Requisitos de Segurança e Privacidade em Startups: Um Estudo Empírico em uma Aplicação de Governança de Dados

Ewerton David Brito de Jesus, Jéssyka Vilela, Carla Silva

Centro de Informática, Universidade Federal de Pernambuco, Recife, Brasil
{edbj2,jffv,ctlls}@cin.ufpe.br

Resumo Vários incidentes de vazamento de dados pessoais têm acontecido, trazendo impactos negativos tanto para o titular como para o controlador dos dados pessoais. Nesse contexto, leis de privacidade foram criadas para que dados pessoais sejam tratados de forma responsável. A segurança da informação, forte aliada à proteção de dados, muitas vezes é negligenciada por empresas de pequeno porte. Este trabalho apresenta a utilização de um modelo de avaliação de riscos de segurança da informação e privacidade em uma aplicação de governança de dados de uma startup de tecnologia de pequeno porte. Dos 14 riscos identificados, 13 estavam em nível alto de risco, principalmente devido à falta de recursos financeiros e profissionais especializados. Neste trabalho, 13 controles foram sugeridos para melhorar a segurança na startup e reflete as dificuldades enfrentadas por empresas de pequeno porte nesse cenário.

Palavras-chave: Requisitos de segurança da informação · Requisitos de privacidade · Avaliação de riscos · Startups · LGPD · Estudo empírico.

1 Introdução

Nos últimos anos, diversas empresas e órgãos públicos têm enfrentado vazamentos de dados, expondo dados pessoais de seus clientes e funcionários. Como exemplo, pode-se citar o vazamento de dados do Ministério da Saúde em 2020, que afetou 243 milhões de pessoas. Uma falha no sistema e-SUS Notifica expôs, por seis meses, dados de cidadãos (incluindo pessoas falecidas), incluindo nome completo, endereço, telefone e CPF (Cadastro de Pessoa Física) [1].

Os vazamentos podem ter origem em uma vulnerabilidade do sistema, explorada por uma pessoa mal-intencionada, por código malicioso em ataque cibernético, acesso a contas de usuários por meio de senhas fracas ou vazadas, pela ação de funcionários ou ex-funcionários que coletam dados dos sistemas e repassam a terceiros, entre outras causas [5]. Tais vazamentos têm aumentado significativamente nos últimos anos, causando impactos financeiros e danos à reputação de empresas e governos em todo o mundo. O custo médio global de vazamento de

dados em 2022 foi de 4,35 milhões de dólares, segundo a pesquisa *Cost of Data Breach* encomendada pela IBM [10]. Esse cenário resultou na criação de leis de privacidade que pudessem proteger as pessoas e seus dados pessoais, aplicando multas a empresas que não cumpram as regulamentações [3]. Em 2018 o Brasil aprovou a Lei Geral de Proteção de Dados (LGPD)[4].

No entanto, muitas organizações ainda não estão em conformidade com as leis de proteção de dados. Para alcançar essa conformidade, é necessário analisar os requisitos de segurança da informação, identificando as lacunas que precisam ser sanadas na empresa e propor medidas para mitigá-las [14]. Nesse contexto, este trabalho define um método de avaliação de riscos relacionados à segurança da informação, que visa também promover a privacidade em uma aplicação de governança de dados de uma *startup*. De fato, a LGPD tem Segurança como um dos seus princípios e o método aqui proposto para segurança da informação também tem o potencial de ajudar as *startups* a se adequarem à lei.

Uma *startup* é uma iniciativa de curto prazo que visa criar um modelo de negócio sustentável e é caracterizada pela necessidade de crescimento rápido, mudanças frequentes nos planos e equipes enxutas. Elas frequentemente se tornam vítimas de vazamentos de dados, pois não implementam diversas medidas de segurança e geralmente não possuem pessoal especializado em segurança da informação [8]. Outras características incluem imaturidade e limitações de recursos humanos e financeiros. É importante direcionar esforços para auxiliar as *startups* a melhorar a sua segurança da informação. De acordo com um estudo da Accenture [6], 43% dos ataques cibernéticos são direcionados a pequenas empresas, sendo que apenas 14% delas estão preparadas para se defender.

O principal objetivo deste trabalho é apoiar *startups* de tecnologia de pequeno porte a identificar lacunas na segurança da informação, proporcionando um caminho de adequação à LGPD. Para esse fim, este trabalho adapta e aplica o Guia de Avaliação de Riscos de Segurança e Privacidade da Secretaria de Governo Digital (GARSP-SGD) [9] em uma *startup* de tecnologia de pequeno porte. Lançado em novembro de 2020, GARSP-SGD é um método de avaliação de riscos criado pela Secretaria de Governo Digital do Ministério da Economia a partir de seus trabalhos de análise de sistemas críticos no setor público. A avaliação de risco é uma das etapas do processo de gestão de risco definido na norma ABNT NBR ISO/IEC 27005 [2]. Este trabalho contribui para difundir a utilização de um método de avaliação de risco desenvolvido por órgão do Governo Federal no contexto de avaliação de uma *startup* no setor privado.

O restante deste artigo está estruturado assim: A seção 2 apresenta os trabalhos relacionados. A seção 3 descreve o método de pesquisa. A seção 4 apresenta a adaptação do método GARSP-SGD e sua aplicação em uma startup. Finalmente, a seção 5 apresenta as conclusões e as direções futuras desta pesquisa.

2 Trabalhos Relacionados

Silva Netto e Silveira [16] analisaram a implementação de medidas de segurança da informação em indústrias de pequeno e médio porte na região do interior

de São Paulo. A pesquisa fez um levantamento com 43 indústrias do setor de fabricação de produtos de metal. Foi avaliada a implementação de controles de segurança da informação relacionados a diferentes camadas (humana, física e lógica) baseados na norma ISO/IEC 27002:2005. Os resultados relevam que, apesar da preocupação com segurança da informação, há uma deficiência na atenção dada tanto à camada humana quanto à camada lógica. Isso indica a necessidade de direcionar o foco não apenas para soluções tecnológicas, mas também para a conscientização e treinamento dos colaboradores [16]. O antivírus foi a ferramenta mais amplamente adotada para promover a segurança da informação. Também foi constatado que aproximadamente 59% das empresas pesquisadas alcançaram um nível satisfatório de segurança. No entanto, a análise dos controles da norma ISO/IEC 27002:2005 indicou que muitas empresas não implementaram todos os controles recomendados. A motivação principal para adotar a gestão da segurança da informação é a prevenção de perdas financeiras. Mas a falta de conhecimento foi vista como um possível fator inibidor e aponta para a necessidade de educação e treinamento contínuos em segurança da informação [16].

Neto et al. [13] apresentam um estudo que avalia a implementação de medidas de segurança da informação entre as Pequenas e Médias Empresas (PMEs). O estudo envolveu 48 PMEs reais, por meio de questionários, para entender a perspectiva dessas empresas em relação à segurança da informação. Além disso, foi desenvolvido um modelo simplificado, que condensou os 133 controles estabelecidos pela norma NBR ISO/IEC 27002:2005 em 22. Esse modelo simplificado foi posteriormente submetido à validação por meio de questionários respondidos por 51 profissionais de Tecnologia da Informação que atuam nas PMEs alvo [13]. O questionário perguntava se o modelo atendia as necessidades da empresa. O resultado foi que 97,4% dos respondentes afirmaram que os controles selecionados atendiam à necessidade de sua empresa. Os resultados da pesquisa confirmam que muitas das PMEs não estão em conformidade com algum tipo de norma ou padrão de segurança da informação. Os autores concluem que "Diante de diversos fatores a serem considerados para a não adequação às normas de segurança da informação, pode-se destacar a cultura organizacional das PMEs como um dos maiores fatores impeditivos". Por fim, o artigo conclui que há uma carência de práticas e modelos de segurança nas empresas de pequeno e médio porte [13].

Kaila e Nyman [12] apresentam uma abordagem para implementar práticas de segurança da informação em pequenas e médias empresas (PMEs). A abordagem se baseia em diretrizes do *National Institute of Standards and Technology* (NIST) e apresenta práticas de segurança da informação que sejam acessíveis para gestores e proprietários de *startups* que estejam dando os primeiros passos na implementação da segurança da informação [12]. O *framework* proposto pelos autores compreende quatro fases [12]. A primeira envolve a identificação de ativos e riscos de segurança da informação. A empresa deve listar ativos a serem protegidos e os principais riscos associados a esses ativos. No segundo passo, deve-se proteger as contas, sistemas críticos, nuvens (*cloud*) e os dados. Nessa fase, o objetivo é mitigar os riscos identificados. Os autores discutem controles preventivos, detectivos e corretivos, enfatizando a importância de não apenas prevenir

ameaças, mas também detectá-las e responder de forma eficaz a elas. No terceiro passo, "Elaborar um Plano de Continuidade", é apresentada a necessidade de um plano de recuperação de desastres que assegura a continuidade das operações após falhas, tornando a segurança compreensível mesmo para não especialistas. Várias abordagens podem ser usadas, incluindo implementação de controles de segurança da informação e planos de contingência [12]. No quarto e último passo, "Monitorar e Avaliar", é enfatizada a importância do monitoramento contínuo. Isso ajuda a identificar eventos adversos. O uso de métricas de segurança, como disponibilidade de serviços e detecção de *malware*, são mencionadas [12].

Os trabalhos analisados nesta seção apontam para a importância que as empresas de pequeno e médio porte tem dado para a segurança da informação. Nosso trabalho trabalho complementa esses trabalhos por definir um método de avaliação de riscos de segurança da informação e privacidade em *startups*.

3 Método de Pesquisa

Este trabalho visa adequar o método do Guia de Avaliação de Riscos de Segurança e Privacidade da Secretaria de Governo Digital (GARSP-SGD) [9] para avaliar uma *startup*; aplicar o método de avaliação proposto ao sistema de uma *startup*; e propor medidas para minimizar os riscos encontrados. Nesta seção, é apresentada a metodologia que guiou a criação e avaliação do método proposto.

Etapa 1 - Pesquisa de controles de segurança e privacidade. O GARSP-SGD tem foco no serviço público, ajudando públicas a avaliar os controles de segurança da informação nos controles e avaliar os prestadores de serviço quanto à segurança da informação. Como resultado, o GARSP-SGD pode ajudar a aumentar a maturidade dos sistemas em relação a sua segurança.

O GARSP-SGD traz originalmente 113 controles de segurança da informação e privacidade que foram coletados de *frameworks* e normas existentes como a ISO/IEC 27002, OWASP e portarias do Governo Federal (material suplementar[1]). A partir da implementação ou não desses controles, é que os níveis de risco do sistema serão calculados. Além disso, os controles de segurança da informação atuam de maneiras diferentes em relação a cada risco, pois "podem contribuir para a prevenção do risco, para sua mitigação, ou ambos ao mesmo tempo. Controles de prevenção atuam na redução da probabilidade da ocorrência do risco e controles de mitigação atuam na redução do impacto do risco"[9].

O GARSP-SGD sugere que os controles possam ser personalizados, adaptados e excluídos de acordo com as necessidades específicas da organização. Com o objetivo de adaptar o método para atender às demandas de *startups*, foi iniciada uma pesquisa em busca de controles relevantes para empresas de pequeno porte. Esses controles foram posteriormente comparados com os 113 controles originais do GARSP-SGD para a etapa de seleção e refinamento de controles.

A pesquisa de controles para *startups* foi realizada a partir de um levantamento dos controles de segurança da informação e privacidade existentes. O

[1] https://zenodo.org/records/11194473

critério para selecionar o grupo de controles para *startup* foi buscar coleções de controles que já fizessem previamente o filtro de controles para pequenas organizações ou que definissem controles críticos para todo tipo de empresa. Com esse critério, foram levantados 54 controles do CIS Controls v8 [11], 10 Open Source Foundation for Application Security (OWASP) [15], 22 controles o Modelo de Segurança Simplificado para Pequenas e Médias Empresas [13] e 28 controles do Guia de Boas Práticas para Agentes de Tratamento de Pequeno Porte [7]. No total, 108 controles foram identificados e organizados em planilhas. A lista completa de controles pode ser consultada no material suplementar.

Esta etapa é importante, pois o método de avaliação de riscos do GARSP-SGD contém controles de segurança da informação de caráter geral, ou seja, os controles não fazem distinção do tipo de empresa e possuem um viés para instituições públicas. Os controles foram levantados para posterior refinamento e adequação do método proposto no trabalho. Essas adaptações e adições garantem que o método seja relevante para as necessidades específicas de *startups*, mantendo a integridade das diretrizes estabelecidas pela ISO/IEC 27005.

Etapa 2 - Seleção de controles e refinamento. Essa etapa foi necessária para adequar os controles encontrados para *startups*. Para isso, os controles levantados na etapa anterior (108 controles) foram comparados aos 113 controles originais GARSP-SGD, seguindo os seguintes critérios: 1) Cada controle da lista de controles levantados na Etapa 1 foi comparado com os 113 controles do GARSP-SGD; 2) Caso o controle para a *startup* já tenha sido abordado, o controle é mantido; 3) Caso o controle para a *startup* não esteja no GARSP-SGD, o controle é adicionado à lista de controles; 4) Os controles do GARSP-SGD restantes foram removidos da avaliação.

Os novos controles foram adicionados juntamente com uma pergunta que representava sua implementação. Para integrá-los ao método GARSP-SGD, foram atribuídas classificações (controle de prevenção ou mitigação) com base na experiência do autor e nos estudos sobre controles de segurança da informação, junto com um peso correspondente a cada um dos 14 riscos identificados pelo GARSP-SGD. Seguindo esses critérios, 79 controles GARSP-SGD que estavam presentes no levantamento de controles para *startups* foram mantidos e os 34 controles remanescentes foram removidos da lista final de controles a serem utilizados na avaliação de riscos. 27 novos controles foram adicionados à lista final, pois estavam na lista de controles para *startups* e não estavam nos controles do GARSP-SGD. Ao final da etapa de refinamento de controles, 106 controles foram selecionados para utilização na análise de risco de segurança da informação.

Etapa 3 - Criação da planilha eletrônica. Visando a facilidade de uso e utilização prática da metodologia de avaliação de riscos, foi desenvolvida uma planilha que aplica o método de avaliação de riscos, reunindo todos os controles de segurança da informação e privacidade fornecidos pelo método. A planilha foi configurada de forma a realizar os cálculos de risco com base nas respostas do usuário sobre a implementação dos controles de segurança e privacidade. Sendo assim, a planilha proporciona uma visão geral do método e apresenta os resultados de forma fácil de visualizar e facilitar a tomada de decisão.

Etapa 4 - Seleção de uma startup para avaliação. O critério utilizado para a escolha da *startup* foi "amostragem por conveniência". A *startup* é de pequeno porte com mais de cinco anos de existência, que atua na área de análise e governança de dados para órgãos públicos.

O fato de a empresa não possuir uma equipe especializada em segurança da informação, além de estar diretamente relacionada a órgãos públicos e atuar como operadora de dados em seus projetos, a torna um ambiente rico para estudos sobre segurança da informação. Por esse motivo, foi selecionada para a aplicação do método de avaliação de riscos.

A aplicação em análise será referida como "aplicação de governança de dados"ao longo de todo o trabalho. O objetivo da aplicação é fornecer funcionalidades de governança de dados para órgãos públicos, incluindo o armazenamento de grandes volumes de dados, o compartilhamento de dados de acordo com critérios de autorização e a criação de catálogos de conjuntos de dados. Os dados pessoais armazenados podem ser, sensíveis ou não, incluindo dados abertos e dados internos dos órgãos públicos que precisam ser compartilhados com outros. Devido a essas características, a aplicação de governança de dados precisa estar em conformidade com a LGPD.

Etapa 5 - Aplicação do método em uma startup. A coleta dos dados foi realizada em diferentes encontros e formatos, as primeiras coletas de dados ocorreram com um Gerente de Projetos da *startup* escolhida. Em seguida, a avaliação de riscos foi feita com o envio da planilha eletrônica com questionário para outros 4 colaboradores de áreas distintas da empresa, onde cada um respondeu às perguntas individualmente.

O objetivo foi obter respostas que incluíssem as visões de diferentes áreas a respeito da implementação dos controles. A partir dessas respostas, o nível de risco da aplicação foi calculado. A avaliação dos controles para *startups* foi realizada em dois encontros feitos em videoconferência e aplicação do método de avaliação de riscos feitos a partir de questionários em planilha eletrônica.

Etapa 6 - Levantamento dos resultados. Os resultados obtidos das respostas aos questionários e da aplicação do método de avaliação de riscos foram sintetizados. Os resultados foram calculados na planilha eletrônica, o nível de risco para cada um dos 14 riscos identificados pelo método GARSP-SGD é apresentado. Com base nessa análise, são sugeridos controles necessários para alcançar diferentes níveis de risco, indicando à *startup* quais controles devem ser implementados para avançar para o próximo nível de segurança. Isso resulta na redução da probabilidade e do impacto de possíveis vulnerabilidades em seus sistemas e processos. E traz o benefício de mostrar aos gestores como evoluir a segurança da informação na *startup*.

4 Planilha Eletrônica de Avaliação de Riscos

Para aplicação do método GARSP-SGD foi criada uma planilha eletrônica que possui múltiplas abas com seguintes características: uma lista de controles, uma lista de riscos, uma matriz de pesos, um questionário e uma folha de resultados.

A aba com a lista de controles, chamada de "Controles", possui os 106 controles que foram utilizados na aplicação do método GARSP-SGD. Esta aba (Fig. 1 (A)) possui colunas quem descrevem: o código de identificação, a pergunta que representa o controle, o grupo do controle e as referências da origem do controle.

A aba "Riscos"com a lista de riscos, apresenta os 14 riscos de segurança da informação e privacidade utilizados pelo método GARSP-SGD, cada risco possui um identificador, nome do risco e sua descrição como apresentado na Fig. 1 (B).

Na aba "Matriz"(Fig. 2 (A).) está a matriz de riscos, ela representa como os controles estão associados aos riscos, quais seus pesos e o tipo de controle. A planilha modifica a matriz de risco original do método, além das cores de cada célula definir se o controle é do tipo mitigação (cinza), prevenção (amarelo) ou ambos (azul), os tipos de controle estão descritos com uma letra ao lado do peso do controle. Por exemplo, o controle ID 3 é do tipo mitigação no risco ID 3 e tem seu peso como 1 (prioritário). Na matriz de risco seu valor é: M1 (cinza).

Para realizarmos a análise de risco, é necessário uma avaliação de um analista ou gestor, a planilha eletrônica possui uma aba para receber essas respostas. A aba "Resposta"possui a seguinte estrutura, na parte superior da planilha, são mostradas três perguntas: (i) Quantos anos de experiência você possui no cargo/função? (ii) Como você avalia seu conhecimento sobre privacidade de dados? (iii) Como você avalia seu conhecimento sobre segurança da informação?. Em seguida, o texto da Fig. 2 (B) é apresentado.

Após as orientações, a lista de controles é apresentada linha a linha, onde cada linha contém o seguinte: o ID do controle, a pergunta que representa o controle, o Grupo, a Referência Original, a Resposta, uma justificativa em campo aberto caso o controle não seja aplicável, o Grau de Importância do controle (0 - Não sei, 1 - Muito Baixo, 2 - Baixo, 3 - Médio, 4 - Alto, 5 - Muito Alto), bem como a Viabilidade de Implementação, um campo fechado com as opções (Viável e Não viável) e, por fim, um campo aberto opcional para justificar a viabilidade do controle. A Fig. 3 (A) apresenta o questionário utilizado na avaliação de riscos.

A partir das respostas nas abas do questionário (podem ser mais de uma), o resultado da análise de risco é calculado. Para cada controle, soma-se a quantidade de respostas de cada aba. Por exemplo, se "Controle Aplicado"tiver a maior quantidade de respostas, o resultado para o controle é "APLICADO". Se a quantidade maior for "Controle não aplicado", então o resultado é "NÃO APLICADO". Caso a quantidade seja "Controle não aplicável", resulta em "NÃO SE APLICA"na lista denominada "Avaliação Final". O nível de importância é calculado a partir da média das respostas para cada controle. A viabilidade é a maior quantidade de respostas "Viável"ou "Não viável"do questionário.

A aba "Resultados"também possui uma matriz de peso em que o resultado da aplicação do controle e os pesos são concatenados em um único texto. Ex: O controle de ID 3 quando aplicado assume o valor "APLICADO-M1", quando não aplicado assume o valor "NAO-APLICADO-M1"e quando não se aplica assume o valor "NAO-SE-APLICA-M1". Esses valores são utilizados para somar a quantidade de pesos totais relacionados a cada risco. Abaixo da matriz de pesos, há uma tabela com o resultado da avaliação de riscos, nela há a lista de riscos e

ID	Controle	Grupo	Referência Original
1	Há uma matriz de responsabilidades com atribuição das responsabilidades pela segurança da informação na organização, pela proteção de dados (encarregado), identificação dos gestores de serviços com dados pessoais, operadores de tratamento de dados, de forma a evidenciar a segregação de funções e assegurar que colaboradores e partes externas entendam suas responsabilidades?	Responsabilização	NC nº 03/IN01/DSIC/GSIPR (item 5.3.7); ABNT NBR ISO/IEC 27002:2013 (item 6.1.1)
2	Há mecanismos para monitoramento do uso dos recursos, de forma a atender as necessidades de capacidade futura e garantir o desempenho requerido das aplicações?	Gestão de Capacidade e Redundância	NC nº 10/IN01/DSIC/GSIPR (item 5.3.2); ABNT NBR ISO/IEC 27002:2013 (item 12.1.3); NBR ISO/IEC 27002:2005 (A.10.3.1);
3	São implementados mecanismos e procedimentos para mitigar ataques de negação de serviço, tais como balanceamento de carga, proxy, firewall, etc.?	Continuidade de Negócio	NC nº 08/IN01/DSIC/GSIPR (Item 7.2); ABNT NBR ISO/IEC 27002:2013 (13.1.2); CIS Controls v8 (item 4.4); ANPD 3.2.3 (p. 54);
4	Existe um Plano de Continuidade de Negócio, que garanta o nível adequado de continuidade para a segurança da informação durante uma situação adversa?	Continuidade de Negócio	NC nº 06/IN01/DSIC/GSIPR; ABNT NBR ISO/IEC 27002:2013 (item 17.1); NBR ISO/IEC 27002:2005 (A.14.1.1);
5	A empresa possui Política de Segurança da Informação? Ela já foi revisada para se adequar a medidas que objetivem a proteção de dados pessoais? Na política deve ser estabelecido com previsão de revisão periódica e que contemple controles relacionados ao tratamento de dados pessoais, como por exemplo, cópias de segurança; uso de senhas; acesso à informação; compartilhamento de dados; atualização de softwares; uso de correio eletrônico; uso de antivírus, entre outros.	Compliance com privacidade	ABNT NBR ISO/IEC 27701:2019 (item 6.2); ANPD 3.1.1 (p. 24);
7	O local que processa as informações é restrito somente ao pessoal autorizado?	Controles de Segurança em Redes, Proteção Física e do Ambiente	NC nº 10/IN01/DSIC/GSIPR (item 5.5.2); ABNT NBR ISO/IEC 27002:2013 (item 11.1); NBR ISO/IEC 27002:2005 (A.9.1.1); NBR ISO/IEC 27002:2005 (A.9.1.2);
8	O trabalho nas áreas seguras é supervisionado?	Controles de Segurança em Redes, Proteção Física e do Ambiente	NC nº 07/IN01/DSIC/GSIPR (item 7); ABNT NBR ISO/IEC 27002:2013 (item 11.1.2); NBR ISO/IEC 27002:2005 (A.9.1.1); NBR ISO/IEC 27002:2005 (A.9.1.2);

ID	Risco	Descrição
1	Acesso não autorizado	Acesso indevido (permissões indevidas) a um ambiente físico ou lógico.
2	Coleção excessiva	Coleta de dados pessoais em quantidade superior ao mínimo necessário à finalidade do tratamento ou atividade que fará uso do dado pessoal.
3	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais	Instituição não atende sua finalidade legal e compartilhaos dados sem consentimento do titular dos dados pessoais (LGPD,art. 27).
5	Falha ou erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada etc.)	Dados de entrada que não são corretamente validados, operações de tratamento automatizadas de sistema que alteram de maneira indevida a composição do dado armazenado.
6	Informação insuficiente sobre a finalidade do tratamento	O tratamento de dados pessoais realizado de forma eletrônica ou documento em papel deve atender a uma finalidade e ser exposto de forma transparentee clara ao detentor dos dados pessoais.
7	Modificação não autorizada	Usuário sem permissões de alteração para um determinado dado pessoal ou registro realiza a modificação não autorizada. Um processamento indevido pode gerar uma modificação não autorizada.
8	Perda	Perdas provocadas por ações intencionais de usuários oriundas deuma exclusão indevida ou devida e não comunicada, e provenientes de ações não intencionais como falhas em sistemas, sobrescrita de dados, falhas em hardware, entre outras.
9	Reidentificação de dados pseudonimizados	Dados pessoais podem ser reidentificados por cruzamento simplesde dados pessoais (LGPD,art. 12 e 13).
10	Remoção não autorizada	Usuário não tem a permissão para retirar ou copiar dados pessoais para outro local.
11	Retenção prolongada de dados pessoais sem necessidade	O término da prestaçãode um serviço ou do prazo da retenção dos dados pessoais para fins legais deve culminar com a exclusão e/ou descarte seguro(a) dos dados pessoais.
12	Roubo	Dados roubados nas dependências interna do controlador/operador, falhas nos controles de segurança dos sistemas (a exemplo da ausência ou fraca criptografia falha de sistema que permita escalação de privilégio ou tratamentos indevidos), entre outras.

Figura 1. (A) Lista de controles; (B) Lista de riscos

a soma dos pesos de cada controles nas seguintes colunas: (i) Total de pesos de Controles Associados ao Risco: soma dos pesos de todos os controles associados ao risco; (ii) Total de pesos de Controles Aplicados ao Risco: soma dos pesos dos controles implementados; (iii) Total de pesos de Controles Não se Aplica ao Risco: soma dos pesos dos controles que não são aplicáveis à empresa avaliada. Os valores dessas colunas são utilizados no cálculo de probabilidade e impacto (Fig. 3 (B)). A avaliação final é feita na coluna "Nível de Risco"(omitida por questão de espaço).

Consolidação dos Controles Encontrados. O resultado da etapa de seleção e refinamento de controles foi uma lista reduzida de controles a serem utilizados no método de avaliação de riscos. Inicialmente, dos 108 controles para *startups* pesquisados, 27 novos controles foram adicionados aos 113 originais do GARSP-SGD. Os controles adicionados podem ser consultados no material suplementar e estão listados a partir do ID de número 113 até 140. Como diversos controles tratavam sobre a mesma medida de segurança, houve a necessidade de avaliar e filtrar aqueles que já estavam sendo abordados. Para evitar duplicações de controles, dos 113 controles originais do GARSP-SGD, 79 controles que já haviam sido anteriormente mencionados nos controles para *startup* e permaneceram na lista final de controles (material suplementar). Os controles que não foram citados na pesquisa de controles para *startup* foram removidos.

Para integrarem o método de avaliação de riscos, os novos controles precisaram receber pesos e estar associados aos riscos. Para alcançar esse objetivo, cada novo controle foi comparado com cada um dos 14 riscos do GARSP-SGD. Se o controle estiver relacionado à prevenção (amarelo), mitigação (cinza) ou ambos (azul), ele recebe uma cor na matriz de pesos, além do peso, caso seja aplicável ao risco (peso 0,5) ou prioritário (peso 1).

Aplicação do Método de Avaliação de Riscos de Segurança e Privacidade. Através das respostas obtidas pela planilha eletrônica enviada para os 4 colaboradores da *startup* escolhida para avaliação de riscos na aplicação de governança de dados, foi possível calcular os níveis de risco para cada um dos 14 riscos de segurança da informação estabelecidos pelo GARSP-SGD [9].

Foram realizadas duas aplicações com abordagens semelhantes. Na primeira aplicação, a avaliação foi conduzida exclusivamente com o Gerente de Projetos da *startup*, em uma sessão síncrona com a planilha para a avaliação de riscos. Uma segunda rodada de análise foi realizada, envolvendo colaboradores de diferentes áreas. No material suplementar são detalhados os resultados dos níveis de risco, os controles aplicados e não aplicados. Ao final, 40 controles foram aplicados, 41 não foram aplicados, 25 não se aplicavam, totalizando 106 controles.

Resultado da Avaliação de Riscos. 14 riscos resultaram da aplicação do método na empresa. Após a análise de risco realizada, foram elaborados dois cenários para a implementação dos controles. As sugestões se referem às quantidades mínimas de controles que não estão aplicados e devem ser implementados, para assim, atingir o próximo nível. No primeiro cenário, os controles devem ser implementados e resultam em um risco residual considerado "Moderado". O segundo cenário consiste na aplicação do primeiro cenário juntamente com

controles adicionais, de modo a que o risco residual seja considerado 'Baixo'. Os detalhes dos riscos e controles selecionados estão no material suplementar.

Além disso, coletamos alguns comentários dos participantes da avaliação do GARSP-SGD por meio de um questionário. Suas perspectivas e *insights* oferecem uma visão abrangente sobre a eficácia do método e os potenciais benefícios que ele pode proporcionar, além de possíveis melhorias. Os colaboradores tinham as seguintes funções na startup: Engenharia de Software, Engenharia de Dados, DevOps e Gerente de Projetos. Não mapeamos as funções para os identificadores dos colaboradores para não quebrar o anonimato dos participantes.

Colaborador 1 - Perspectiva sobre a Eficácia: O colaborador expressou uma visão positiva da eficácia do método de avaliação de riscos, destacando sua importância na prevenção de incidentes e na promoção de uma cultura de segurança. Ele ressaltou que os controles de revisão são cruciais para a implementação eficaz de práticas de segurança em empresas de todos os tamanhos.

"Eu acredito que os métodos aplicados pelos controles de revisão são bastante importantes para prevenção de incidentes, garantido a eficácia de implementação dos demais controles, como adoção de boas práticas na restrição de acessos, cobrir vulnerabilidades em diversas camadas da empresa e implementação de planos de resposta aos riscos. [...] O simples ato de socializar esses conceitos ajudam no processo de transformação cultural da empresa, tornando mais comum a preocupação dos colaboradores com a preservação do ambiente profissional".

Potenciais Benefícios: O colaborador identificou diversos benefícios, incluindo a redução de custos relacionados a falhas de segurança, a melhoria da reputação da empresa e a capacidade de tomar decisões mais informadas.

"Diversos benefícios podem ser extraídos na aplicação desses métodos, mas consigo apontar para: redução de custos atrelados à ocorrência de falhas de segurança; melhorar (ou manter) a reputação da empresa, atraindo novos clientes; reduzir incertezas nas tomadas de decisões, aproveitando melhor o tempo; e maior responsabilidade do coletivo com a proteção de seu ambiente de trabalho".

Sugestões de Melhoria: Ele também sugeriu a complementação das avaliações com terceiros testando segurança para melhorar a avaliação de riscos.

"Acredito que além do uso de questionários como método de avaliação de risco, também podem ser complementadas avaliações práticas de testes de segurança executadas por terceiros (setor de segurança e/ou sistemas autônomos)".

Colaborador 2 - Perspectiva sobre a Eficácia: O Colaborador 2 expressou uma visão positiva sobre a eficácia do método de avaliação de riscos aplicado nesta pesquisa. Ele destacou que o método, baseado na análise de ativos, ameaças e vulnerabilidades, foi eficaz em identificar e priorizar os riscos existentes e não monitorados pela empresa, tais como o vazamento de dados, a interrupção dos serviços de TI e a perda de produtividade. Além disso, ele notou que o método ofereceu diretrizes claras para o monitoramento e combate desses riscos.

"A pesquisa realizada com a empresa demonstrou que o método de avaliação de riscos de segurança da informação foi eficaz em identificar e priorizar os riscos existentes e não monitorados pela empresa. O método, que é baseado na análise de ativos, ameaças e vulnerabilidades, permitiu identificar uma série de riscos que

poderiam impactar negativamente as atividades da empresa, como o vazamento de dados, a interrupção dos serviços de TI e a perda de produtividade".

Destacam-se como pontos importantes mencionados pelo colaborador a adequação à LGPD, o colaborador destacou que o método de avaliação de riscos facilita a adequação da empresa à LGPD, apresentando de forma direcionada quais controles impactam e monitoram pontos relacionados com a lei.

"A adequação da empresa à LGPD também foi facilitada pelo método de avaliação de riscos, apresentando de maneira direcionada quais controles impactam e monitoram diretamente pontos relacionados com a lei. O método é robusto e flexível, o que o torna adequado para uma startup".

Potenciais Benefícios para a Empresa: O Colaborador 2 enfatizou que a avaliação ajuda na identificação dos processos que necessitam de correções e adequações para mitigar melhor os riscos às atividades da *startup*, assim como ajudar a propor itens relevantes para a melhoria da segurança da informação.

"A pesquisa apoiou na identificação dos processos que necessitam ser corrigidos e adequados para uma maior mitigação dos riscos às atividades da empresa. A pesquisa foi benéfica em propor os itens que seriam relevantes de maneira prioritária para a melhoria da segurança da informação na organização, apresentando através de cenários e análises qualitativas e quantitativas como e quanto a empresa pode melhorar com a aplicação dos controles indicados".

Colaborador 3 - Perspectiva sobre a Eficácia: O Colaborador 3 também achou o método eficaz e destacou que ele fornece uma visão geral dos requisitos de segurança aplicáveis à empresa.

"Acho eficaz, ajuda a ter uma visão geral dos requisitos de segurança que poderiam ou deveriam ser utilizados na empresa".

Potenciais Benefícios: Ele resumiu os benefícios como uma visão abrangente das falhas de segurança e um guia para a implementação de controles.

"Uma visão bem ampla de todas as falhas de segurança que a empresa pode ter, sendo um norte para a implementação dos controles".

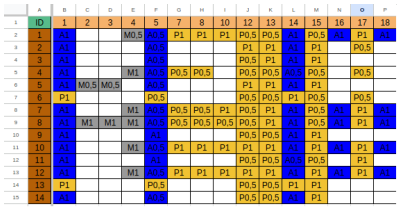
Sugestões de Melhoria: O colaborador sugeriu a inclusão de uma opção "parcialmente implementado"com explicações para melhorar o método.

Colaborador 4 - Perspectiva sobre a Eficácia: O Colaborador 4 demonstrou uma perspectiva otimista sobre o método, destacando sua base na LGPD e sua capacidade de difundir conceitos de segurança em startups.

"Visto que o método aplicado tem base na LGPD, na área de segurança da informação e Gestão de riscos e que os controles foram levantados visando o cenário de startups, tenho uma perspectiva bastante otimista, pois acaba difundindo conceitos legais de segurança nesse nicho, que geralmente é limitado pela falta de equipes especializadas para lidar com a segurança. A aplicação do método acaba gerando visibilidade para gestão tratar dessa problemática e embasamento para contornar as falhas existentes".

Potenciais Benefícios: Melhoria na visibilidade dos processos de tratamento de dados e maior alinhamento com as leis de proteção de dados.

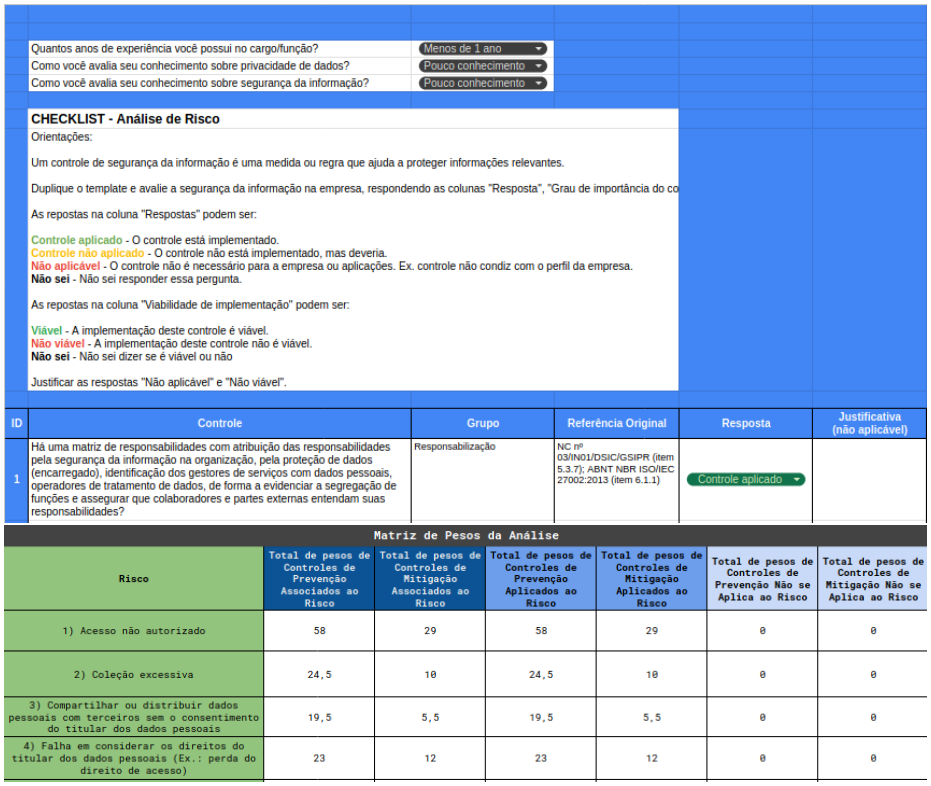
"Tenho pouco conhecimento na área de segurança da informação mas, na minha opinião, alguns benefícios que pude perceber através desse método são:



ID	1	2	3	4	5	7	8	10	12	13	14	15	16	17	18
1	A1			M0,5	A0,5	P1	P1	P1	P0,5	P0,5	A1	P0,5	A1	P1	A1
2	A1				A0,5				P1	P1	A1	P1		P0,5	
3	A1				A0,5				P0,5	P1	A1	P1			
4	A1			M1	A0,5	P0,5	P0,5		P0,5	P0,5	A0,5	P0,5		P0,5	
5	A1	M0,5	M0,5		A0,5				P1	P1	A1	P1			
6	P1				P0,5				P0,5	P0,5	P1	P0,5		P0,5	
7	A1			M1	A0,5	P0,5	P0,5	P1	P0,5	P1	A1	P0,5	A1	P1	A1
8	A1	M1	M1	M1	A0,5	P0,5	P0,5	P0,5	P0,5	P1	A1	P0,5	A1	P1	A1
9	A1				A1				P0,5	P0,5	A1	P1			
10	A1			M1	A0,5	P1	P1	P1	P1	P1	A1	P1	A1	P1	A1
11	A1				A1				P0,5	P0,5	A0,5	P0,5		P1	
12	A1			M1	A0,5	P1	P1	P1	P1	P1	A1	P1	A1	P1	A1
13	P1				P0,5				P0,5	P0,5	P1	P1			
14	A1				A0,5				P0,5	P0,5	A1	P1			

Orientações:
Um controle de segurança da informação é uma medida ou regra que ajuda a proteger informações relevantes.
Duplique o *template* e avalie a segurança da informação na empresa, respondendo as colunas "Resposta", "Grau de importância do controle", "Viabilidade de implantação":
As repostas na coluna "Respostas" podem ser:
Controle aplicado - O controle está implementado. Controle não aplicado - O controle não está implementado, mas deveria. Não aplicável - O controle não é necessário para a empresa ou aplicações. Ex. controle não condiz com o perfil da empresa. Não sei - Não sei responder essa pergunta.
As repostas na coluna "Viabilidade de implementação" podem ser:
Viável - A implementação deste controle é viável. Não viável - A implementação deste controle não é viável. Não sei - Não sei dizer se é viável ou não
Justificar as respostas "Não aplicável" e "Não viável".

Figura 2. (A) Matriz de pesos. (B) Orientações



Quantos anos de experiência você possui no cargo/função?	Menos de 1 ano
Como você avalia seu conhecimento sobre privacidade de dados?	Pouco conhecimento
Como você avalia seu conhecimento sobre segurança da informação?	Pouco conhecimento

CHECKLIST - Análise de Risco

Orientações:

Um controle de segurança da informação é uma medida ou regra que ajuda a proteger informações relevantes.

Duplique o template e avalie a segurança da informação na empresa, respondendo as colunas "Resposta", "Grau de importância do co

As repostas na coluna "Respostas" podem ser:

Controle aplicado - O controle está implementado.
Controle não aplicado - O controle não está implementado, mas deveria.
Não aplicável - O controle não é necessário para a empresa ou aplicações. Ex. controle não condiz com o perfil da empresa.
Não sei - Não sei responder essa pergunta.

As repostas na coluna "Viabilidade de implementação" podem ser:

Viável - A implementação deste controle é viável.
Não viável - A implementação deste controle não é viável.
Não sei - Não sei dizer se é viável ou não

Justificar as respostas "Não aplicável" e "Não viável".

ID	Controle	Grupo	Referência Original	Resposta	Justificativa (não aplicável)
1	Há uma matriz de responsabilidades com atribuição das responsabilidades pela segurança da informação na organização, pela proteção de dados (encarregado), identificação dos gestores de serviços com dados pessoais, operadores de tratamento de dados, de forma a evidenciar a segregação de funções e assegurar que colaboradores e partes externas entendam suas responsabilidades?	Responsabilização	NC nº 03/IN01/DSIC/GSIPR (item 5.3.7); ABNT NBR ISO/IEC 27002:2013 (item 6.1.1)	Controle aplicado	

Matriz de Pesos da Análise

Risco	Total de pesos de Controles de Prevenção Associados ao Risco	Total de pesos de Controles de Mitigação Associados ao Risco	Total de pesos de Controles de Prevenção Aplicados ao Risco	Total de pesos de Controles de Mitigação Aplicados ao Risco	Total de pesos de Controles de Prevenção Não se Aplica ao Risco	Total de pesos de Controles de Mitigação Não se Aplica ao Risco
1) Acesso não autorizado	58	29	58	29	0	0
2) Coleção excessiva	24,5	10	24,5	10	0	0
3) Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais	19,5	5,5	19,5	5,5	0	0
4) Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso)	23	12	23	12	0	0

Figura 3. (A) Fragmento do questionário; (B) Fragmento do resultado da avaliação.

melhoria na visibilidade dos processos de tratamento de dados, mesmo que a empresa não os armazene diretamente. Maior alinhamento com as leis de proteção de dados, passando mais credibilidade e confiança aos usuários/clientes. Outro benefício relevante, é contribuir para que a empresa se mantenha atualizada no mercado, visto que segurança da informação é um tema atual e de destaque na área de tecnologia, como podemos observar através de notícias, por exemplo, que evidenciam os impactos que falhas na segurança causam na vida das pessoas".

5 Conclusões e Trabalhos Futuros

Este trabalho adaptou e aplicou o método de avaliação de riscos do GARSP-SGD em uma aplicação de governança de dados de uma *startup*. O método proposto oferece orientações valiosas para aprimorar a segurança da informação e a privacidade em *startups*, identificando riscos específicos a que essas empresas estão expostas. Adicionalmente, este trabalho estimula discussões sobre questões cruciais relacionadas à segurança da informação e à privacidade nessas organizações.

É importante destacar que o sistema avaliado não foi originalmente desenvolvido com base em controles de segurança da informação e privacidade. Portanto, a ausência dos controles e o resultado de alto risco de segurança são compreensíveis. De fato, os controles são foram requisitos do projeto do original do sistema e os controles abordados pelo método abrangem aspectos que ainda não estão maduros na empresa, como a existência de uma equipe de respostas a incidentes cibernéticos. No entanto, os controles podem servir como orientações para futuras melhorias na organização e em seus sistemas, cumprindo o objetivo de conscientizar os gestores e funcionários sobre possíveis melhorias na segurança da informação e no tratamento dos dados pessoais.

No entanto, é fundamental reconhecer que, por se tratar de um levantamento baseado no GARSP-SGD, os riscos, o peso de cada controle e seus tipos são apenas sugestões e podem não refletir completamente a realidade da empresa. Portanto, é essencial que todo o processo de gestão de riscos seja aplicado, identificando, no contexto da empresa, quais riscos os gestores e funcionários acreditam que a empresa enfrenta e quais controles impactam esses riscos. Além disso, é necessário estabelecer prioridades para a implementação de controles. Após realizada as primeiras análises, o impacto das implantação dos controles deve ser medido em relação ao tempo e à implementação deles, avaliando em cada etapa o nível de risco num processo contínuo e interativo. Essas questões são cruciais para uma avaliação de riscos eficaz em uma empresa, especialmente para envolver a alta administração no processo, o que é um fator-chave para o sucesso.

Como trabalhos futuros pode-se avaliar os controles mais adequados para startups em uma pesquisa com múltiplas empresas, avaliando com gestores aqueles que são mais críticos e viáveis. A aplicação do método GARSP-SGP pode ser aplicado em diferentes fases de um sistema em desenvolvimento, acompanhando a implementação de cada controle desde a fase de coleta de requisitos até sua implantação. O método também pode evoluir como uma aplicação de gestão de riscos, onde painéis apoiariam os gestores na tomada de decisão e no acompa-

nhamento a implementação dos controles.

Agradecimentos. Este trabalho foi parcialmente apoiado pela FACEPE.

Referências

1. Alecrim, E.: Ministério da saúde expõe dados de 243 milhões de pessoas (2020), https://tecnoblog.net/noticias/2020/12/02/ministerio-saude-expoe-dados-243-milhoes-pessoas/
2. Associação Brasileira de Normas Técnicas (ABNT): ABNT NBR ISO/IEC 27005:2011 - Tecnologia da informação – Técnicas de segurança – Gestão de riscos em segurança da informação. ABNT, Rio de Janeiro, RJ, Brasil (2011)
3. Bisso, R., Kreutz, D., Rodrigues, G., Paz, G.: Vazamentos de dados: Histórico, impacto socioeconômico e as novas leis de proteção de dados. Revista Eletrônica Argentina-Brasil de Tecnologias da Informação e da Comunicação **3**(1) (2020)
4. BRASIL: LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Lei Geral de Proteção de Dados Pessoais (2018), https://www.planalto.gov.br/ccivil$_0$3/$_a$to2015 − 2018/2018/lei/l13709.htm
5. CERT.br, NIC.br, CGI.br: Fascículo: Vazamento de dados (2021), https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf
6. CISO: Ser pequena não significa que a empresa nunca sofrerá um ataque (2022), https://www.cisoadvisor.com.br/ser-pequena-nao-significa-que-a-empresa-nunca-sofrera-um-ataque/
7. de Proteção de Dados, A.A.N.: Guia de tratamento para agentes de pequeno porte (2021), https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf
8. Futsæter, N.: Best practices and motivational factors for information security in startups: An exploratory case study of four Norwegian tech startups. Master's thesis, NTNU (2019)
9. de Governo Digital, S.: Guia de avaliação de riscos de segurança e privacidade (2020), https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias-e-modelos
10. IBM: Cost of a data breach report 2022 (2022), https://www.ibm.com/reports/data-breach
11. for Internet Security, C.: Cis controls version 8 (2021), https://www.cisecurity.org/controls/cis-controls-list/
12. Kaila, U., Nyman, L.: Information security best practices: First steps for startups and smes. Technology Innovation Management Review **8**(11), 32–42 (2018)
13. Neto, G., Alencar, G., Queiroz, A.: Proposta de modelo de segurança simplificado para pequenas e médias empresas pp. 299–306 (2015)
14. Netto, D., Peixoto, M., Silva, C.: Privacy and security in requirements engineering: Results from a systematic literature mapping. In: Anais do WER19 - Workshop em Engenharia de Requisitos, Recife-PE, Brasil. Editora PUC-Rio (2019)
15. OWASP: Owasp proactive controls (2018), https://owasp.org/www-project-proactive-controls/
16. Silva Netto, A.d., Silveira, M.A.P.d.: Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. Journal of Information Systems and Technology Management **4**, 375–397 (2007)