proteção e privacidade de dados e para demonstrar diligência e conformidade com normativas de boas práticas. Foi utilizado o Design Science Research como método de pesquisa para a proposição do modelo. Para a sua validação, o COM.PRIVACY foi aplicado em uma organização que possibilitou a observação e a identificação de melhorias durante a sua utilização, sendo a sua avaliação feita por um grupo de especialistas. Concluiu-se que o modelo apoia a validação e a comprovação de conformidade com requisitos de proteção e privacidade de dados em todas as operações de tratamento de dados, podendo ser adotado tanto na atividade de adequação e implementação das normativas, no processo de aferição e verificação de conformidade com essas normas, assim como na promoção da transparência do tratamento de dados aos seus titulares.

Palavras-chave: proteção de dados; privacidade de dados; gerenciamento de evidências; segurança da informação

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 de Tecnologias de Informação e Comunicação (TICs) vêm conduzindo a dinâmica mundial na era digital; e esse cenário estruturado a partir de dados remodela diferentes áreas de negócio, apresenta necessidades particulares e abre novas frentes de estudos relacionados a arquitetura, armazenamento, recuperação, segurança e proteção de dados. 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".

Nesse contexto, Lima e Presser (2022, p. 110) apresentam os ambientes de Big Data, nos quais "[...] softwares e computadores foram produzidos para processar grandes quantidades de dados e, assim, convertê-los em vantagens competitivas informacionais". Esses ambientes também trazem consigo grandes desafios no que se refere a controles de segurança na gestão desses dados para prover a sua proteção e uso adequado.

Para Isaak e Hanna (2018), os dados pessoais e as informações corporativas coletadas pelas organizações são submetidos a diferentes níveis de controle de segurança, variando de acordo com a sua atuação e as regulamentações aplicáveis a cada uma delas.

Já sob a perspectiva dos titulares dos dados, os inúmeros cadastros realizados em plataformas digitais com dados pessoais dificultam o controle. Para Sousa, Barrancos e Maia (2019, p. 242), o uso de dados como instrumento para o consumo de recursos "[...] ocasiona a denominada assimetria informacional em que o aumento da quantidade de dados reduz o conhecimento dos cidadãos principalmente sobre o uso dos mesmos".

Diante da relevância e da 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.

A lei propulsora da 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 tenham leis equivalentes às suas para transacionar dados pessoais, tal como 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 essa modalidade de privacidade digital e equivalência à GDPR (Facchini Neto; Demoliner, 2018).

Outro ponto a ser observado é o aspecto social envolvido nesta legislação, visto que o titular do dado é o sujeito protegido pela Lei. Dessa forma, se por um lado está o direito do cidadão pela proteção e pela privacidade de seus dados, de outro a necessidade de adequação às normativas e às legislações demanda a implementação de boas práticas que envolvem desde a cautela e a autorização na coleta dos dados até a proteção e a garantia de exclusão desses dados.

Dentre essas práticas, destacam-se a provisão, a organização e a manutenção de evidências de conformidade concretas que possam ser utilizadas para comprovar a diligência e a conformidade com normativas e fontes regulatórias. Essas práticas estão associadas aos requisitos de "Responsabilização" e "Conformidade com a privacidade", também previstos nas legislações e nas normativas, os quais são o foco de estudo desta pesquisa.

A temática "evidências" é adotada em diversos contextos, tais como contabilidade, cibersegurança, qualidade, entre outros, devendo em todos eles, sendo elas físicas ou digitais, ser suficientes e adequadas para serem apresentadas em auditorias de qualquer natureza, tanto para fins de certificações quanto para atendimento a órgãos reguladores ou clientes e fornecedores. 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.

Diante do exposto, este artigo tem como objetivo apresentar a proposta de um modelo denominado COM.PRIVACY para gerenciamento de evidências de proteção e privacidade de dados, atendimento às normativas de referência e

auxílio na atividade de comprovação de conformidade com essas normas. Pretende-se que o modelo seja utilizado na tutela do direito à proteção e à privacidade de dados e contribua com o processo de adequação de cenários às normativas de proteção e privacidade de dados, elevando assim a capacidade de comprovação do tratamento de dados pessoais.

Com base na obrigatoriedade de proteção e privacidade de dados por força de lei e na importância de estudos que apresentem abordagens para gerenciar evidências que validem os requisitos de proteção e privacidade de dados às normativas, elaborou-se a seguinte questão de pesquisa como elemento principal de investigação: 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?

Este artigo apresenta, em sua seção 2, a base teórica utilizada para a proposição do modelo, que envolve o Privacy by Design (PbD), a ISO 29100 e as operações de tratamento de dados. A seção 3 exibe as etapas da pesquisa e as atividades realizadas para a construção do COM.PRIVACY. A seção 4 demonstra a estrutura do modelo, bem como as diretrizes para a sua aplicação. A seção 5 mostra os resultados da avaliação do COM.PRIVACY realizada por um conjunto de especialistas da área de segurança de dados e informação. E, por fim, a seção 6 apresenta as conclusões da pesquisa desenvolvida.

2 Referencial teórico

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

2.1 Privacy by Design

Privacy by Design é um conceito desenvolvido nos anos 1980 por Ann Cavoukian, comissária de proteção de dados de Ontário, Canadá, para ser aplicado

em TICs, práticas organizacionais, estruturas físicas e 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 regulatórias; em vez disso, a garantia de privacidade deve, idealmente, tornar-se o modo de operação padrão de uma organização (Cavoukian, 2009, p. 1).

Cavoukian definiu sete princípios fundamentais do PbD, são eles:

a) ser proativo e não reativo - ser preventivo e não corretivo;
b) privacidade como padrão;
c) privacidade incorporada ao design;
d) funcionalidade completa - soma positiva, não soma zero;
e) segurança de ponta a ponta - proteção completa no ciclo de vida;
f) visibilidade e transparência; e
g) respeito pela privacidade do usuário.

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

Nesta pesquisa os princípios do PbD propostos por Cavoukian (2009) foram personalizados e consolidados em quatro princípios norteadores, sendo eles: (1) segurança e privacidade atuando em universos complementares; (2) segurança e privacidade de ponta a ponta, atuante em todas as operações de tratamento de dados; (3) segurança e privacidade da concepção do produto/serviço/processo à comprovação de uma alegação; e (4) transparência e foco no titular dos dados.

2.2 ISO 29100

Para a elaboração do modelo COM.PRIVACY, buscou-se identificar como referência normativa uma estrutura para a proteção de dados com base em conceitos alinhados mundialmente que pudessem ser aplicados juntamente com diferentes legislações e com características neutras quanto a soluções tecnológicas. A ISO 29100 traz essas características e reforça que, devido ao crescente número de tecnologias que processam dados pessoais, é importante se ter normas de segurança da informação que forneçam uma base de entendimento comum para a proteção desses tipos de dados. A norma acrescenta que é indispensável assegurar a privacidade, e estar conforme com as diversas leis pode ser uma tarefa difícil para as organizações.

Dentre os seus objetivos, a ISO 29100 se propõe a apoiar o desenho, a implementação, a operação e a manutenção de sistemas de TIC no tratamento e na proteção de dados pessoais e incentivar soluções inovadoras para protegê-los, padronizando a privacidade e fornecendo uma base para uma arquitetura técnica de referência; para a implementação e o uso de tecnologias de privacidade; e para a gestão geral de privacidade e especificações de engenharias.

No que se refere ao seu escopo, a ISO 29100 é aplicável às pessoas naturais e às organizações envolvidas em especificação, aquisição, arquitetura, concepção, desenvolvimento, teste, manutenção, administração e operação de sistemas de TIC, ou ainda, em serviços em que controles de privacidade são necessários para o tratamento de dados pessoais (ABNT, 2020, p. 1). Em relação aos seus princípios, a ISO 29100 apresenta os seguintes: Consentimento e escolha; Legitimidade e especificação do objetivo; Limitação de coleta; Minimização de dados; Limitação de uso, retenção e divulgação; Precisão e qualidade; Abertura, transparência e notificação; Acesso e participação individual; Responsabilização; Segurança da informação; e *Compliance* com a privacidade.

A ISO 29100, a partir de um entendimento comum sobre proteção e privacidade de dados, fornece uma estrutura abordando aspectos organizacionais

e técnicos, os quais podem orientar empresas na implementação de requisitos e controles de proteção e privacidade de dados.

2.3 Operações de tratamento de dados

As operações de tratamento de dados referem-se às ações realizadas com os dados. Para a definição dessas operações a serem adotadas no modelo COM.PRIVACY, foram analisadas as operações de tratamento indicadas na ISO 29100, na GDPR e na LGPD.

A ISO 29100 traz, em seu item 2.21, a seguinte definição para tratamento de dados pessoais: "[...] operação ou conjunto de operações realizadas sobre dados pessoais (DP) [...]" (ABNT, 2020, p. 1). Em nota, apresenta exemplos de operações de tratamento de DP, sendo elas: coleta, armazenamento, alteração, recuperação, consulta, divulgação, anonimização, pseudoanonimização, disseminação ou disponibilização, exclusão ou destruição de dados pessoais.

O artigo 5° da LGPD afirma que o 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 (Brasil, 2018).

Por sua vez, a GDPR, em seu art. 4°, 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 registro, 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 (European Union, 2016).

Observa-se que não há um consenso entre as operações no que se refere às suas nomenclaturas, sendo assim, a partir da análise realizada nos três artefatos,

foram definidas as nove operações de tratamento de dados a serem utilizadas no modelo proposto:

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, a alteração, a ocultação (anonimização, pseudoanonimização, criptografia);
h) reutilização: ato do reúso, ou seja, reutilizar os dados para outros fins para os quais foram coletados; e
i) descarte: ato de eliminar/excluir/destruir os dados.

Ressalta-se que, para a utilização do COM.PRIVACY, foi necessário adotar um conjunto de operações de tratamento de dados que contemplasse desde a coleta até o seu descarte. As operações de tratamento apresentadas são 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.

3 Procedimentos metodológicos

Para a proposição do COM.PRIVACY, optou-se pela adoção do método Design Science Research (DSR). 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).

Pelo cunho prático do modelo proposto, considera-se que esta pesquisa está alinhada aos propósitos do DSR, uma vez que se propõe a desenvolver um artefato inovador para gerenciar evidência de proteção e privacidade de dados e dar suporte na comprovação de conformidade com as normativas de referência sobre o tema. O detalhamento de cada uma das etapas desenvolvidas é apresentado a seguir.

3.1 Etapa 1: identificar o problema e a motivação

Com base na literatura sobre proteção e privacidade de dados, 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 esses requisitos podem ser validados. Dessa forma, buscou-se sistematizar um modelo de gerenciamento de evidências de proteção e privacidade de dados que apoie a comprovação de alegações referentes a essa temática.

3.2 Etapa 2: definir objetivos e solução

Diante dos problemas identificados, foi definido como objetivo desta pesquisa propor um modelo e adequar as abordagens de gerenciamento de evidências em casos de garantia para que possam ser utilizadas no âmbito de proteção e privacidade de dados e auxiliar na validação de requisitos e controles.

3.3 Etapa 3: projetar e desenvolver o artefato

Nesta etapa foram realizadas as seguintes atividades: (a) definição das camadas de atuação do modelo; (b) definição dos requisitos de privacidade e do fluxo de atividades para a identificação dos demais requisitos e pré-requisitos que irão compor o modelo; (c) 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; (d) definição das operações de tratamento de dados que irão compor o modelo COM.PRIVACY e proposição de um questionamento para orientar a construção da matriz que apresenta as relações existentes entre os requisitos (princípios) e as operações de tratamento; (e) criação de um método para identificar/coletar evidências e a sua organização; (f) realização de estudos e análises das abordagens de gerenciamento de evidências de casos de garantia, aplicadas no âmbito de sistema e em demais cenários; (g) criação de um método para o gerenciamento de evidências do modelo; (h) desenvolvimento do modelo descrevendo cada componente definido; (i) descrição das estratégias de gerenciamento propostas para uso; e (j) criação e descrição das orientações de implantação e da forma de aplicação do modelo.

3.4 Etapa 4: demonstrar o artefato

Para validar o COM.PRIVACY e verificar se as contribuições que podem ser obtidas com o 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 a LGPD e necessitam de ações seguras e com privacidade em seu tratamento. A aplicação do modelo nesse contexto oportunizou a sua avaliação em um cenário que tem a necessidade real e constante de comprovar conformidade com normativas.

Durante a aplicação do modelo, foram observadas e analisadas as seguintes questões: (a) pertinência dos princípios e das nomenclaturas definidas para o modelo; (b) adequação das ações sugeridas em cada uma das camadas; (c) pertinência da abordagem definida para gerenciar as evidências; (d) sugestões e opiniões obtidas e/ou percebidas durante a aplicação do modelo; (e) problemas ou dificuldades enfrentadas.

3.5 Etapa 5: avaliar o artefato

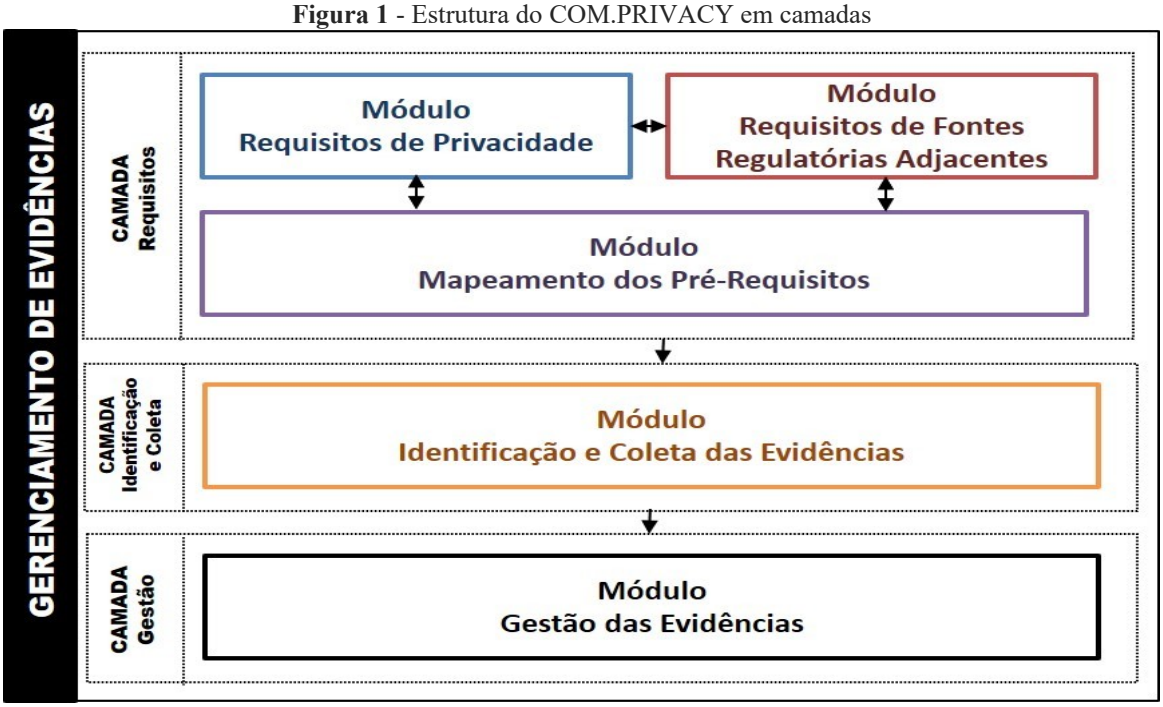
A avaliação do COM.PRIVACY foi realizada por um conjunto de especialistas por meio do método Painel de Especialistas. O modelo foi apresentado aos

especialistas em reuniões virtuais individuais. O instrumento de avaliação do modelo constituiu-se de um questionário em formato digital com perguntas fechadas, sendo disponibilizada em cada uma delas uma questão para observações e/ou sugestões. Os dados resultantes da avaliação foram compilados e analisados, sendo os ajustes das melhorias aplicados na versão final do modelo.

4 COM.PRIVACY

Com o objetivo de segmentar as etapas e as atividades, o modelo COM.PRIVACY foi estruturado seguindo o fluxo em *top-down,* em três camadas, sendo elas: (1) uma para atividades relacionadas aos requisitos a serem atendidos, (2) outra referente à identificação e à coleta de evidências e (3) outra destinada à gestão das evidências. A Figura 1 ilustra a estrutura do modelo em camadas.

Figura 1 - Estrutura do COM.PRIVACY em camadas



Fonte: Dados da pesquisa.

4.1 Camada de requisitos

Nesta camada são tratados os requisitos de conformidade com a proteção e a privacidade de dados e demais fontes relacionadas que apresentam interferência

sobre eles e às quais se pretende atender. Nesse contexto, requisitos são todas as condições necessárias para satisfazer o objetivo de proteger e garantir a privacidade de dados, considerando as normativas de referência.

Os requisitos identificados de proteção e privacidade de dados devem ser observados e atendidos aplicando o conceito de Privacy by Design – privacidade desde a geração de novos serviços, produtos e processos. Com o intuito de segmentar e facilitar a identificação dos requisitos, esta camada foi dividida em três módulos: Requisitos de Privacidade, Requisitos de Fontes Regulatórias Adjacentes e Mapeamento dos Pré-Requisitos.

4.1.1 Módulo requisitos de privacidade

Para clarificar a aderência da ISO 29100 às Leis GDPR e LGPD, foi realizado um estudo de correlação entre os requisitos de ambas as leis, sendo adotados, como requisitos primários de proteção e privacidade de dados para este modelo, os 11 princípios apresentados pela ISO 29100, sendo eles: Consentimento e escolha; Legitimidade e especificação do objeto; Limitação da coleta; Minimização de dados; Limitação de uso, retenção e divulgação; Precisão e qualidade; Abertura, transparência e notificação; Acesso e participação individual; Responsabilização; Segurança da informação; e Conformidade com a privacidade.

4.1.2 Módulo requisitos de fontes regulatórias adjacentes

Este módulo se destina 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, trazem, em seu conteúdo, exigências relacionadas a alguma das operações de tratamento de dados. 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 de dados e precisam ser atendidos. Para a realização das buscas de requisitos nos artefatos adjacentes, os termos relacionados aos requisitos da ISO 29100 e as operações de tratamento de dados

apresentados devem ser utilizados como referência.

4.1.3 Módulo mapeamento dos pré-requisitos

Os requisitos primários abordados anteriormente retratam as condições determinantes para a conformidade que se busca alcançar, porém, para que essas sejam atendidas, é necessário mapear os pré-requisitos essenciais para que os primários sejam cumpridos satisfatoriamente. Para isso, os documentos dos quais os requisitos primários foram extraídos devem ser analisados minuciosamente em busca desses pré-requisitos, utilizando os requisitos primários como guia para as buscas.

4.2 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 àquelas 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, organograma, fluxo de dados, arquitetura de redes, entre outras.

Já as evidências dinâmicas são aquelas modificadas com frequência e extraídas o mais recente possível de sua apresentação, como, por exemplo, arquivos de CFTV, imagens, registros de ponto, entre outras. Tanto para os requisitos quanto para as evidências, o modelo disponibiliza formulários e questões que atuam como um guia para os registros, os quais proporcionam um mapeamento das características de cada artefato a ser utilizado como evidência e possibilitam que esses artefatos sejam catalogados, modelados e gerenciados na camada do modelo seguinte.

Para identificar e coletar as evidências, o modelo adota dois instrumentos de apoio, são eles: (1) a matriz que relaciona as operações de tratamento de dados com os requisitos de privacidade, apresentada na Figura 2, e (2) a abordagem em perspectivas, apresentada na Figura 3.

Figura 2 - Matriz análise das etapas do ciclo de tratamento com os requisitos de proteção e privacidade de dados

Requisitos / Oper. de Tratamento	1	2	3	4	5	6	7	8	9	10	11	12	13
Coleta	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Armazenamento	-	-	-	-	☑	☑	-	-	☑	☑	☑	☑	☑
Acesso	-	-	-	-	☑	☑	☑	☑	☑	☑	☑	☑	
Compartilhamento	-	-	-	-	☑	-	-	-	☑	☑	☑		
Transferência	-	-	-	-	☑	-	-	-	☑	☑	☑		
Divulgação	-	-	-	-	☑	-	-	-	☑	☑	☑		
Processamento	-	-	-	-	-	☑	☑	☑	☑	☑	☑		☑
Reutilização	☑	☑	☑	☑	☑	-	-	-	☑	☑	☑	☑	☑
Representação	-	☑	-	☑	☑	-	-	-	☑	☑	☑		
Descarte	-	-	-	-	☑	-	☑	☑	☑	☑	☑	☑	

1 – Consentimento e escolha
2 – Legitimidade e especificação 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

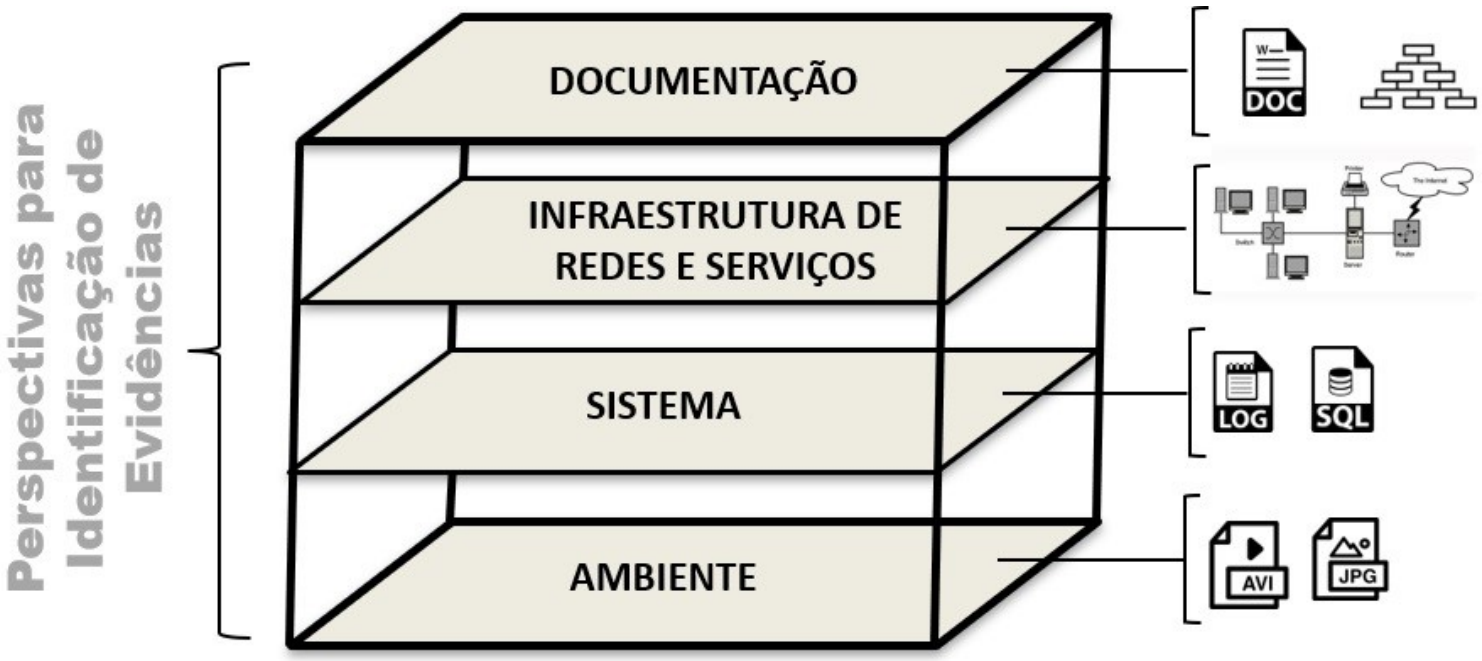
Fontes Regulatórias Adjacentes

Fonte: Dados da pesquisa.

Para a identificação e a coleta de evidências, essa matriz é utilizada como guia. Utilizam-se também os pré-requisitos para complementar o entendimento e consideram-se as ações implementadas em cada um deles em busca de resposta ao seguinte questionamento: Q.1 - Qual(is) é(são) o(s) artefato(s) a ser(em) utilizado(s) como evidência para cada ponto de intersecção da matriz sinalizada com ☑?

Cada resposta a essa questão resulta nas possibilidades de extração de artefatos provenientes dos controles implementados. Para facilitar a identificação das evidências em resposta à Q.1, optou-se por segmentar a análise em perspectivas, conforme apresentado na Figura 3.

Figura 3 - Perspectivas para a identificação de evidências



Fonte: Dados da pesquisa.

4.3 Camada de gestão das evidências

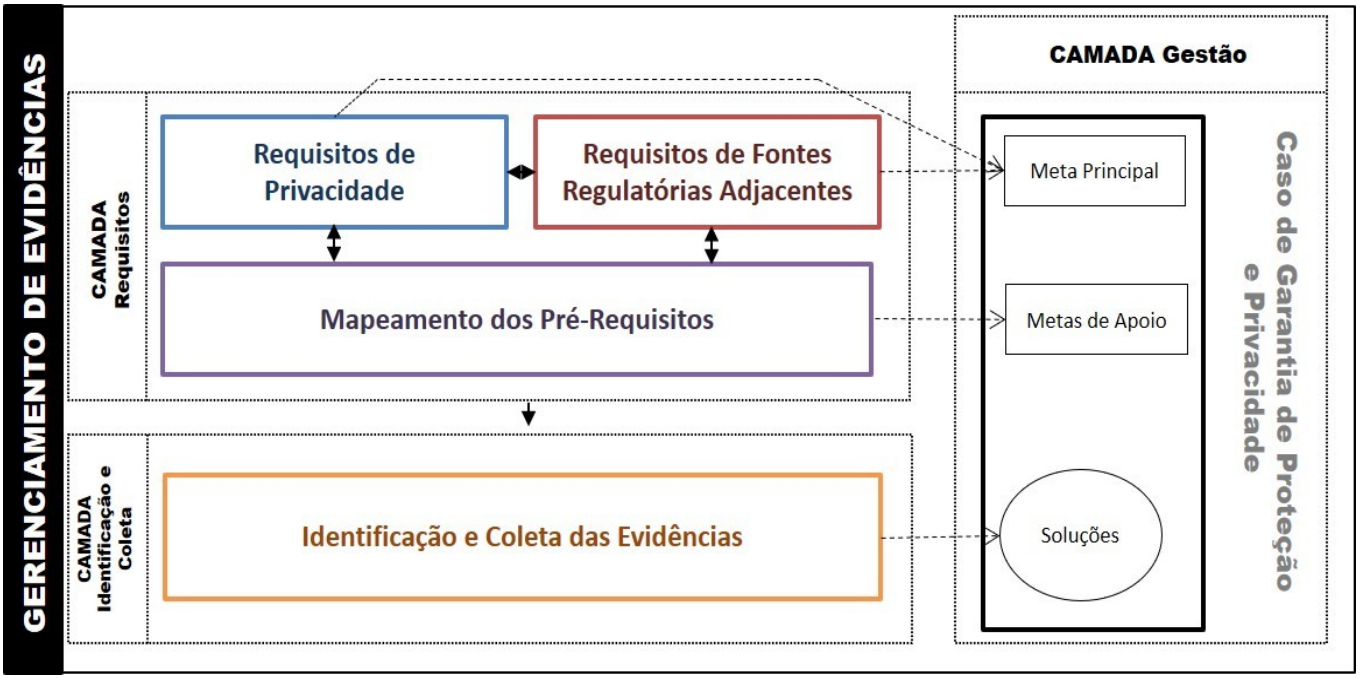
Para representar a conformidade e gerir as evidências, optou-se por adotar, como notação para a representação gráfica, a modelagem de um caso de garantia de privacidade. Para OMG (2020), casos de garantia consistem em uma coleção de afirmações auditáveis, argumentos e evidências criadas para apoiar a alegação de que um sistema/serviço irá satisfazer os seus requisitos de garantia.

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, com vistas a comprovar a aderência aos requisitos de privacidade preconizados na normativa de referência ISO 29100 com o uso da Goal Structuring Notation (GSN). 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, independentemente da nomenclatura utilizada.

Para definir a estrutura do caso de garantia de privacidade, buscou-se

correlacionar as camadas propostas no modelo com os elementos da GSN, conforme apresentado na Figura 4.

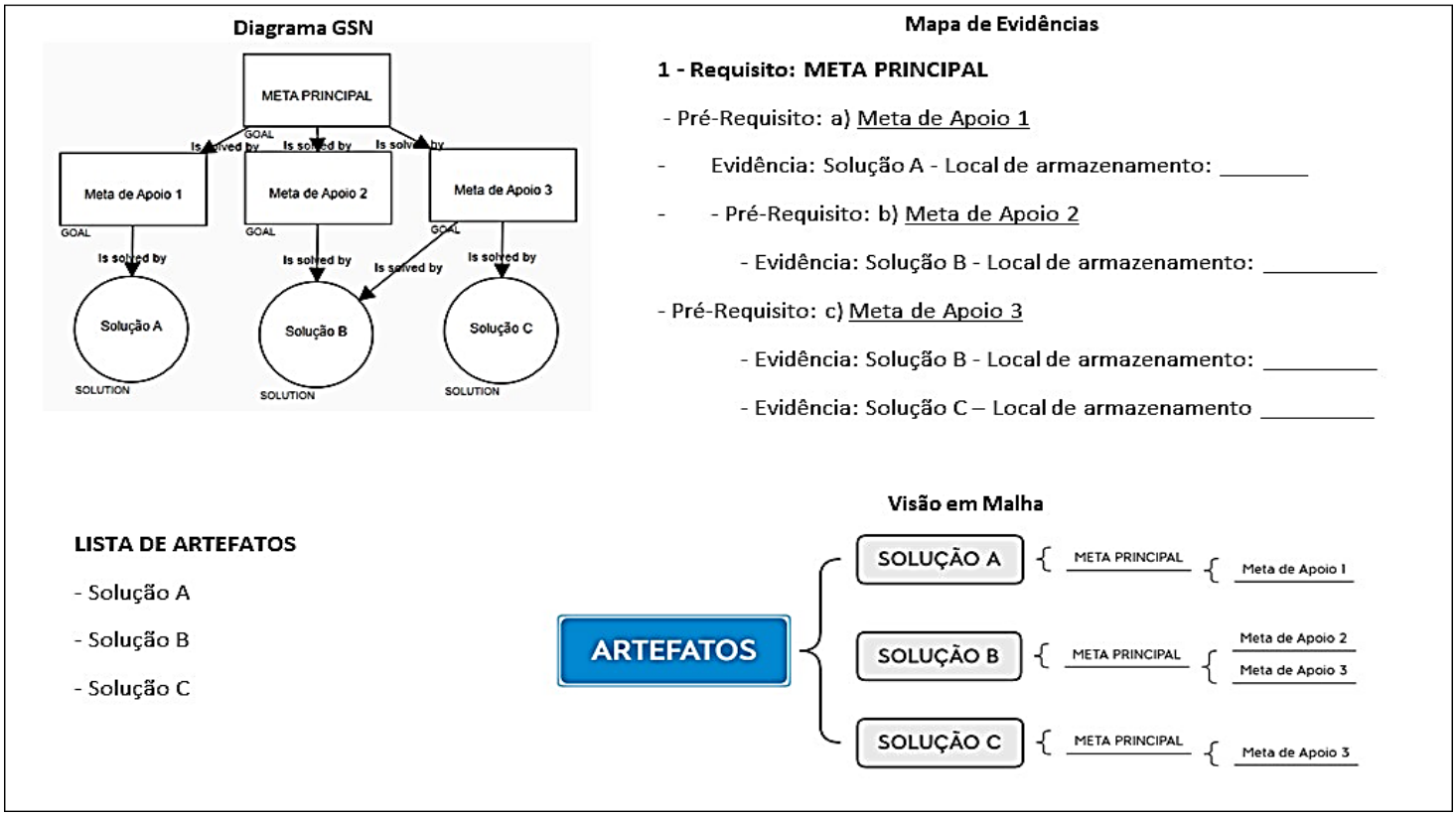
Figura 4 - Correlação das camadas do modelo para a formação do caso de garantia de privacidade



Fonte: Dados da pesquisa.

Os Módulos Requisitos de Privacidade e Requisitos de Fontes Regulatórias Adjacentes, pertencentes à camada de requisitos, irão compor as metas principais do caso de garantia. As saídas do Módulo Mapeamento dos Pré-Requisitos irão compor as metas de apoio e as saídas da camada de Identificação e Coleta das Evidências constituirão as soluções. Para facilitar a visualização, o caso de garantia proposto aqui foi segmentado em visões. A Figura 5 elucida as visões contempladas pelo modelo.

Figura 5 - Visões do caso de garantia de privacidade

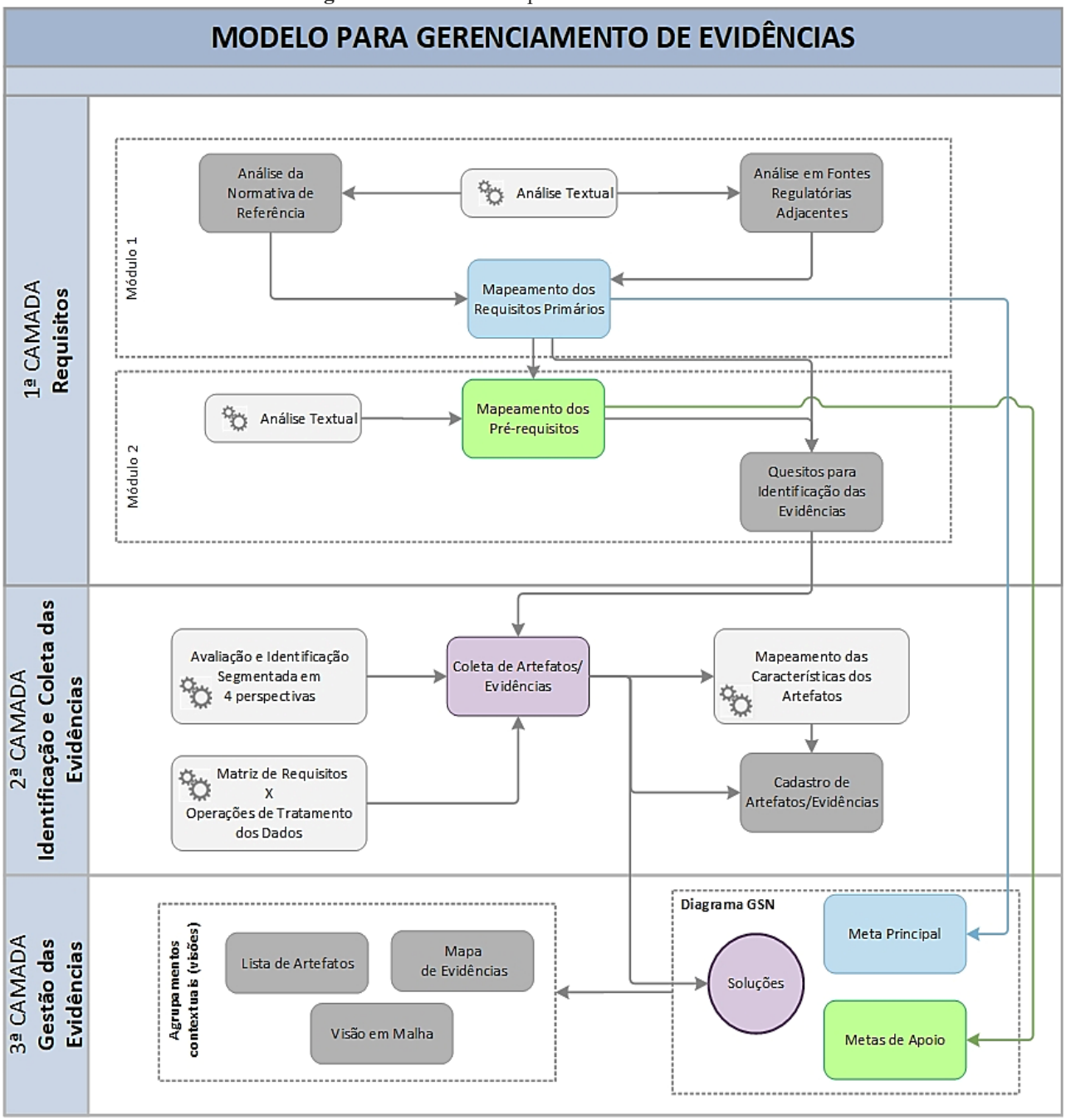


Fonte: Dados da pesquisa.

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 completa proposta para o COM.PRIVACY pode ser observada na Figura 6.

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

Figura 6 - Estrutura completa do COM.PRIVACY



Fonte: Dados da pesquisa.

5 Avaliação do COM.PRIVACY

Para testar as suas funcionalidades e consolidar as etapas e os produtos resultantes do COM.PRIVACY, ele foi aplicado e avaliado na instituição Casacaresc – uma operadora de plano de saúde com 12.096 beneficiários – no processo de Adesão

de Beneficiários.

Esta seção apresenta os resultados de uma avaliação realizada com especialistas da área de segurança da informação, proteção e privacidade de dados para validar o COM.PRIVACY. A avaliação foi realizada utilizando o método Painel de Especialistas (Rocha; Honorato; Costa, 2016) 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 observadas 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); e
g) verificar se, na visão dos especialistas entrevistados, o COM.PRIVACY contribui com o contexto de proteção e privacidade de dados com a sua abordagem em gerenciamento de evidências e se eles recomendariam o uso do modelo (contribuição/recomendação).

5.1 Planejamento e preparação da avaliação

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

Dada a natureza dos objetivos definidos para a avaliação do COM.PRIVACY, foi elaborado um questionário contendo uma questão para cada um dos objetivos definidos para avaliação:

a) Q1. [ESCOPO] o modelo abrange o campo de conhecimento necessário para estruturar o processo de gerenciamento de evidências no âmbito de segurança e privacidade de dados;
b) Q2. [PROFUNDIDADE E PRECISÃO] 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;
c) Q3. [GENERALIDADE] omodelo, da forma como foi estruturado, possibilita a sua aplicação em diferentes setores e negócios, considerando as especificidades de cada segmento;
d) Q4. [ROBUSTEZ E COMPLETEZA] o modelo é abrangente o suficiente e apresenta os componentes necessários para sustentar uma alegação de segurança e privacidade de dados;
e) Q5. [CLAREZA] o modelo é facilmente entendido e fácil de ser aplicado;
f) Q6. [CONSISTÊNCIA] 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;
g) Q7. [CONTRIBUIÇÃO/RECOMENDAÇÃO] considerando as opções de modelos/métodos/metodologias existentes, recomenda a adoção do modelo de gerenciamento de evidências apresentado, pois ele oferece grande contribuição na comprovação de requisitos e alegações de segurança e privacidade de dados.

Os especialistas tiveram a oportunidade de qualificar a sua resposta de acordo com a escala Likert – 1 Discordo, 2 Nem discordo, nem concordo e 3 Concordo –, além de dispor de um campo para eventuais observações.

5.2 Aplicação da avaliação do COM.PRIVACY

A avaliação teve a participação de seis especialistas e foi realizada de forma individual. Antes do seu início, foi realizada uma apresentação contendo uma explicação sobre o COM.PRIVACY, o seu funcionamento e as etapas para a sua aplicação, assim como foi exibido um exemplo de diagramas, listas e mapas, 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 da apresentação, foi encaminhado um link do Google Forms para que o especialista respondesse à avaliação.

5.3 Apresentação dos resultados da avaliação do COM.PRIVACY

Em relação à função profissional que os participantes desempenham nas organizações em que atuam, têm-se: Participante 1: Analista de sistemas; Participante 2: Professor e empreendedor; Participante 3: Coordenador do setor administrativo, financeiro e contábil; Participante 4: Chief Information Security Officer (Ciso); Participante 5: Especialista em proteção e privacidade de dados; e Participante 6: Superintendente jurídico e encarregado de dados – configurando assim um cenário multidisciplinar.

Já em relação ao tempo de atuação dos profissionais na função, dois dos participantes têm entre um e cinco anos, dois entre 11 e 15 anos, um entre 16 e 20 anos e um mais do que 21 anos. No que se refere à quantidade de projetos nos quais os profissionais já participaram na área de segurança da informação e/ou privacidade de dados, três profissionais participaram de menos do que três projetos, dois participaram entre quatro e dez projetos e um participou de mais do que dez projetos.

Referente ao escopo do modelo, em que se procurou verificar se o universo/delimitação do campo de conhecimento é o suficiente para cumprir o seu propósito, todos os participantes concordaram com essa afirmação.

Ao se avaliar o item profundidade e precisão do modelo, procurou-se

identificar, na percepção dos participantes, quantos dos especialistas concordariam com a afirmação: 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. Ou seja, o nível de aprofundamento e decomposição do modelo é suficiente e adequado ao seu propósito. Todos os participantes concordaram com essa afirmação.

Já sobre a generalidade do COM.PRIVACY, a questão 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 implementá-lo em cenários distintos com diferentes características. O resultado demonstrou que os seis especialistas participantes concordaram com essa afirmação.

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

Ao observar a percepção dos especialistas participantes em relação à clareza do modelo para verificar se é facilmente entendido e fácil de ser aplicado, todos concordaram com essa afirmação.

Já em relação à sua consistência, pretendeu-se observar a concordância dos participantes 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 que apoiam a comprovação de alegações de segurança e privacidade de dados”. Para esta afirmação, as respostas também foram unânimes em relação à concordância dos participantes, ou seja, todos concordaram com a afirmação.

Na última questão da avaliação, foi verificada a percepção dos especialistas em relação à contribuição/recomendação, a qual buscou obter o nível de concordância com a seguinte questão: Considerando as opções de

modelos/métodos/metodologias existentes, recomenda a adoção do modelo de gerenciamento de evidências apresentado, pois ele apresenta grande contribuição na comprovação de requisitos e alegações de segurança e privacidade de dados. A esta questão, também todos os participantes foram favoráveis.

Dentre as respostas obtidas na avaliação, alguns pontos foram sugeridos pelos especialistas, sendo todos eles acatados e inseridos no modelo e nas sugestões de trabalhos futuros, quais sejam: a definição da periodicidade de aplicação do modelo, a adoção de um catálogo contendo os possíveis artefatos que podem ser utilizados como evidências e a consulta a entidades de classes, departamento jurídico e demais departamentos na identificação de fontes regulatórias adjacentes para evitar que itens relevantes sejam deixados de fora da análise.

Analisada a concordância dos especialistas participantes com a afirmação de contribuição e indicação do COM.PRIVACY, juntamente com as observações obtidas nesta questão, conclui-se que o modelo atende ao seu propósito. Com isso, acredita-se que a avaliação realizada pelos especialistas foi considerada satisfatória e atingiu os objetivos definidos. Observa-se que os propósitos do COM.PRIVACY estão alinhados à percepção dos especialistas e que o modelo pode vir a contribuir com o gerenciamento de evidências de proteção e privacidade de dados.

6 Conclusões

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

O COM.PRIVACY pode ser aplicado em empresas de qualquer porte, pois foi estruturado para que possa ser implementado considerando escopos definidos, ou seja, pode ser aplicado em um processo, em uma área ou em um produto.

Para validar o modelo proposto, o COM.PRIVACY foi submetido à avaliação de especialistas, que forneceram a sua opinião em relação a escopo, profundidade e precisão, generalidade, robustez e completeza, clareza, consistência e contribuição/recomendação. Considerando o perfil, o envolvimento dos participantes e os resultados obtidos, constatou-se que os propósitos do COM.PRIVACY estão alinhados à percepção dos especialistas e que o modelo pode contribuir com o gerenciamento de evidências de proteção e privacidade de dados

No que se refere à questão definida para nortear esta pesquisa – 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? –, essa é respondida ao considerar que o COM.PRIVACY mapeia e registra informações acerca dos artefatos a serem utilizados para comprovação dos requisitos em formulários e apresenta essas informações de forma sistematizada em listas, catálogos e diagramas, demonstrando como e em quais evidências os requisitos previstos nas normativas são validados. Ademais, o modelo contempla registros de informações a serem utilizadas no gerenciamento das evidências para apoiar a sua rastreabilidade, atualização e facilidade de localização.

Considera-se que o COM.PRIVACY pode 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; com os cidadãos, uma vez que propõe uma abordagem que pode ser utilizada na validação e na comprovação de seus direitos de privacidade como titulares dos dados; com as organizações, pois o modelo proposto pode apoiá-las na adequação e na aderência às normativas de proteção e privacidade de dados e ser adotado como referência para o gerenciamento de evidências; com os órgãos reguladores/certificadores e auditores, por proporcionar a padronização nas

comprovações do tratamento de dados pessoais; e com os profissionais da área de proteção e privacidade de dados, por oferecer a oportunidade de adotar um modelo que objetiva garantir a qualidade e a aceitação das evidências.

Entende-se que esta investigação inicia uma discussão sobre mecanismos para auxiliar na validação de requisitos e controles relacionados à proteção e à privacidade de dados com abordagem em evidências. Dessa forma, sugere-se que uma das propostas de trabalhos futuros envolva modelos e metodologias que possam ser utilizados na avaliação da qualidade e da pertinência das evidências apresentadas. Este trabalho procurou identificá-las e apresentá-las de forma sistemática. Entende-se que avaliar se elas são suficientes e apropriadas para o seu propósito é de extrema relevância para se obter um processo com ciclo completo.

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

Também para a continuidade do modelo, propõe-se que ele 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. E, por fim, em relação aos componentes do COM.PRIVACY, sugere-se que novos sejam adicionados ao modelo, de forma a facilitar a visualização e possibilitar o controle de versões e informações mais claras das fontes de extração das evidências.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 29100**: tecnologia da informação: técnicas de segurança: estrutura de privacidade. Rio de Janeiro, ABNT, 2020.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**: seção 1, Brasília, n. 157, p. 59, 15 ago. 2018.

CAVOUKIAN, Ann. Privacy by design: the 7 foundational principles. **Information and Privacy Commissioner of Ontario**, Toronto, 2009.

EUROPEAN UNION. General data protection regulation. **EUR-Lex**, Luxemburgo, 2016.

FACCHINI NETO, Eugênio; DEMOLINER, Karina Silva. Direito à privacidade e novas tecnologias: breves considerações acerca da proteção de dados pessoais no Brasil e na Europa. **Revista Internacional Consinter de Direito**, Porto, ano 6, n. 7, p. 19-40, 2018. Disponível em: https://doi.org/10.19135/revista.consinter.0007.01. Acesso em: 7 maio 2023.

HEVNER, Alan; CHATTERJEE, Samir. **Design research in information systems**: theory and practice. Berlin: Springer, 2010.

ISAAK, Jim; HANNA, Mina J. User data privacy: Facebook, Cambridge analytica, and privacy protection. **Computer**, New York, v. 51, n. 8, p. 56-59, 2018. Disponível em: http://doi.org/ 10.1109/MC.2018.3191268. Acesso em: 10 mar. 2022.

KOKALY, Sahar. Managing assurance cases in model based software systems. *In*: INTERNATIONAL CONFERENCE ON SOFTWARE ENGINEERING COMPANION, 39., 2017, Buenos Aires. **Anais** […]. Buenos Aires: IEE, 2017. p. 453-456.

LIMA, Paulo Ricardo Silva; PRESSER, Nadi Helena. A Lei Geral de Proteção de Dados e os desafios para a gestão nas organizações brasileiras na era do big data. **Revista P2P & Inovação**, Brasília, v. 8, n. 2, p. 109-120, 2022. Disponível em: https://doi.org/10.21721/p2p.2022v8n2.p109-120. Acesso em: 2 maio 2023.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

OBJECT MANAGEMENT GROUP (OMG). **Structured Assurance Case Metamodel (SACM)**: version 2.1., Milford, Apr. 2020.

ROCHA, Junia M.; HONORATO, Mauro Jacob; COSTA, Eduardo. Assessment of expert panels. **IEEE Latin America Transactions**, New York, v. 14, n. 1, p. 303-308, 2016. Disponível em: http://doi.org/10.1109/TLA.2016.7430093. Acesso em: 30 ago. 2022.

SCHAAR, Peter. Privacy by Design. **Identity in the Information Society**, Estados Unidos, v. 3, n. 2, p. 267-274, 2010. Disponível em: http://doi.org/ 10.1007/s12394-010-0055-x. Acesso em: 5 maio 2022.

SOUSA, Rosilene Paiva Marinho de; BARRANCOS, Jacqueline Echeverría; MAIA, Manuela Eugênio. Acesso à informação e ao tratamento de dados

pessoais pelo poder público. **Informação & Sociedade: Estudos**, João Pessoa, v. 29, n. 1, p. 237-251, 2019.

Data protection and privacy: a model for evidence management

Abstract: The legislation and regulations related to data protection and privacy present the requirements that organizations, processes, products and environments need to meet to be considered secure. Among the recommended requirements, the "Accountability" and "Privacy Compliance" requirements stand out, which define that organizations must be responsible and able to demonstrate compliance with current laws and regulations. In addition to the challenge of implementing such requirements, it is necessary to adopt systematized processes that prove how and on what evidence these requirements are validated. This article presents a model called COM.PRIVACY to manage evidence of data protection and privacy to demonstrate diligence and compliance with good practice regulations. Design Science Research (DSR) was used as a research method for proposing the model. For its validation, COM.PRIVACY was applied in an organization that made it possible to observe and identify improvements during its use, in addition to submitting a questionnaire to specialists to evaluate the model. It was concluded that the model supports the validation and proof of compliance with data protection and privacy requirements in all data processing operations, and can be adopted both in the activity of adequacy and implementation of regulations, in the process of measurement and verification compliance with them, as well as to promote transparency in the processing of data to their holders.

Keywords: data protection; data privacy; evidence management; information security

Recebido: 20/10/2022
Aceito: 03/06/2023

Declaração de autoria

Concepção e elaboração do estudo: Gislaine Parra Freund, Douglas Dyllon Jeronimo de Macedo, Priscila Basto Fagundes
Coleta de dados: Gislaine Parra Freund
Análise e interpretação de dados: Gislaine Parra Freund, Douglas Dyllon Jeronimo de Macedo, Priscila Basto Fagundes
Redação: Gislaine Parra Freund, Douglas Dyllon Jeronimo de Macedo, Priscila Basto Fagundes

Revisão crítica do manuscrito: Gislaine Parra Freund, Douglas Dyllon Jeronimo de Macedo, Priscila Basto Fagundes

Como citar:

FREUND, Gislaine Parra; MACEDO, Douglas Dyllon Jeronimo de; FAGUNDES, Priscila Basto. Proteção e privacidade de dados: um modelo para o gerenciamento de evidências. **Em Questão**, Porto Alegre, v.29, e-128009, 2023. DOI: https://doi.org/10.1590/1808-5245.29.128009