Universidade Federal de Pernambuco
Centro de Informática

Graduação em Sistemas de Informação

Avaliação de Riscos de Segurança da Informação e Privacidade em Startup

Ewerton David Brito de Jesus

Trabalho de Graduação

Recife
21 de setembro de 2023

Universidade Federal de Pernambuco
Centro de Informática

Ewerton David Brito de Jesus

Avaliação de Riscos de Segurança da Informação e Privacidade em Startup

Trabalho apresentado ao Programa de Graduação em Sistemas de Informação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Orientadora: *Profa. Dra. Jéssyka Flavyanne Ferreira Vilela*

Recife
21 de setembro de 2023

Ficha de identificação da obra elaborada pelo autor,
através do programa de geração automática do SIB/UFPE

Jesus, Ewerton David Brito de.
Avaliação de riscos de segurança da informação e privacidade em startup / Ewerton David Brito de Jesus. - Recife, 2023.
63 p., tab.

Orientador(a): Jéssyka Flavyanne Ferreira Vilela
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Pernambuco, Centro de Informática, Sistemas de Informação - Bacharelado, 2023.
Inclui referências, apêndices.

1. LGPD. 2. Avaliação de riscos. 3. Segurança da Informação. 4. Privacidade. 5. Startups. I. Vilela, Jéssyka Flavyanne Ferreira. (Orientação). II. Título.

000 CDD (22.ed.)

À minha querida mãe Nazaré, pelo amor incondicional, apoio inabalável e pela luz que sempre guiou meu caminho. À minha amada irmã, Priscila, e aos meus sobrinhos, por serem minha inspiração diária e por compreenderem as ausências necessárias durante essa jornada. Ao meu estimado irmão, Marcelo, pelo suporte constante e pelo orgulho que compartilhamos em nossa trajetória. Dedico com carinho a Ana, que sempre me apoiou nos momentos mais difíceis.

E, por fim, dedico este trabalho ao meu amado pai, que não pôde testemunhar o término da minha jornada na universidade, mas que sempre se orgulhou das minhas conquistas e incessantemente me incentivou a buscar o conhecimento. Seu legado perdura em cada passo que dou, e esta conquista é também em sua honra.

Que esta dedicação represente o amor, apoio e gratidão que sinto por todos vocês, que tornaram possível a realização deste sonho.

Agradecimentos

Gostaria de expressar minha gratidão, à minha orientadora, Profa. Dra. Jéssyka Vilela. Sua orientação foi crucial para a conclusão deste trabalho, mas além disso, sua paciência, compreensão e apoio nos momentos mais desafiadores foram fundamentais. Também gostaria de expressar minha sincera gratidão aos amigos e colegas pelo incentivo e motivação.

A todos vocês, muito obrigado por fazerem parte deste capítulo da minha vida e por tornarem possível este momento tão importante. Suas contribuições foram cruciais e suas amizades inestimáveis.

Resumo

Nos últimos anos, diversas organizações têm enfrentado vazamentos de dados, expondo dados pessoais valiosos. Devido a esses incidentes e aos impactos negativos que causam nas pessoas envolvidas, leis de privacidade foram criadas para proteger as pessoas. A segurança da informação muitas vezes é negligenciada por empresas de pequeno porte. O trabalho se propõe a fazer uma avaliação de riscos de segurança da informação e privacidade de 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. 13 controles foram sugerido para melhorar a segurança na *startup*. O resultado da análise de risco reflete as dificuldades enfrentadas por esse tipo de empresa na implementação de controles de segurança da informação e privacidade.

Palavras-chave: LGPD, avaliação de riscos, segurança da informação, privacidade, startups

Abstract

In recent years, several organizations have faced data leaks, exposing valuable personal data. Because of these incidents and the negative impacts they have on the people involved, privacy laws have been created to protect people. Information security is often neglected by small companies. This research aims to carry out an information security and privacy risk assessment of a data governance application for a small technology startup. Of the 14 risks identified, most were at a high risk level, mainly due to a lack of financial resources and specialized professionals. 13 controls were suggested to improve security at the startup. The result of the risk analysis reflects the difficulties faced by this type of company in implementing information security and privacy controls.

Keywords: LGPD, risk assessment, information security, privacy, startups

Sumário

Lista de Figuras

Lista de Tabelas

CAPÍTULO 1

Introdução

1.1 Contexto

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 caso da Acesso Soluções de Pagamento S.A. que em 2021 sofreu um incidente que afetou mais de 160 mil pessoas, os dados vazados foram dados cadastrais como nome de usuário, CPF, instituição de relacionamento, número de agência e conta [4]. O Banco do Estado de Sergipe teve 395 mil usuários afetados em 2022 [5], os cibercriminosos tiveram acesso a um sistema interno do banco que registrava informações relacionadas ao Pix: nome, CPF, banco em que a chave está registrada, agência, conta, data da abertura da conta e data de registro da chave. Outro caso que ganhou espaço na mídia foi 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 dos cidadãos (incluindo pessoas falecidas). Dados como nome completo, endereço, telefone e CPF ficaram acessíveis a criminosos devido a credenciais de acesso inseridas de forma incorreta no código-fonte do site [6].

Esses vazamentos de dados ocorrem quando dados são acessados, coletados ou divulgados por pessoas, organizações ou cibercriminosos de forma não autorizada. Entre os dados frequentemente expostos estão as credenciais de acesso a sistemas (usuários e senhas), informações financeiras como cartões de crédito, documentos pessoais como RG e CPF, informações de contato como número de telefone, e-mail, registros de saúde e prontuários médicos. Os vazamentos podem ser originados por abuso de uma vulnerabilidade do sistema realizada por uma pessoa mal-intencionada, por código malicioso em ataque cibernético, acesso a contas de usuários que possuem senhas fracas ou vazadas, pela ação de funcionários ou ex-funcionários que coletam dados dos sistemas e repassam a terceiros [7].

Os vazamentos de dados 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 um vazamento de dados em 2022 foi de 4,35 milhões de dólares, segundo a pesquisa Cost of Data Breach encomendada pela IBM [8]. A pesquisa mostra também que os dados vazados mais valiosos são os dados pessoais dos usuários, sejam eles anonimizados ou não [8]. Devido a esses incidentes e aos impactos negativos que causam nas pessoas envolvidas, criou-se um cenário preocupante que 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 [9]. Um dos grandes marcos foi a criação da General Data Protection Regulation (GDPR) que serve de inspiração para outras regulamentações:

> "A União Europeia mantém em vigor desde 2018 seu regulamento geral, o General Data Protection Regulation (GDPR). Esse regulamento, impulsionou o Brasil na elaboração da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, publicada no Diário Oficial da União (D.O.U.) em 15/8/2018, com o objetivo de aprimorar a governança de dados pessoais pelos órgãos públicos, instituições e empresas [...]"[10].

As discussões sobre as leis de privacidade ganharam força nas empresas frente aos possíveis impactos, sejam eles financeiros, em sua reputação ou a seus usuários. De acordo com Bisso *et al.* [9], até recentemente, "[...] pouco se dava atenção à privacidade e a segurança de dados. Entretanto, os dados e exemplos de penalidades mostram que o cenário mudou drasticamente nos últimos anos, isto é, estes assuntos tornaram-se uma prioridade de estado". É possível notar que esse é um assunto de extrema importância.

Porém, muitas organizações não estão preparadas para se adaptar ao novo cenário. Uma pesquisa realizada pelo Serasa em 2020 [11] com 513 empresas mostra que apenas 50% das empresas estão preparadas até a entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil. Empresas de menor porte apresentam níveis menores de preparo e conhecimento em relação a lei, já que "quanto maior a empresa, maiores os níveis de conhecimento e preparação para a LGPD [...] Em média, 73% das empresas que já tinham conhecimento estavam preparadas, e esse percentual foi para 86% entre as de grande porte".

Para evitar serem sancionadas, as empresas precisam desenvolver meios de proteger os dados pessoais de seus funcionários, clientes e usuários, aplicando as diretrizes estabelecidas pela lei. Para isso, é dever dos gestores analisarem a segurança da informação e privacidade, identificando as lacunas que precisam ser sanadas e propor medidas para mitigá-las, aumentando a aderência da empresa às leis e protegendo os valiosos dados de seus usuários. Neste contexto, este trabalho propõe-se a conduzir uma avaliação dos riscos relacionados à segurança da informação e à privacidade em uma aplicação de governança de dados de uma *startup*. O objetivo é auxiliar os gestores na identificação desses riscos e na proposição de controles de segurança da informação e privacidade que contribuam para a sua mitigação.

1.2 Justificativa

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. De acordo com Futsæter [12], essas empresas 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. Além disso, elas manuseiam dados valiosos para criminosos, como informações de cartões de crédito e dados de saúde de pacientes. Outras características comuns incluem imaturidade e limitações de recursos humanos e financeiros. É de extrema importância direcionar esforços para auxiliar as *startups* a melhorar sua segurança da informação, uma vez que isso reduz o risco de ataques cibernéticos. De acordo com um estudo da Accenture sobre os custos do cibercrime, 43% dos ataques cibernéticos são direcionados a pequenas empresas, sendo que apenas 14% delas estão preparadas para se defender [13].

Para alcançar o objetivo de proporcionar maior segurança a esse tipo de empresa, a implementação de um processo de gestão de riscos de segurança da informação é fundamental, pois permite que a organização identifique os riscos aos quais está exposta, criando um processo formal para avaliar a probabilidade da ocorrência e as consequências desses riscos [14]. Portanto, é crucial fornecer ferramentas que auxiliem os gestores na identificação de medidas que possam melhorar a segurança de suas empresas. Levando em consideração que a segurança cibernética muitas vezes é negligenciada por empresas de pequeno porte [13], a atenção dos gestores a essas questões, com orientações claras sobre as necessidades de segurança da empresa, resulta em uma proteção mais eficaz dos dados pessoais de seus usuários e reduz a probabilidade de incidentes, conforme mencionado anteriormente.

1.3 Objetivos

O principal objetivo deste trabalho é apoiar *startups* de tecnologia de pequeno porte a identificar lacunas na segurança da informação e privacidade, deixando-as mais próximas de estarem adequadas às diretrizes da LGPD. Para este fim, o trabalho se propõe a fazer uma avaliação de riscos de segurança da informação e privacidade de uma aplicação de governança de dados de uma *startup* de tecnologia de pequeno porte.

Os objetivos específicos do trabalho são:

- Revisar literatura sobre os controles de segurança e privacidade para análise de riscos e para *startup*.
- Adequar o método do Guia de Avaliação de Riscos de Segurança e Privacidade da Secretaria de Governo Digital (GARSP-SGD) [1] para avaliar uma *startup*.
- Aplicar o método de avaliação proposto ao sistema de uma *startup*.
- Propor medidas para minimizar os riscos encontrados.

Dentre as contribuições deste trabalho, destaca-se a utilização de um método de avaliação de risco desenvolvido por órgão do Governo Federal, como é o caso do método de avaliação de riscos utilizado na avaliação da *startup*, no setor privado. Sendo assim, este trabalho colabora com a difusão da sua implementação e aprimora sua aplicação através dos resultados obtidos em um novo tipo de organização. Como resultado, visa ajudar a melhorar a segurança da informação e privacidade em *startup*, identificando os riscos aos quais estão expostas.

1.4 Estrutura

O trabalho está estruturado da seguinte forma, no Capítulo 2 é feita uma fundamentação teórica sobre os principais conceitos abordados pelo trabalho. A Lei Geral de Proteção de Dados Pessoais é introduzida, apresentando ao leitor seu objetivo, conceitos relevantes, seus principais componentes. Em seguida, é explicado o conceito de segurança da informação e controles

de segurança da informação. O capítulo também aborda o Guia de Avaliação de Risco de Segurança e Privacidade da Secretaria do Governo Digital (GARSP-SGD) [1] em detalhes e por fim, apresenta os trabalhos relacionados. No Capítulo 3, é apresentada a metodologia do trabalho, como os dados foram coletados, o perfil da empresa, da aplicação e dos colaboradores que responderam ao questionário. No Capítulo 4, é apresentada a planilha eletrônica utilizada na avaliação de risco, mostra sua estrutura e funcionalidades. No Capítulo 5, os resultados da etapa de seleção e escolha e refinamento dos controles pesquisados, assim como os resultados da avaliação de risco são apresentados. No Capítulo 6 a conclusão do trabalho a partir dos resultados obtidos juntamente com as contribuições do trabalho e trabalhos futuros.

CAPÍTULO 2

Fundamentação Teórica

2.1 Lei Geral de Proteção de Dados Pessoais (LGPD)

A Lei Geral de Proteção de Dados Pessoais (LGPD) entrou em vigor em setembro de 2020, sendo a primeira regulamentação abrangente de proteção de dados do Brasil. "Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural." [15]. A partir de sua criação, empresas de diferentes setores se viram na necessidade de estarem em conformidade com a lei, como mostra Almeida [10], "[...] com a publicação das diretrizes postas pela LGPD, organizações e/ou instituições, se viram diante da obrigatoriedade de se adequar com lisura as normativas para a efetivação de tratamento de dados, objetivando a proteção dos direitos fundamentais de privacidade, ética e de liberdade, princípio da transparência". A LGPD é um marco na busca pela proteção de dados pessoais dos cidadãos brasileiros.

2.1.1 Aplicação da Lei

A LGPD define o escopo de sua aplicação como "[...] qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados."[15]. Ela pode ser aplicada nas operações de tratamento desde que: (I) sejam realizadas em território nacional; (II) tenha como objetivo a oferta de bens ou serviços para pessoas no Brasil; (III) os dados pessoais tenham sido coletados em território nacional. Com exceção dos dados coletados para fins jornalísticos, artísticos ou acadêmicos. Assim como exclui, dados coletados para segurança pública, defesa nacional, segurança de Estado ou atividades de investigação de infrações penais [15].

Para aplicação da lei, define-se os papéis dos agentes de tratamento, que são o controlador, a quem compete as decisões sobre o tratamento de dados, o operador que é a pessoa ou organização que trata os dados em nome do controlador e o titular dos dados que é a pessoa a quem se referem os dados pessoais. Segundo o Guia de Boas Práticas LPGD [16], "antes de iniciar alguma espécie de tratamento de dados pessoais, o agente deve se certificar previamente que a finalidade da operação esteja registrada de forma clara e explícita e os propósitos especificados e informados ao titular dos dados". Para este fim, a LGPD define dez hipóteses de tratamento de dados chamadas de bases legais.

2.1.2 Bases Legais

O tratamento de dados pessoais poderá ser realizado desde que enquadrado em uma das hipóteses elencadas na lei. Ou seja, caso os agentes de tratamento não atendam a uma das hipóteses, não possuem a permissão para executar o tratamento de dados. As hipóteses são enumeradas no Art. 7º da lei:

1. Mediante consentimento do titular;
2. Para o cumprimento de obrigação legal ou regulatória;
3. Para a execução de políticas públicas;
4. Para a realização de estudos e pesquisas;
5. Para a execução ou preparação de contrato;
6. Para o exercício de direitos em processo judicial, administrativo ou arbitral;
7. Para a proteção da vida ou da incolumidade física do titular ou de terceiro;
8. Para a tutela da saúde do titular;
9. Para atender interesses legítimos do controlador ou de terceiro;
10. Para proteção do crédito.

2.1.3 Princípios de tratamento

Além de estar enquadrado em uma hipótese legal, o tratamento de dados pessoais, que é a atividade definida na LGPD, precisa também garantir que dez princípios estejam sendo respeitados [15]. Conforme previsto no Art. 5º, são eles:

1. **Finalidade**: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

2. **Adequação**: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

3. **Necessidade**: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

4. **Livre acesso**: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

5. **Qualidade dos dados**: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

6. **Transparência**: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

7. **Segurança**: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

8. **Prevenção**: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

9. **Não discriminação**: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

10. **Responsabilização e prestação de contas**: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

2.1.4 Direitos dos titulares

A LGPD estabeleceu uma estrutura legal que dá aos titulares de dados direitos que devem ser respeitados pelos agentes de tratamento em todo percurso do tratamento de dados. O Art. 18º afirma que:

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> I - confirmação da existência de tratamento;
> II - acesso aos dados;
> III - correção de dados incompletos, inexatos ou desatualizados;
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
> (Redação dada pela Lei nº 13.853, de 2019) Vigência VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei

2.2 Segurança da informação

A segurança da informação pode ser definida como uma área do conhecimento que tem por objetivo proteger os ativos de informação de uma organização contra acessos não autorizados,

alterações indevidas ou sua indisponibilidade, conforme apontado por Sêmola [17]. "Organizações de todos os tipos e tamanhos (incluindo o setor privado e público, organizações comerciais e sem fins lucrativos), coletam, processam, armazenam e transmitem informações em diferentes formatos, incluindo o eletrônico, físico e verbal"[18]. Segundo Neto [19], “a informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida”. Para alcançar esse objetivo, os ativos de informação necessitam estar de acordo com os três princípios básicos da segurança da informação.

Confidencialidade: O princípio da confidencialidade, segundo Sêmola [17], afirma que "toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas às pessoas a quem é destinada". Dantas [20] também afirma que ocorre a quebra da confidencialidade quando a informação é acessada por indivíduos não autorizados, assegurando que a informação mantenha seu valor e impedindo que ela seja divulgada sem autorização. Assim como também significa que os dados transmitidos entre um emissor e destinatário por meio de redes de comunicação, não tenha seu conteúdo acessado, de forma acidental ou proposital, por terceiros [21].

Integridade: O princípio da integridade afirma que a informação não deve ter seu conteúdo alterado e que "seja mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais"[17]. "Ocorre a quebra da integridade quando a informação é corrompida, falsificada, roubada ou destruída. Garantir a integridade é manter a informação na sua condição original."[20] Alguns exemplos de quebra da integridade incluem:

> "[...] inserções, substituições ou exclusões de parte do conteúdo da informação; as alterações nos seus elementos de suporte, que podem ocorrer quando são realizadas alterações na estrutura física e lógica onde ela está armazenada, ou quando as configurações de um sistema são alterados para se ter acesso a informações restritas, bem como são superadas as barreiras de segurança de uma rede de computadores. [20]"

Disponibilidade: o princípio da disponibilidade significa que "toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que eles necessitem delas para qualquer finalidade"[17]. É garantir a prestação contínua do serviço, sem interromper o fornecimento de informações, para as pessoas e serviços interessados [21].

2.2.1 Controles de Segurança da Informação

Para tornar a informação segura, é necessário aplicar um conjunto adequado de medidas, sejam elas políticas, processos, procedimentos, software e hardware [18]. As medidas são chamadas de controles de segurança da informação, como afirma Sêmola:

> "[...] são as práticas, os procedimentos e os mecanismos usados para a proteção da informação e seus ativos, que podem impedir que ameaças explorem vulnerabilidades, reduzir essas vulnerabilidades, limitar a probabilidade ou o impacto de sua exploração, minimizando ou mesmo evitando os riscos"[17].

A ISO/IEC 27002 [18] também acrescenta que os controles "precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos"[18]. Os controles de segurança da informação também podem ser chamados de mecanismos de segurança da informação [17]. Os controles de segurança da informação, podem ser classificados como preventivos, detectivos e corretivos.

Controles preventivos: essa classificação de controles tem como objetivo impedir que incidentes de segurança da informação aconteçam, de forma a diminuir a probabilidade da ocorrência dos incidentes [17]. Alguns exemplos são:

1. Políticas de segurança;
2. Instruções e procedimentos de trabalho;
3. Campanhas e palestras de conscientização de usuários;
4. Especificações de segurança;
5. Equipamentos de controle de acesso;
6. *Firewall*;
7. Antivírus;
8. Configurações adequadas de roteadores e dos sistemas operacionais.

Controles detectivos: essa classificação de controle tem por objetivo identificar ameaças que possam explorar alguma vulnerabilidade da organização [17]. Alguns exemplos são:

1. Análise de riscos;
2. Sistemas de detecção de intrusão;
3. Alertas de segurança;
4. Câmeras de vigilância;
5. Alarmes.

Controles corretivos: essa classificação de controles objetiva a criação de ações que possam diminuir o impacto de vulnerabilidades que foram exploradas por pessoas ou programas mal-intencionados [17]. Como exemplo:

1. Equipes para emergências;
2. Restauração de backup;
3. Plano de continuidade operacional;

4. Plano de recuperação de desastres.

Os controles de segurança podem não estar limitados a apenas uma classificação, como exemplo do plano de continuidade de negócios que é tanto uma ação para prevenir (controle preventivo) quando é criado na organização, quanto uma ação de mitigação (controle corretivo), pois, a partir de sua aplicação, diminui o impacto das vulnerabilidades exploradas [17].

Para adotar controles de segurança da informação, a organização precisa realizar um planejamento para identificar os riscos aos quais está sujeita e determinar quais controles precisa implementar. A partir disso, realizar o monitoramento para verificar se os controles implementados estão funcionando corretamente e quais ações corretivas devem ser adotadas. Em resumo, "a adoção de controles, tanto de gestão como de segurança é parte essencial da autorregulação realizada pela gestão da organização"[22].

2.2.2 CIS Controls V8

Os controles do *Center for Internet Security* (CIS) [2] refletem o conhecimento combinado de especialistas de empresas, governos e indivíduos de diversas funções em diferentes setores da economia que criam, adotam e apoiam os controles CIS em seus respectivos ambientes. Os controles do CIS são um conjunto de medidas que ajudam a mitigar os ataques cibernéticos contra sistemas e redes. Por ser uma fonte confiável de controles de segurança a nível global, é um importante instrumento a ser levado em consideração quando se trata da segurança da informação.

A partir da constatação do *framework* de que empresas de pequeno porte podem ter dificuldades com a adoção das medidas de segurança iniciais, apresentando dificuldade em aplicar medidas posteriores [2], o CIS criou Grupos de Implementação de Controles CIS (IGs) para ajudar empresas de diferentes portes a aplicar os controles de acordo com suas necessidades. A seleção dos IGs é feita a partir de uma autoavaliação das empresas, ou seja, a empresa analisa sua realidade e seleciona o grupo de controles adequado. Os controles são agrupados de forma a serem aplicados a empresas com perfis de risco semelhantes. O grupo IG1 (Tabela 2.1) se refere ao "[...] conjunto básico de medidas de segurança de defesa cibernética que toda empresa deve aplicar para se proteger contra os ataques mais comuns"[2].

Item	Nome do Controle	Grupo do Controle
1.1	Estabelecer e manter um inventário detalhado de ativos corporativos	Inventário e controle de ativos corporativos
1.2	Endereçar ativos não autorizados	Inventário e controle de ativos corporativos
2.1	Estabelecer e manter um inventário de software	Inventário e controle de ativos de software
2.2	Assegurar que o software autorizado seja atualmente suportado	Inventário e controle de ativos corporativos
2.3	Endereçar o software não autorizado	Inventário e controle de ativos corporativos

3.1	Estabelecer e manter um processo de gestão de dados	Proteção de dados
3.2	Estabelecer e manter um inventário de dados	Proteção de dados
3.3	Configurar listas de controle de acesso a dados	Proteção de dados
3.4	Aplicar retenção de dados	Proteção de dados
3.5	Descartar dados com segurança	Proteção de dados
3.6	Criptografar dados em dispositivos de usuário final.	Proteção de dados
4.1	Estabelecer e manter um processo de configuração segura	Configuração segura de ativos corporativos e software
4.2	Estabelecer e Manter um Processo de Configuração Segura para a Infraestrutura de Rede	Configuração segura de ativos corporativos e software
4.3	Configurar o bloqueio automático de sessão nos ativos corporativos	Configuração segura de ativos corporativos e software
4.4	Implementar e gerenciar um firewall nos servidores	Configuração segura de ativos corporativos e software
4.5	Implementar e gerenciar um firewall nos dispositivos de usuário final	Configuração segura de ativos corporativos e software
4.6	Gerenciar com segurança os ativos e software corporativos	Configuração segura de ativos corporativos e software
4.7	Gerenciar contas padrão nos ativos e software corporativos	Configuração segura de ativos corporativos e software
5.1	Estabelecer e manter um inventário de contas	Gestão de contas
5.2	Usar senhas exclusivas	Gestão de contas
5.3	Desabilitar contas inativas	Gestão de contas
5.4	Restringir privilégios de administrador a contas de Administrador dedicadas	Gestão de contas
6.1	Estabelecer um Processo de Concessão de Acesso	Gestão do controle de acesso
6.2	Estabelecer um Processo de Revogação de Acesso	Gestão do controle de acesso
6.3	Foi elaborada uma política de privacidade para o serviço?	Gestão do controle de acesso
7.1	Estabelecer e manter um processo de gestão de vulnerabilidade	Gestão contínua de vulnerabilidades
7.2	Estabelecer e manter um processo de remediação	Gestão contínua de vulnerabilidades
7.3	Executar a gestão automatizada de patches do sistema operacional	Gestão contínua de vulnerabilidades
7.4	Executar a gestão automatizada de patches de aplicações	Gestão contínua de vulnerabilidades
8.1	Estabelecer e manter um processo de gestão de log de auditoria	Gestão de registros de auditoria
8.2	Coletar logs de auditoria	Gestão de registros de auditoria
8.3	Garantir o armazenamento adequado do registro de auditoria	Gestão de registros de auditoria

9.1	Garantir o uso apenas de navegadores e clientes de e-mail suportados plenamente	Proteções de e-mail e navegador Web
9.2	Usar serviços de filtragem de DNS	Proteções de e-mail e navegador Web
10.1	Instalar e manter um software anti-malware	Defesas contra malware
10.2	Configurar atualizações automáticas de assinatura anti-malware	Defesas contra malware
10.3	Desabilitar a execução e reprodução automática para mídias removíveis	Defesas contra malware
11.1	Estabelecer e manter um processo de recuperação de dados	Recuperação de dados
11.2	Executar backups automatizados	Recuperação de dados
11.3	Proteger os dados de recuperação	Recuperação de dados
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	Recuperação de dados
12.1	Assegurar que a infraestrutura de rede esteja atualizada	Gestão da infraestrutura de rede
14.1	Estabelecer e manter um programa de conscientização de segurança	Conscientização sobre segurança e treinamento de competências
14.2	Treinar membros da força de trabalho para reconhecer ataques de engenharia social	Conscientização sobre segurança e treinamento de competências
14.3	Treinar membros da força de trabalho nas melhores práticas de autenticação	Conscientização sobre segurança e treinamento de competências
14.4	Treinar a força de trabalho nas Melhores Práticas de Tratamento de Dados	Conscientização sobre segurança e treinamento de competências
14.5	Treinar membros da força de trabalho sobre as causas da exposição não intencional de dados	Conscientização sobre segurança e treinamento de competências
14.6	Treinar Membros da força de trabalho no Reconhecimento e Comunicação de Incidentes de Segurança	Conscientização sobre segurança e treinamento de competências
14.7	Treinar a força de trabalho sobre como identificar e comunicar se o seus ativos corporativos estão faltando atualizações de segurança	Conscientização sobre segurança e treinamento de competências
14.8	Treinar a força de trabalho sobre os perigos de se conectar e transmitir dados corporativos em redes inseguras	Conscientização sobre segurança e treinamento de competências
15.1	Estabelecer e manter um inventário de provedores de serviços	Gestão de provedor de serviços
16.1	Estabelecer e manter um processo seguro de desenvolvimento de aplicações	Segurança de aplicações

17.1	Designar Pessoal para Gerenciar Tratamento de Incidentes	Gestão de respostas a incidentes
17.2	Estabelecer e manter informações de contato para relatar incidentes de segurança	Gestão de respostas a incidentes
17.3	Estabelecer e manter um processo corporativo para relatar incidentes	Gestão de respostas a incidentes

Tabela 2.1: Lista de controles CIS [2]

2.2.3 Guia de Boas Práticas - ANPD

Além dos controles CIS, outra referência de controles foi o Guia de Boas Práticas para Agentes de Tratamento de Pequeno Porte lançado em outubro de 2021 pela ANPD [3]. Este guia foi desenvolvido com objetivo de apresentar medidas de segurança da informação que possam proteger os dados pessoais tratados por agentes de tratamento de pequeno porte (microempresas, empresas de pequeno porte, startups, empresas de inovação), pois estes possuem menos recursos humanos e financeiros para se protegerem, o que leva a necessidade de criar um conjunto de orientações diferenciado estas empresas estarem em conformidade com a LGPD [3].

Os controles são sugeridos no capítulo três “medidas de segurança da informação”, eles estão agrupados em medidas administrativas: política de segurança da informação, conscientização e treinamento e gerenciamento de contratos. Para medidas técnicas, os grupos: controle de acesso, segurança de dados pessoais armazenados, segurança das comunicações, programa de gerenciamento de vulnerabilidades, medidas relacionadas ao uso de dispositivos móveis, medidas relacionadas ao serviço de nuvem. Ao todo 29 controles relevantes foram identificados e estão expostos na Tabela 2.2.

Item	**Nome do Controle**	**Grupo**
3.1.1	Existência da política de segurança da informação	Política de segurança da informação
3.1.2	Conscientização e Treinamento para funcionários	Conscientização e Treinamento
3.1.2	Reportar incidentes e vulnerabilidades	Conscientização e Treinamento
3.1.3	Termos de confidencialidade (non-disclosure agreement - NDA)	Gerenciamento de contratos
3.1.3	Gestão de Contratos e Aquisição com observância à LGPD	Gerenciamento de contratos
3.1.3	Cláusulas de proteção de dados nos contratos de TI com terceiros	Gerenciamento de contratos
3.1.3	Sistema de controle de acesso: aplicável a todos usuários	Controle de acesso
3.1.3	Sistema de controle de acesso: senhas fortes	Controles de acesso
3.1.3	Sistema de controle de acesso: evitar configuração padrão	Controles de acesso
3.1.3	Sistema de controle de acesso: evitar compartilhamento de senhas	Controles de acesso
3.1.3	Sistema de controle de acesso: principio do menor privilégio	Controles de acesso

3.1.3	Sistema de controle de acesso: utilizar a autenticação multi-fatores (MFA)	Controles de acesso
3.2.2	Processamento de dados deve ser feito apenas com dados necessários para finalidade.	Segurança dos dados pessoais armazenados
3.2.2	Implementar soluções que dificultem a identificação do titular, como as técnicas de pseudonimização	Segurança dos dados pessoais armazenados
3.2.2	Usar configurações de segurança nas estações de trabalho e evitar transferência de dados para dispositivos de armazenamento externo	Segurança dos dados pessoais armazenados
3.2.2	Realizar backups regulares, armazenados em locais seguros	Segurança dos dados pessoais armazenados
3.2.2	Formatar mídias físicas ou digitais antes de descartar	Segurança dos dados pessoais armazenados
3.2.2	Estabelecer em contrato eliminação dos dados	Segurança dos dados pessoais armazenados
3.2.3	Nas comunicações, utilizar conexões cifradas (com uso de TLS/HTTPS) ou aplicativos com criptografia fim a fim.	Segurança das comunicações
3.2.3	Gerenciamento de trafego de rede (firewall, antivirus, email, antispam, filtros).	Segurança das comunicações
3.2.3	Remover qualquer dado pessoal que esteja em redes públicas, como o site da empresa	Segurança das comunicações
3.2.4	Para monitorar e aplicar correções de sistemas e aplicativos lançadas pelos servidores.	Manutenção de programa de gerenciamento de vulnerabilidades
3.2.4	Manter antivírus e antimalwares sempre atualizados e com varreduras periódicas em todos os dispositivos da empresa.	Manutenção de programa de gerenciamento de vulnerabilidades
3.3	Estejam sujeitos aos mesmos procedimentos de controle de acesso dos outros equipamentos de TI.	Medidas relacionadas ao uso de dispositivos móveis
3.2.2	Deve-se separar os dispositivos móveis de uso privado daqueles de uso institucional.	Medidas relacionadas ao uso de dispositivos móveis
3.3	Implementação de funcionalidade que permita apagar todos os dados no dispositivo, de forma remota, para ser usada em caso de perda ou roubo do equipamento.	Medidas relacionadas ao uso de dispositivos móveis
3.4	Contrato de acordo de nível de serviço (SLA – Service Level Agreement)	Medidas relacionadas ao serviço em nuvem

3.4	Serviço de nuvem deve atender requisitos de segurança da informação	Medidas relacionadas ao serviço em nuvem
3.4	Utilização de autenticação de múltiplos fatores para usuários na Nuvem	Medidas relacionadas ao serviço em nuvem

Tabela 2.2: Lista de controles ANPD para agentes de tratamento de pequeno porte [3]

2.2.4 OWASP Proactive Controls

A *Open Web Application Security Project* (OWASP) é uma organização que sem fins lucrativos, cujo seu principal objetivo é orientar profissionais e empresas a desenvolverem software seguro. É conhecida por seu levantamento dos 10 principais riscos de segurança da informação OWASP Top 10. A OWASP criou um catálogo de medidas de segurança que mitigam os principais riscos de segurança da informação. Essas medidas são chamadas de Top 10 Proactive Controls e seu objetivo é "despertar consciência sobre segurança de aplicações descrevendo as áreas mais preocupantes que desenvolvedores de software devem estar cientes"[23]. O OWASP define 10 controles que devem ser aplicados em empresas:

1. C1: Defina os Requisitos de Segurança
2. C2: Aproveite os Frameworks e Bibliotecas de Seguras
3. C3: Acesso seguro à base de dados.
4. C4: Codifique e Escape os Dados.
5. C5: Valide todas as entradas.
6. C6: Implementar Identidade Digital
7. C7: Aplique controles de acesso
8. C8: Proteja os dados em todos os lugares
9. C9: Implementar registro e monitoramento de segurança
10. C10: Lidar com todos os erros e exceções

2.3 Guia de Avaliação de Riscos de Segurança e Privacidade

Um importante conceito que influencia diretamente no sucesso de uma empresa é a gestão de riscos. “Basicamente, podemos entender a gestão de risco como uma tentativa de minimizar as fontes de riscos de segurança da informação, por meio da análise e da avaliação dos elementos

que constituem a segurança da informação" [19]. Neste contexto, o risco pode ser definido como "um evento hipotético, cuja ocorrência pode afetar de forma positiva ou negativa uma organização" [22]. A gestão de riscos tem o efeito de fazer um sistema funcionar de forma adequada mesmo diante de eventos ocasionados por agentes maliciosos, acidentes, mau uso ou desastres naturais [22].

Lançado em novembro de 2020, o Guia de Avaliação de Riscos de Segurança e Privacidade da Secretaria de Governo Digital (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 análises de sistemas críticos no setor público. A avaliação de risco é uma das etapas do processo de gestão de risco definida na norma ABNT NBR ISO/IEC 27005. Ela compreende a identificação, análise e avaliação dos riscos [14]. "A Identificação do Risco é o processo de encontrar, listar e caracterizar os elementos ou fatores dos riscos. Durante a identificação, várias análises são efetuadas, e pode ser empregado um amplo arcabouço de técnicas"[22]. A análise de riscos determina a magnitude ou nível de cada risco individual e pode empregar métodos qualitativos e quantitativos, atribuindo níveis para as probabilidades e consequências de cada risco [22]. Os controles de segurança da informação são de suma importância nesse processo, pois a partir de sua implementação, agem diretamente nos riscos, o resultado da aplicação de controles em relação à riscos é chamado de "risco residual"[22].

O objetivo do método GARSP-SGD é "fornecer aos responsáveis pelo tratamento de dados pessoais no órgão ou entidade uma orientação para identificar lacunas de segurança da informação e de privacidade sobre os sistemas, contratos e processos da instituição"[1]. O método tem foco no serviço público ajudando instituições 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 ajuda a aumentar a maturidade dos sistemas em relação a sua segurança. Além disso, com a entrada em vigor da LGPD, o método foi adaptado para atender não apenas a segurança da informação, mas a critérios de privacidade também, ajudando as instituições a se adequarem à lei.

O GARSP-SGD traz originalmente um conjunto de 113 controles de segurança da informação e privacidade esses controles foram coletados de *frameworks* e normas existentes como a ISO/IEC 27002, OWASP e portarias do Governo Federal (Apêndice **??**). A partir da implementação ou não desses controles, é que os níveis de risco do sistema serão calculados. Cabe ressaltar que o GARSP-SGD foi feito para ser flexível, então a instituição é livre para alterar, incluir ou excluir os controles a partir de suas necessidades.

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"[1].

2.3.1 Riscos de segurança e privacidade

O GARSP-SGD traz um conjunto de riscos de segurança da informação que foram elencados no Relatório de Impacto à Proteção de Dados do Comitê Central de Governança de Dados, esse relatório é uma "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos funda-

mentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco"[15]. Os riscos foram adaptados da norma ISO/IEC 29134:2017 que trata de técnicas de segurança para a avaliação de impacto à privacidade. É uma norma que fornece diretrizes para a realização de uma avaliação de impacto à privacidade (PIA), esse processo identifica e avalia os riscos potenciais à privacidade associados a um novo sistema, processo ou produto. O método GARSP-SGD traz ao todo 14 riscos de segurança da informação e privacidade que foram adaptados a partir dos riscos elencados pela norma ISO/IEC 29134.

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 fora da administração pública federal sem o consentimento do titular dos dados pessoais**: Instituição não atende sua finalidade legal e compartilha os dados sem consentimento do titular dos dados pessoais (LGPD, art. 27).

4. **Falha em considerar os direitos do titular dos dados pessoais**: Garantia de atendimento dos direitos do titular, conforme descrito nos artigos 17 a 23 da LGPD.

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.)**

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 transparente e 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 de uma 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 identificados por cruzamento simples de 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 prestação de um serviço ou do prazo para 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 internas do controlador/operador19, 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.

13. **Tratamento sem consentimento do titular dos dados pessoais (caso o tratamento não esteja previsto em legislação ou regulação pertinente)**:Controlador de dados pessoais não obtém consentimento do titular para realizar um tratamento de dados pessoais sem embasamento legal.

14. **Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular**: A realização de operação de processamento de dados pessoais deve estar em conformidade com a LGPD. Qualquer operação de processamento que não atenda este requisito pode produzir informações com vinculações ou associações indevidas.

2.3.2 Avaliação de riscos

O método GARSP-SGD se baseia no fato de que os controles agem mitigando ou prevenindo determinados riscos, de acordo com os pesos pré-definidos, eles representam um grau de importância em relação ao risco [1], a Tabela 2.3 apresenta os valores adotados pelo método. Quando um controle mitiga um risco, ele está diminuindo o impacto na ocorrência deste. Já no caso dos controles de prevenção, eles diminuem a probabilidade de ocorrência. Um controle pode atuar em ambos os casos, diminuindo a probabilidade e impacto em relação aos riscos. Quando os controles não se aplicam ao sistema, não afetam a probabilidade ou impacto. O inicio da avaliação do sistema começa com o nível de risco mais alto, pois assume-se que os controles ainda não foram implementados.

Peso	Descrição
0	Controle não se aplica
0,5	Controle se aplica
1	Controle se aplica e prioritário

Tabela 2.3 Pesos adotados pelo GARSP-SGD [1]

Para definir a associação entre os controles e cada risco, o método também apresenta uma matriz (Figura 2.1) que relaciona os controles aos riscos, seu grau de importância e os tipos de controle nas diferentes cores: prevenção na cor amarela, mitigação na cor cinza e ambos na cor azul. As informações na matriz, "orientarão a obtenção do nível de risco para o sistema que trata dados pessoais"[1].

2.3.3 Cálculo do risco

Para calcular o nível de risco a qual uma organização está sujeita, o GARSP-SGD busca "medir, a partir da entrada das respostas atribuídas aos controles (aplicado, não aplicado e não se aplica), o nível de risco para os riscos aos quais o sistema está exposto". Para isso, é necessário calcular a probabilidade da ocorrência do risco:

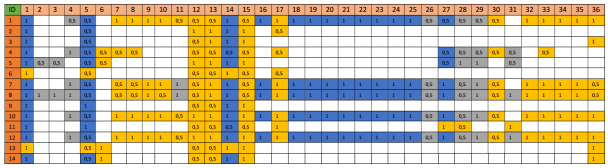


Figura 2.1 Matriz de risco [1]

> "Para se obter a probabilidade de determinado risco, calcula-se primeiramente a soma de todos os pesos dos controles de prevenção associados a ele que foram identificados como 'aplicado', visto que determinados controles podem não ser aplicáveis a ele, nem ao sistema."[1]

Em seguida, subtrai-se desse valor, a soma de todos os pesos dos controles que não se aplicam ao risco. Por fim, divide-se os dois valores para obter a probabilidade de ocorrência do risco. O resultado final é a probabilidade de ocorrência de um risco. Para calcular o impacto, deve-se somar os pesos dos controles de mitigação. Obtendo assim, o cálculo do impacto. Se todos os controles forem aplicados, temos um valor de probabilidade igual a 1 e se nenhum controle for aplicado, temos o valor igual a 0. Logo, quanto mais próximo de 1, maior a quantidade de controles aplicados (implementados) que reduzem a probabilidade de ocorrência ou impacto daquele risco [1]. As fórmulas a seguir descrevem em detalhes o cálculo de probabilidade e impacto.

- Sendo $P =$ Probabilidade.
- Sendo $I =$ Impacto.
- Sendo $X =$ Peso total dos controles associados ao risco (prevenção ou mitigação).
- Sendo $Y =$ Peso total dos controles aplicados ao risco (prevenção ou mitigação).
- Sendo $Z =$ Peso total dos controles que não se aplicam ao risco.

Cálculo de probabilidade:

$$P = \frac{X_{\text{Prevenção}}}{Y_{\text{Prevenção}} - Z_{\text{Prevenção}}}$$

Cálculo do impacto:

$$I = \frac{X_{\text{Mitigação}}}{Y_{\text{Mitigação}} - Z_{\text{Mitigação}}}$$

Os valores resultantes são comparados com a tabela na Figura 2.2 que se refere aos níveis de classificação do risco baseado na porcentagem de controles implementados. À medida que os controles são implementados, a classificação da probabilidade ou do impacto é reduzida. O GARSP-SGD também define parâmetros escalares para avaliação de riscos, os parâmetros definidos pelo documento são: Baixo (5), Moderado (10) e Alto (15). As organizações têm a liberdade de alterar esses valores com base em sua realidade.

Controles implementados	Probabilidade	Impacto
0 a 50 por cento	Alta	
50 a 85 por cento	Moderada	Alto
85 a 100 por cento	Baixa	Moderado

Figura 2.2 Classificação do risco [1]

Por fim, a matriz de probabilidade e impacto (Figura 2.3) é obtida a partir dos parâmetros escalares, multiplicando a probabilidade pelo impacto, resultando no nível ou grau de magnitude do risco. No modelo, a classificação do nível de risco é dado pelas cores verde, que significa risco baixo; amarelo, que significa risco médio e vermelho, que significa risco alto.

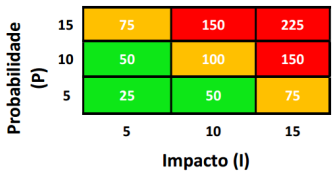


Figura 2.3 Matriz de probabilidade e impacto [1]

2.4 Trabalhos relacionados

2.4.1 Gestão da Segurança da Informação: Fatores que influenciam sua adoção em pequenas e médias empresas

O artigo "Gestão da Segurança da Informação: Fatores que influenciam sua adoção em pequenas e médias empresas" [24] se propôs a analisar a implementação de medidas de segurança da informação em indústrias de pequeno e médio porte na região do interior de São Paulo. Para atingir seus objetivos, a pesquisa fez um levantamento com 43 indústrias do setor de fabricação de produtos de metal. Avaliando 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 obtidos pela pesquisa revelaram que, apesar da preocupação demonstrada pelas empresas em relação à segurança da informação, há uma deficiência na atenção dada tanto à camada humana quanto à camada lógica. Esses resultados ressaltam a necessidade de direcionar o foco não apenas para soluções tecnológicas, mas também para a conscientização e treinamento dos colaboradores [24]. Outro resultado de relevância é a identificação do antivírus como a ferramenta mais amplamente adotada para garantir a segurança da informação. Além disso, 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 uma baixa adequação, sugerindo que muitas empresas não implementaram todos os controles recomendados [24]. A pesquisa também ressaltou que a motivação principal para a adoção da gestão da segurança da informação é a prevenção de perdas financeiras, destacando a importância da mensuração financeira como um grande incentivo. Por outro lado, a falta de conhecimento foi identificada como um possível fator inibidor, apontando

para a necessidade de educação e treinamento contínuos em segurança da informação [24].

2.4.2 Modelo de Segurança Simplificado para Pequenas e Médias Empresas

O trabalho de Neto *et al.* [25] apresenta um estudo que avalia a implementação de medidas de segurança da informação entre as Pequenas e Médias Empresas (PMEs). Os autores conduziram um estudo que 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 profissionais de Tecnologia da Informação que atuam nas PMEs [25].

O modelo simplificado foi enviado para 51 profissionais das áreas de tecnologia da informação e comunicação com um questionário que 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. Outra análise feita pelos autores é 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"[25]. Por fim, o artigo conclui, por meio da observação dos dados, que há uma carência de práticas e modelos de segurança nas empresas de pequeno e médio porte [25].

2.4.3 Information Security Best Practices: First Steps for Startups and SMEs

O artigo "*Information Security Best Practices: First Steps for Startups and SMEs*"[26] apresenta uma abordagem para implementar práticas de segurança da informação em pequenas e médias empresas (PMEs). Os autores propõem uma abordagem baseada no ciclo PDCA (Plan, Do, Check, Act), amplamente utilizado em *frameworks* de governança da segurança da informação. O texto 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 [26].

O *framework* proposto pelos autores compreende quatro fases [26]. 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, nesta 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 apresentado a necessidade de um plano de recuperação de desastres. Isso 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 [26]. 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 (*Service Level Agreement*) e detecção de *malware*, são mencionadas[26].

CAPÍTULO 3

Metodologia

Neste capítulo, é apresentada a metodologia que guiou este trabalho sobre avaliação de riscos de segurança da informação e privacidade em *startups*. Este trabalho foi realizado como um estudo de caso, envolvendo a coleta de dados e aplicação do método de avaliação de riscos proposto em uma *startup* de pequeno porte. Ao longo deste capítulo, é descrito cada etapa da metodologia, destacando seu propósito e contribuição.

3.1 Etapa 1: Pesquisa de controles de segurança da informação e privacidade

O GARSP-SGD [1] 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 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 [2], 10 Open Source Foundation for Application Security (OWASP) [23], 22 controles o Modelo de Segurança Simplificado para Pequenas e Médias Empresas [25] e 28 controles do Guia de Boas Práticas para Agentes de Tratamento de Pequeno Porte [3]. No total, 108 controles foram identificados e organizados em planilhas. A relação de controles pesquisados é explicada na Seção **??**. A lista completa de controles pode ser consultada em Apêndice A.

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 a metodologia utilizada pelo 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.

3.2 Etapa 2: Seleção de controles e refinamento

A etapa de seleção e filtro 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.

Para fazer a seleção dos controles foi aplicado o seguinte critério:

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 *startup* já tenha sido abordado, o controle é mantido.
3. Caso o controle para *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. Na Seção **??** a seleção de controles é apresentada em detalhes.

3.3 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 de avaliação de riscos e apresentando os resultados de forma fácil de visualizar e facilitar a tomada de decisão. A planilha eletrônica está descrita no Seção 4.1.

3.4 Etapa 4: Seleção de uma startup para avaliação

O critério utilizado para a escolha da *startup* foi "amostragem por conveniência". Isso se deve à facilidade de acesso do autor aos gestores e funcionários da *startup*. A empresa selecionada é

uma *startup* 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.

3.5 Etapa 5: Aplicação do método de avaliação de riscos 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.

- Engenharia de Software: 2
- Engenharia de Dados: 1
- DevOps: 1
- Gerente de Projetos: 1

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. Como mostrado na Tabela 3.1, a avaliação dos controles para *startups* foi realizada em dois encontros feitos em aplicação de videoconferência e aplicação método de avaliação de riscos feitos a partir de questionários em planilha eletrônica. O modelo do questionário pode ser consultado na Seção 4.1.

3.6 Etapa 6: Levantamento dos resultados

Na última etapa deste trabalho, os resultados obtidos a partir das respostas aos questionários e da aplicação do método de avaliação de riscos foram sintetizados na Seção 5.2. 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

Data	Duração	Objetivo
14/03/2023	2h	avaliar controles SGD
20/03/2023	40m	avaliar controles SGD
23/03/2023	1h	aplicar método com gerente de projetos
12/09/2023	1h	aplicar método com colaboradores

Tabela 3.1 Entrevistas

um conjunto 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*. A sugestão de controles pode ser consultada na Seção 5.4. Em seguida, os comentário dos colaborados a respeito da aplicação do método GARSP-SGD é mostrado na Seção **??**.

CAPÍTULO 4

Planilha Eletrônica de Avaliação de Riscos

4.1 Descrição da planilha eletrônica

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 (Figura 4.1) 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	B	C	D
1	ID	Controle	Grupo	Referência Original
2	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)
3	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);
4	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);
5	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);
6	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	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	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);

Figura 4.1 Lista de controles presentes na planilha.

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 Figura 4.2.

	A	B	C
1	ID	Risco	Descrição
2	1	Acesso não autorizado	Acesso indevido (permissões indevidas) a um ambiente físico ou lógico.
3	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.
4	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).
6	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.
7	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.
8	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.
9	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.
10	9	Reidentificação de dados pseudonimizados	Dados pessoais podem ser reidentificados por cruzamento simplesde dados pessoais (LGPD,art. 12 e 13).
11	10	Remoção não autorizada	Usuário não tem a permissão para retirar ou copiar dados pessoais para outro local.
12	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.
13	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 4.2 Lista de riscos presentes na planilha.

Na aba "Matriz"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).

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	ID	1	2	3	4	5	7	8	10	12	13	14	15	16	17	18
2	1	A1			M0,5	A0,5	P1	P1	P1	P0,5	P0,5	A1	P0,5	A1	P1	A1
3	2	A1				A0,5				P1	P1	A1	P1		P0,5	
4	3	A1				A0,5				P0,5	P1	A1	P1			
5	4	A1			M1	A0,5	P0,5	P0,5		P0,5	P0,5	A0,5	P0,5		P0,5	
6	5	A1	M0,5	M0,5		A0,5				P1	P1	A1	P1			
7	6	P1				P0,5				P0,5	P0,5	P1	P0,5		P0,5	
8	7	A1			M1	A0,5	P0,5	P0,5	P1	P0,5	P1	A1	P0,5	A1	P1	A1
9	8	A1	M1	M1	M1	A0,5	P0,5	P0,5	P0,5	P0,5	P1	A1	P0,5	A1	P1	A1
10	9	A1				A1				P0,5	P0,5	A1	P1			
11	10	A1			M1	A0,5	P1	P1	P1	P1	P1	A1	P1	A1	P1	A1
12	11	A1				A1				P0,5	P0,5	A0,5	P0,5		P1	
13	12	A1			M1	A0,5	P1	P1	P1	P1	P1	A1	P1	A1	P1	A1
14	13	P1				P0,5				P0,5	P0,5	P1	P1			
15	14	A1				A0,5				P0,5	P0,5	A1	P1			

Figura 4.3 Matriz de pesos.

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:

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

Em seguida o seguinte texto de orientação é apresentado:

> 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".

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 Figura 4.4 apresenta o questionário utilizado na avaliação de riscos.

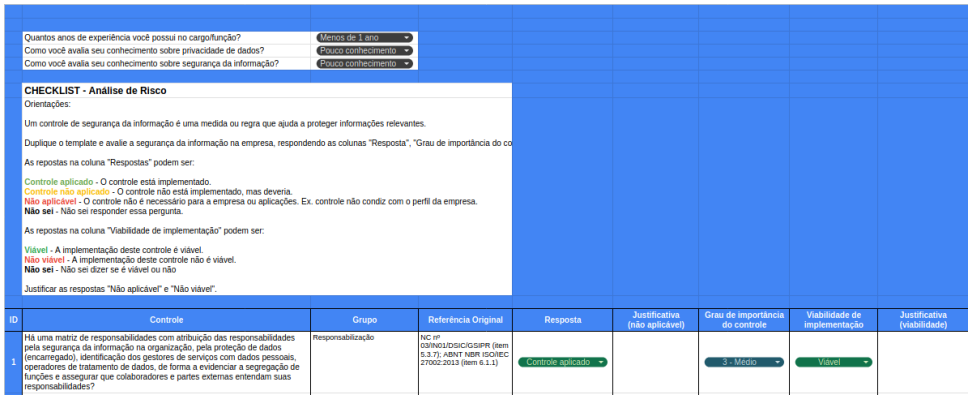


Figura 4.4 Questionário de controles.

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 de resposta. Por exemplo, se "Controle Aplicado"tiver a maior quantidade de respostas, o resultado para o controle é "APLICADO". Se a quantidade maior de respostas 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 Figura 4.5 demonstra como são apresentadas essas informações ao usuário.

Análise de Risco de Segurança da informação e Privacidade

Legenda	
APLICADO	Controle implementado
NAO APLICADO	Controle não implementado
NAO SE APLICA	Controle não necessário para o sistema

Legenda
Mitigação (M)
Prevenção (P)
Mitigação e Prevenção (A)
Controle não ativo

Atualizar

Análise do Sistema

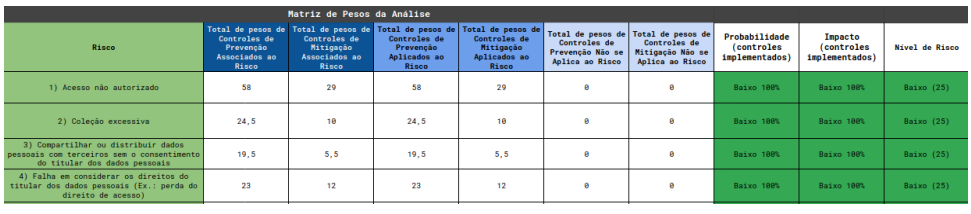
Controle	1	2	3	4	5	7	8	10	12
Nível de importância	Médio	Médio	Médio	Médio	Médio	Médio	Médio	Médio	Médio
Viabilidade	Viável	Viável	Viável	Viável	Viável	Viável	Viável	Viável	Viável
Respostas Aplicado	1	1	1	1	1	1	1	1	1
Respostas Não aplicado	0	0	0	0	0	0	0	0	0
Respostas Não aplicável	0	0	0	0	0	0	0	0	0
Avaliação Final	APLICADO	APLICADO	APLICADO	APLICADO	APLICADO	APLICADO	APLICADO	APLICADO	APLICADO

Figura 4.5 Questionário de controles.

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 a soma dos pesos de cada controles nas seguintes colunas:

- Total de pesos de Controles Associados ao Risco: soma dos pesos de todos os controles associados ao risco.
- Total de pesos de Controles Aplicados ao Risco: soma dos pesos dos controles implementados.
- 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 já apresentados na Seção 2.3.3 deste documento. A avaliação final é feita na coluna "Nível de Risco"como mostra a seguinte Figura 4.6.



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	Probabilidade (controles implementados)	Impacto (controles implementados)	Nível de Risco
1) Acesso não autorizado	58	29	58	29	0	0	Baixo 100%	Baixo 100%	Baixo (25)
2) Coleção excessiva	24,5	10	24,5	10	0	0	Baixo 100%	Baixo 100%	Baixo (25)
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	Baixo 100%	Baixo 100%	Baixo (25)
4) Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso)	23	12	23	12	0	0	Baixo 100%	Baixo 100%	Baixo (25)

Figura 4.6 Resultado da avaliação de risco.

CAPÍTULO 5

Resultados

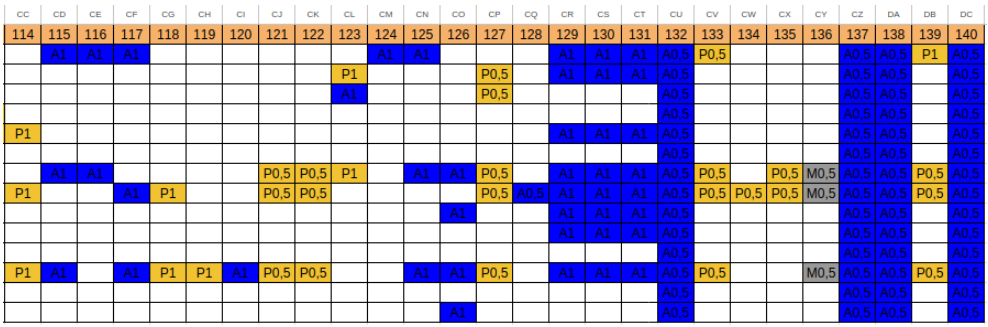
5.1 Consolidação dos controles encontrados

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 Apêndice A 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 (Apêndice A). Os controles que não foram citados na pesquisa de controles para *startup* foram removidos, ao todo foram 34 controles. A Tabela 5.1 resume os resultados da etapa de seleção e refinamento dos controles.

Controles	**Quantidade**
Controles GARSP-SGD	113
Controles *startup*	108
Controles duplicados	79
Controles removidos	34
Controles novos	27
Controles finais	106

Tabela 5.1 Resultado da etapa de refinamento de controles.

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). A matriz de pesos resultante pode ser consultada na Figura 5.1.



CC	CD	CE	CF	CG	CH	CI	CJ	CK	CL	CM	CN	CO	CP	CQ	CR	CS	CT	CU	CV	CW	CX	CY	CZ	DA	DB	DC
114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140
	A1	A1	A1							A1	A1				A1	A1	A1	A0,5	P0,5				A0,5	A0,5	P1	A0,5
									P1				P0,5		A1	A1	A1	A0,5					A0,5	A0,5		A0,5
									A1				P0,5					A0,5					A0,5	A0,5		A0,5
																		A0,5					A0,5	A0,5		A0,5
P1															A1	A1	A1	A0,5					A0,5	A0,5		A0,5
																		A0,5					A0,5	A0,5		A0,5
	A1	A1					P0,5	P0,5	P1		A1	A1	P0,5		A1	A1	A1	A0,5	P0,5		P0,5	M0,5	A0,5	A0,5	P0,5	A0,5
P1			A1	P1			P0,5	P0,5					P0,5	A0,5	A1	A1	A1	A0,5	P0,5	P0,5	P0,5	M0,5	A0,5	A0,5	P0,5	A0,5
												A1			A1	A1	A1	A0,5					A0,5	A0,5		A0,5
															A1	A1	A1	A0,5					A0,5	A0,5		A0,5
																		A0,5					A0,5	A0,5		A0,5
P1	A1		A1	P1	P1	A1	P0,5	P0,5			A1	A1	P0,5		A1	A1	A1	A0,5	P0,5			M0,5	A0,5	A0,5	P0,5	A0,5
																		A0,5					A0,5	A0,5		A0,5
												A1						A0,5					A0,5	A0,5		A0,5

Figura 5.1 Matriz de pesos dos novos controles.

5.2 Aplicação do método de avaliação de riscos de segurança e privacidade

Através das respostas obtidas pela planilha eletrônica enviada para os 5 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 [1]. Uma visão geral da aplicação do método é apresentada na Tabela 5.2. 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 ferramenta desenvolvida para a avaliação de riscos. Uma segunda rodada de análise foi realizada, envolvendo colaboradores de diferentes áreas (Seção 3.5). Nas seções subsequentes, são apresentados os resultados dos níveis de risco, os controles aplicados e não aplicados.

Categoria	**Resultado**
Controles aplicados	40
Controles não aplicados	41
Controles não se aplicam	25
Total de controles	106

Tabela 5.2 Resultado da aplicação do método.

5.2.1 Lista de controles aplicados

A seguir estão listados os controles considerados aplicados nos projetos da *startup*, ou seja, os controles estão implementados. A lista foi obtida através das respostas ao questionário presente na planilha eletrônica enviada aos colaboradores da *startup*.

ID	**Controle**	**Resultado**
3	São implementados mecanismos e procedimentos para mitigar ataques de negação de serviço, tais como balanceamento de carga, proxy, firewall, etc.?	Aplicado
7	O local que processa as informações é restrito somente ao pessoal autorizado?	Aplicado
10	O acesso externo aos sistemas é provido de meios de segurança que protegem a confidencialidade e integridade dos dados trafegados, tais como o uso de VPN?	Aplicado
14	Há uma avaliação de impactos potenciais, riscos e consequências, incluindo impactos de segurança cibernética, quando da identificação de necessidade de mudanças?	Aplicado
15	As mudanças são comunicadas para todas as partes interessadas?	Aplicado

ID	Controle	Resultado
16	Existe um prazo formalmente definido para o tratamento de vulnerabilidades técnicas relevantes identificadas?	Aplicado
32	É exigida autorização de prévia de autoridade competente para liberação de credenciais em sistemas, bancos de dados e serviços de segurança (VPN) que suportam o serviço, seja para atividade fim ou para atividade de desenvolvimento?	Aplicado
40	Há redundância dos recursos de processamento da informação suficiente para atender aos requisitos de disponibilidade previstos em contrato?	Aplicado
41	Foi elaborada uma política de privacidade para o serviço?	Aplicado
48	O sistema em análise segue uma política de senha com definição de tamanho mínimo e formato?	Aplicado
49	As informações das credenciais de acesso dos usuários estão gravadas em recursos de tecnologia da informação protegidos e sob a forma criptografada?	Aplicado
50	As informações das credenciais de acesso dos usuários são transmitidas de forma protegida?	Aplicado
51	Um mecanismo de recuperação de senha está implementado de forma a assegurar a recuperação da senha de maneira segura, sem fornecimento de senha por parte da aplicação, e que obrigue a alteração de senha do usuário no primeiro acesso?	Aplicado
52	Uma análise crítica de direitos de acesso é realizada em um período de tempo previamente definido ou a qualquer momento depois de qualquer mudança nos direitos de usuários ou para verificação de incidentes de segurança? Essas mudanças são registradas em um inventário de contas para controle?	Aplicado
53	Há mecanismos para encerramento (expirar) de qualquer sessão cuja inatividade do usuário exceda um período de tempo predeterminado?	Aplicado
59	O log registra as ações executadas pelos usuários?	Aplicado
60	O log registra data e hora do evento com alguma fonte de tempo sincronizada?	Aplicado
63	Requisitos de segurança são identificados e considerados em todas as fases do projeto do sistema?	Aplicado
64	Existem controles de versão para garantir a gestão dos códigos-fonte?	Aplicado
65	As mensagens de erro do sistema não revelam detalhes da sua estrutura interna?	Aplicado
67	O servidor da aplicação fornece opções de protocolos criptográficos para conexão em versões seguras, estáveis e atualizadas? Nas comunicações, utilizar conexões cifradas (com uso de TLS/HTTPS) ou aplicativos com criptografia fim a fim.	Aplicado
77	O acesso para realizar as operações de tratamento de dados pessoais é provido ao número mínimo de indivíduos necessários para executar as operações de tratamento?	Aplicado
78	Meios de autenticação forte são providos para o processamento dos dados pessoais, em especial os dados sensíveis (dados de saúde e demais dados previstos pelo art.5º, II da LGPD))? Exemplo: autenticação de múltiplos fatores.	Aplicado
79	A empresa controla por meio de um processo formal a concessão de direitos de acesso privilegiado para o processamento de dados?	Aplicado
83	O compartilhamento ou transferência de dados pessoais é realizado por meio de um canal criptografado e de cifra recomendada?	Aplicado
85	Acordos de confidencialidade, termos de responsabilidade, termos de sigilo são assinados com os órgãos e operadores de dados pessoais? É importante que os termos e acordos informem a respeito dos itens a seguir, mas a eles não se limitem: tipos de tratamento de dados pessoais a serem realizados por quem irá receber os dados; ações requeridas quando do encerramento do compartilhamento, como destruição dos dados, responsabilidade e ações dos signatários para evitar a divulgação não autorizada dos dados pessoais; base legal para o compartilhamento; direito de auditar e monitorar as atividades que envolvem os dados pessoais; processo para notificar ou relatar vazamentos; violações ou divulgações não autorizadas dos dados pessoais; ações a serem tomadas diante da violação do acordo; e outras medidas possíveis.	Aplicado
86	Os contratos firmados com os operadores contêm cláusulas que contemplam, não se limitando a: uma declaração adequada sobre a escala, natureza e finalidade do processamento contratado; relatar casos de violação de dados, processamento não autorizado ou outro não cumprimento dos termos e condições contratuais; medidas aplicáveis na rescisão do contrato, especialmente no que diz respeito à exclusão segura de dados pessoais; impedimento de tratamento de dados pessoais por subcontratados, exceto por aprovação do controlador?	Aplicado
90	O serviço oferecido pelo provedor do serviço em nuvem atende os requisitos de segurança da informação estabelecidos pela empresa?	Aplicado
105	No processamento de dados, é utilizado o mínimo necessário de dados pessoais para atingir a finalidade pretendida?	Aplicado
108	A empresa implementa processos para que o tratamento dos dados pessoais seja preciso, completo, atualizado, adequado e relevante para a finalidade de uso?	Aplicado
115	Os ativos e softwares corporativos são gerenciados com segurança? Por exemplo: gestão de configuração por meio de version-controlled-infrastructure-as-code e acesso a interfaces administrativas por meio de protocolos de rede seguros, como Secure Shell (SSH) e Hypertext Transfer Protocol Secure (HTTPS)?	Aplicado
116	As contas padrão nos ativos e software corporativos, como root, administrador e outras contas de fornecedores pré-configuradas são gerenciadas com segurança? Exemplos de implementações podem incluir: desativar contas padrão, torná-las inutilizáveis, assim como trocar as senhas.	Aplicado
117	Apenas as contas de administador dedicadas possuem privilégios de administrador nos ativos corporativos? Realize atividades gerais de computação, como navegação na Internet, e-mail e uso do pacote de produtividade, a partir da conta primária não privilegiada do usuário.	Aplicado
123	O termo de confidencialidade (non-disclosure agreement - NDA) é assinado pelos funcionários da empresa para que estes se comprometam a não divulgar informações confidenciais que envolvam dados pessoais?	Aplicado
128	São utilizadas bibliotecas e frameworks de fontes confiáveis que são ativamente mantidas e utilizadas por muitas aplicações? Crie e mantenha um catálogo com todas as bibliotecas de terceiros e proativamente mantenha atualizado.	Aplicado
129	As bases de dados possuem mecanismos ativo de proteção como permitir consultar seguras via parametrização de consultas, configuração segura ativa em todos os bancos de dados, autenticação seja feita por canais seguros de comunicação (criptografados)?	Aplicado
130	Técnicas de codificação (Encoding) e escape dos dados são utilizadas para evitar ataques do tipo injeção (sql injection, code injection)?	Aplicado
131	A aplicação checa se os dados recebidos estão sintaticamente e semanticamente corretos antes de serem utilizados de qualquer forma? Ex. uso de expressões regulares no input dos dados.	Aplicado
133	É implementado um sistema de controle de acesso aplicável a todos os usuários, com níveis de permissão na proporção da necessidade de trabalhar com o sistema e de acessar dados pessoais? Esse sistema pode, por exemplo, permitir a criação, aprovação, revisão e exclusão de contas dos usuários.	Aplicado
137	Os contrato de aquisição de serviços de nuvem possuem acordo de nível de serviço contemplando a segurança dos dados armazenados?	Aplicado
138	O serviço oferecido pelo provedor do serviço em nuvem atende os requisitos de segurança da informação estabelecidos pela empresa?	Aplicado

Tabela 5.3: Lista de controles aplicados na empresa.

5.2.2 Lista de controles não aplicados

A seguir estão listados os controles considerados não aplicados na startup, ou seja, controles que os respondentes avaliam como não implementados, mas que deveriam ser. A lista foi obtida através das respostas ao questionário presente na planilha eletrônica enviada aos colaboradores da *startup*.

ID	Controle	Resultado
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?	Não aplicado

ID	Controle	Resultado
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?	Não aplicado
4	Existe um Plano de Continuidade de Negócio, que garanta o nível adequado de continuidade para a segurança da informação durante uma situação adversa?	Não aplicado
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.	Não aplicado
12	É realizado o controle de mudanças em atualizações de software e outros componentes das soluções de TIC, assegurando que estes estejam atualizados?	Não aplicado
17	Há um inventário completo e atualizado dos ativos de informação, contendo o fornecedor, o número da versão, os dados pessoais processados, a classificação dos dados pessoais (sensíveis ou apenas dados pessoais), quais softwares estão instalados e em quais sistemas, e a(s) pessoa(s) na organização responsável(s) pelos ativos?	Não aplicado
18	Há um processo de análise e monitoramento de vulnerabilidades?	Não aplicado
21	Existem formalmente e são executados procedimentos específicos para resposta aos incidentes, contemplando: a definição de incidente; o escopo da resposta; quando e por quem as autoridades devem ser contatadas; papéis, responsabilidades e autoridades; avaliação de impacto do incidente; medidas para reduzir a probabilidade e mitigar o impacto do incidente; descrição da natureza dos dados pessoais afetados; as informações sobre os titulares de dados pessoais envolvidos; procedimentos para determinar se um aviso para indivíduos afetados e outras entidades designadas (por exemplo, órgãos reguladores) é necessário?	Não aplicado
22	Os ativos de informação estão configurados de forma a registrar todos os eventos relevantes de segurança da informação, contendo, pelo menos, a identificação inequívoca do usuário, a natureza do evento, a data, hora e fuso horário, o identificador do ativo de informação, as coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento?	Não aplicado
23	Há um sistema para monitoramento de aplicações, alertas e vulnerabilidades utilizado para auxiliar na detecção e tratamento de incidentes de segurança cibernética (IPS, IDS, etc.)?	Não aplicado
24	O plano de comunicação foi atualizado para incluir os contatos que devem ser notificados, caso haja uma violação de privacidade, ou para reportar detalhes de processamento, como contatos com a autoridade de proteção de dados e/ou grupos diretamente relacionados?	Não aplicado
27	Há uma política ou norma de backup que aborde os procedimentos operacionais que padronizam os processos de geração de cópias de segurança e recuperação de arquivos, assim como os processos de controle de acesso, armazenamento, movimentação e descarte das mídias que contêm cópias de segurança?	Não aplicado
28	Está estabelecida a abrangência dos procedimentos de backup para cada tipo de informação (por exemplo, completa ou diferencial)?	Não aplicado
29	É definido a abrangência dos testes de backup e sua periodicidade, de forma que os testes sejam planejados observando as dependências e relacionamentos entre sistemas, considerando inclusive os ambientes de continuidade de negócios, com o objetivo de minimizar a possibilidade de que a ausência de sincronismo entre os dados inviabilize ou dificulte sua recuperação?	Não aplicado
31	O período de retenção das cópias de segurança e os requisitos de releitura são predefinidos, levando-se em consideração os requisitos de negócio, contratuais, regulamentares ou legais?	Não aplicado
33	Existe e é executado um processo formal de desenvolvimento de sistema seguro? Trate de itens como: padrões de design de aplicação seguro, práticas de codificação seguras, treinamento de desenvolvedor, gestão de vulnerabilidade, segurança de código de terceiros e procedimentos de teste de segurança de aplicação.	Não aplicado
37	É realizada periodicamente uma análise/avaliação de riscos da arquitetura da Solução de TIC, indicando os eventos de risco e seus respectivos níveis de risco ao qual o sistema está exposto, baseada em prévia análise de vulnerabilidades dos ativos que compõem a Solução de TIC?	Não aplicado
38	Os recursos de segurança da informação e de tecnologia da informação encontram-se em versões seguras, estáveis e atualizadas?	Não aplicado
42	Existe Relatório de Impacto à Proteção de Dados Pessoais, conforme previsto na Lei 13.709 de 14 de agosto de 2018; relacionado à solução de TIC?	Não aplicado
43	Há um inventário completo e atualizado dos dados pessoais, contendo os agentes de tratamento (controlador e operador), encarregado, descrição do fluxo de tratamento dos dados pessoais (como são coletados, armazenados, processados, retidos e eliminados), abrangência da área geográfica do tratamento (nacional, estadual, municipal), finalidade do tratamento dos dados pessoais, categoria dos dados pessoais (identificação pessoal, financeiros, características pessoais, outros), categoria de dados sensíveis, dados pessoais compartilhados e transferência internacional?	Não aplicado
45	Há utilização de criptografia para a proteção dos dados sensíveis ou críticos armazenados em dispositivos móveis, mídias removíveis ou em banco de dados?	Não aplicado
46	Existe uma frequência estabelecida para geração dos backups?	Não aplicado
47	São realizadas cópias de segurança dos logs de acordo com períodos de retenção, que consideram os requisitos de negócio, contratuais, regulamentares ou legais?	Não aplicado
55	O sistema implementa restrições/limitadores para sucessivas tentativas de acesso mal-sucedidas?	Não aplicado
57	O log registra identificação do usuário, incluindo administrador e acessos privilegiados?	Não aplicado
58	O log registra endereço IP ou outro atributo que permita a identificação de onde o usuário efetuou o acesso?	Não aplicado
61	Os logs gerados são protegidos, quando da geração, contra edição e exclusão?	Não aplicado
88	O desenvolvimento dos sistemas tem como base os riscos e as medidas de segurança identificadas no RIPD (Relatório de Impacto de Proteção à Dados Pessoais)?	Não aplicado
89	O desenvolvimento dos sistemas é orientado à proteção da privacidade dos dados pessoais (Privacy by Design)?	Não aplicado
91	Há uma política ou norma de proteção de dados pessoais que aborde a finalidade da empresa perante o processamento de dados; a transparência com relação à coleta e processamento de dados pessoais; a estrutura estabelecida para a proteção de dados pessoais; regras para tomar decisões em questões de proteção de dados pessoais; critérios de aceitação de risco de privacidade; compromisso de satisfazer os requisitos aplicáveis de proteção à privacidade?	Não aplicado
93	É implementada e mantida uma estratégia abrangente de treinamento e conscientização, destinada a garantir que os envolvidos (funcionários, usuários e desenvolvedores) entendam suas responsabilidades e os procedimentos de proteção de dados pessoais?	Não aplicado
99	É realizada uma análise periódica sobre os dados coletados, se eles continuam limitados ao mínimo necessário para o atendimento a finalidade?	Não aplicado
114	Foi estabelecido um processo de configuração segura para ativos corporativos (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos não computacionais/IoT; e servidores), software (sistemas operacionais e aplicações) e dispositivos de rede?	Não aplicado
118	As atualizações do sistema operacional e de aplicações em ativos corporativos são realizadas por meio da gestão automatizada de patches de forma mensal ou com mais frequência?	Não aplicado
124	É vedado o compartilhamento de contas ou de senhas entre funcionários, visto que isso é um vetor crítico de vulnerabilidade de segurança da informação?	Não aplicado
125	Os usuários de um sistema possuem o menor nível de acesso necessário para a realização de suas atividades? Funções de alto nível, tais como as de administrador de sistema, devem ser restringidas apenas àqueles funcionários que necessitem exercer esse papel e sejam capazes de assumir essa responsabilidade. Esse é o princípio do menor privilégio (need to know)	Não aplicado
126	São aplicadas técnicas de técnicas de pseudonimização em dados armazenados sensíveis que dificultem a identificação do titular? Um exemplo dessa técnica é a criptografno ia.	Não aplicado
127	São adotadas medidas para evitar a transferência de dados pessoais de estações de trabalho para dispositivos de armazenamento externo, como pendrives, discos rígidos externos, dentre outros, tendo em vista o risco de se perder a guarda dos dados pessoais transferidos? Caso essa operação seja imprescindível, sugere-se a adoção de controles adicionais a esses dispositivos externos, como inventariá-los, cifrar os dados e armazená-los em locais seguros.	Não aplicado

ID	Controle	Resultado
140	A organização possui procedimentos operacionais documentados e acessíveis, abrangendo atividades como inicialização e desligamento de sistemas, geração de cópias de segurança, manutenção de equipamentos, tratamento de mídias e segurança da informação? Esses procedimentos incluem instruções para configuração de sistemas, processamento de informações, agendamento de tarefas, tratamento de erros, contatos de suporte, recuperação em caso de falha, gerenciamento de trilhas de auditoria e registros de sistemas, além de procedimentos de monitoramento? A direção autoriza mudanças nesses procedimentos, considerando-os como documentos formais? A organização busca uniformidade no gerenciamento de sistemas de informação, utilizando os mesmos procedimentos, ferramentas e utilitários quando possível?	Não aplicado

Tabela 5.4: Lista de controles não aplicados.

5.2.3 Lista de controles não se aplica

A seguir estão listados os controles considerados não aplicáveis à startup, ou seja, controles que os respondentes avaliam que não devem ser implementados na empresa ou que estão fora do escopo e perfil da empresa. A lista foi obtida através das respostas ao questionário presente na planilha eletrônica enviada aos colaboradores da *startup*.

ID	Controle	Resultado
8	O trabalho nas áreas seguras é supervisionado?	Não se aplica
13	Mudanças são planejadas e testadas?	Não se aplica
19	Existe uma equipe de detecção, tratamento e resposta a incidentes de segurança cibernética (CSIRT)?	Não se aplica
20	Existe um canal apropriado para notificar os incidentes de segurança da informação de forma rápida?	Não se aplica
30	As mídias que contêm cópias de segurança são armazenadas em uma localidade remota (“offsite”), a uma distância suficiente que garanta sua integridade e disponibilidade contra possíveis danos advindos de um desastre ocorrido no sítio primário?	Não se aplica
54	Existem restrições de autenticação do usuário para acesso simultâneo a serviço(s), sistema(s) e/ou rede(s)?	Não se aplica
56	As credenciais de acesso e logs são armazenadas separadamente dos dados das aplicações e dos sistemas?	Não se aplica
81	A empresa utiliza técnicas ou métodos apropriados para garantir exclusão ou destruição segura de dados pessoais (incluindo originais, cópias e registros arquivados), de modo a impedir sua recuperação?	Não se aplica
87	O compartilhamento e a transferência de dados pessoais com terceiros, operadores ou órgãos públicos são registrados, incluindo quais dados pessoais foram divulgados, a quem, a que horas e com que finalidade?	Não se aplica
90	Os contratos firmados com os operadores de dados pessoais contêm cláusulas que asseguram o tratamento de dados pessoais conforme previsto pela Lei Geral de Proteção de Dados?	Não se aplica
95	O controlador obtém consentimento (LGPD, art 7º, I) do titular de dados para o tratamento de dados pessoais que não se enquadre nas demais hipóteses previstas pelo art. 7º e 11 da LGPD?	Não se aplica
100	A finalidade do tratamento é comunicada ao titular dos dados pessoais, mesmo no caso de execução de políticas públicas e competência legal, antes que as informações sejam coletadas ou usadas?	Não se aplica
101	No contrato, há a obrigação do operador de dados pessoais notificar o Controlador em caso de ocorrência de violação de dados pessoais?	Não se aplica
102	Os terceiros operadores de dados informaram no contrato sobre a utilização de subcontratos para processar dados pessoais?	Não se aplica
103	Os titulares de dados pessoais são notificados de alterações na forma de tratamento de dados?	Não se aplica
104	São fornecidas aos titulares de dados pessoais informações claras e facilmente acessíveis sobre as políticas, procedimentos, práticas do controlador de dados pessoais em relação ao manuseio de dados pessoais (dados coletados, processamento efetuado, finalidade a ser alcançada com o processamento, com quem compartilha e a finalidade, capacidade de consentir compartilhamento específicos), como os dados são protegidos, dados de comunicação com o encarregado, entre outras informações de importância a transparência e publicidade?	Não se aplica
119	Apenas navegadores e clientes de e-mail suportados plenamente têm permissão para executar na empresa, usando apenas a versão mais recente dos navegadores e clientes de e-mail fornecidos pelo fornecedor?	Não se aplica
120	São utilizados os serviços de filtragem de DNS em todos os ativos corporativos para bloquear o acesso a domínios mal-intencionados conhecidos?	Não se aplica
121	Todos os ativos corporativos possuem software anti-malware instalados e mantidos?	Não se aplica
122	A funcionalidade de execução e reprodução automática para mídias removíveis está desabilitada nos ativos corporativos?	Não se aplica
132	É estabelecido com fornecedores de TI terceiros, contratos que incluam dentre outras, cláusulas de segurança da informação que assegurem a adequada proteção de dados pessoais?	Não se aplica
134	Todas as mídias que contenham dados pessoais são formatadas antes do descarte? Quando isso não for possível, como em CDs, DVDs, papel e de mídia portátil, sugere-se que seja realizada a destruição física da mídia.	Não se aplica
135	Os dispositivos móveis de uso privado não são usados para fins de uso institucional? Caso não seja possível implementar medidas de segurança equivalentes às da organização, recomenda-se que dispositivos móveis pessoais não sejam utilizados para fins institucionais.	Não se aplica
136	A empresa atualmente implementa e monitora a funcionalidade de remoção remota de dados pessoais em dispositivos móveis, tanto institucionais quanto pessoais, como parte das medidas de segurança da informação?	Não se aplica
139	São utilizadas técnicas de autenticação multi-fator, como por exemplo, aplicativos autenticadores ou SMS para acesso aos serviços em nuvem relacionados a dados pessoais?	Não se aplica

Tabela 5.5: Lista de controles que não se aplicam à empresa

5.3 Resultado da avaliação de riscos

Nas próximas seções, são discutidos os 14 riscos resultantes da aplicação do método na empresa e a abrangência de implementação dos controles.

Risco 1 - Acesso não autorizado

Para o risco de acesso não autorizado, 56% dos controles de prevenção estão implementados como demonstrado na Figura 5.2. Isso resulta em uma probabilidade de valor "Moderado". Já para os controles do tipo mitigação, 49% dos controles de mitigação estão implementados. O impacto ao sistema é considerado "Alto". O risco residual para acesso não autorizado é "Alto".

Risco	Probabilidade (controles implementados)	Impacto (controles implementados)	Nível de Risco
1) Acesso não autorizado	Moderado 56%	Alto 49%	Alto (150)

Figura 5.2 Resultado Risco 1 - Acesso não autorizado

Risco 2 - Coleção Excessiva

Para o risco de coleção excessiva, 52% dos controles de prevenção estão implementados, o que resulta em uma probabilidade considerada de valor "Moderado"como demonstrado na Figura 5.3. Já para os controles do tipo mitigação, 65% dos controles estão implementados, resultando em um impacto de valor "Moderado". O impacto ao sistema é considerado Moderado (10). O risco residual para coleção excessiva é "Moderado".

Risco	Probabilidade (controles implementados)	Impacto (controles implementados)	Nível de Risco
2) Coleção excessiva	Moderado 52%	Moderado 65%	Moderado (100)

Figura 5.3 Resultado Risco 2 - Coleção Excessiva

Risco 3 - Compartilhamento de dados com terceiros sem consentimento

Para o risco de compartilhar ou distribuir dados pessoais com terceiros sem consentimento do titular dos dados pessoais, o resultado foi de 47% dos controles de prevenção implementados, o que resulta em uma probabilidade considerada alta como demonstrado na Figura 5.4. Já para os controles do tipo mitigação 60% dos controles estão aplicados fazendo o impacto ser considerado "Alto". Como resultado, o risco residual é "Alto".

Risco	Probabilidade (controles implementados)	Impacto (controles implementados)	Nível de Risco
3) Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais	Alto 47%	Moderado 60%	Alto (150)

Figura 5.4 Resultado Risco 3 - Compartilhamento de dados com terceiros sem consentimento

Risco 4 - Falha em considerar os direitos dos titulares

Para o risco da falha em considerar os direitos do titular dos dados pessoais, foram implementados 57% dos controles de prevenção, o que resulta em uma probabilidade considerada alta como demonstrado na Figura 5.5. Já para os controles do tipo mitigação 45% dos controles estão aplicados, resultando no impacto "Alto". O risco residual é "Alto".

Risco	Probabilidade (controles implementados)	Impacto (controles implementados)	Nível de Risco
4) Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso)	Moderado 57%	Alto 45%	Alto (150)

Figura 5.5 Resultado Risco 4 - Falha em considerar os direitos dos titulares

Risco 5 - Falha ou erro de processamento

Para o risco de falha ou erro de processamento, o resultado foi que 47% dos controles de prevenção estão implementados, o que resulta em uma probabilidade considerada alta como demonstrado na Figura 5.6. Já para os controles do tipo mitigação, 46% dos controles estão aplicados fazendo o impacto ser considerado alto. Como resultado, o risco residual é "Alto".

Risco	Probabilidade (controles implementados)	Impacto (controles implementados)	Nível de Risco
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.)	Alto 47%	Alto 46%	Alto (225)

Figura 5.6 Resultado Risco 5 - Falha ou erro de processamento

Risco 6 - Informação insuficiente sobre a finalidade do tratamento

Para o risco de informação insuficiente sobre a finalidade do tratamento, o resultado foi que 38% dos controles de prevenção estão implementados, o que resulta em uma probabilidade considerada alta como demonstrado na Figura 5.7. Já para os controles do tipo mitigação 75% dos controles estão implementados. O impacto ao sistema é considerado "Moderado". Por fim, o risco residual é "Alto".

Risco	Probabilidade (controles implementados)	Impacto (controles implementados)	Nível de Risco
6) Informação insuficiente sobre a finalidade do tratamento	Alto 38%	Moderado 75%	Alto (150)

Figura 5.7 Resultado Risco 6 - Informação insuficiente sobre a finalidade do tratamento

Risco 7 - Modificação não autorizada

Para o risco de modificação não autorizada, o resultado foi que 55% dos controles de prevenção estão sendo aplicados, o que resulta em uma probabilidade de valor "Moderado"como demonstrado na Figura 5.8. Já para os controles do tipo mitigação 41% dos controles estão aplicados. O impacto ao sistema é considerado alto, o que resulta em um risco residual "Alto".

Risco	Probabilidade (controles implementados)	Impacto (controles implementados)	Nível de Risco
7) Modificação não autorizada	Moderado 55%	Alto 41%	Alto (150)

Figura 5.8 Resultado Risco 7 - Modificação não autorizada

Risco 8 - Perda

Para o risco de perda, o resultado foi que 49% dos controles de prevenção estão sendo aplicados, o que resulta em uma probabilidade considerada alta (15) como demonstrado na Figura 5.9. Já para os controles do tipo mitigação 46% dos controles estão aplicados. O impacto ao sistema é considerado alto (15). Ao fim, o risco residual é alto (225).

Risco	Probabilidade (controles implementados)	Impacto (controles implementados)	Nível de Risco
8) Perda	Alto 49%	Alto 46%	Alto (225)

Figura 5.9 Resultado Risco 8 - Perda

Risco 9 - Reidentificação de dados pseudonomizados

Para o risco de reidentificação de dados pseudonomizados , o resultado foi que 41% dos controles de prevenção estão sendo aplicados, o que resulta em uma probabilidade considerada alta (15) como demonstrado na Figura 5.10. Já para os controles do tipo mitigação 59% dos controles estão aplicados fazendo o impacto ser considerado moderado (10). Como resultado, o risco residual é Alto (150).

Risco	Probabilidade (controles implementados)	Impacto (controles implementados)	Nível de Risco
9) Reidentificação de dados pseudonimizados	Alto 41%	Moderado 59%	Alto (150)

Figura 5.10 Resultado Risco 9 - Reidentificação de dados pseudonomizados

Risco 10 - Remoção não autorizada

Para o risco de remoção não autorizada, o resultado foi que 55% dos controles de prevenção estão sendo aplicados, o que resulta em uma probabilidade considerada moderada como de-

monstrado na Figura 5.11. Já para os controles do tipo mitigação 40% dos controles estão implementados, resultando no impacto ser considerado alto. O risco residual é "Alto".

Risco	Probabilidade (controles implementados)	Impacto (controles implementados)	Nível de Risco
10) Remoção não autorizada	Moderado 55%	Alto 40%	Alto (150)

Figura 5.11 Resultado Risco 10 - Remoção não autorizada

Risco 11 - Retenção prolongada de dados pessoais sem necessidade

Para o risco de retenção prolongada de dados pessoais sem necessidade, o resultado foi que 29% dos controles de prevenção estão sendo aplicados, o que resulta em uma probabilidade considerada alta (15) como demonstrado na Figura 5.12. Já para os controles do tipo mitigação 44% dos controles estão aplicados fazendo o impacto ser considerado alto (15). Como resultado, o risco residual é alto (225).

Risco	Probabilidade (controles implementados)	Impacto (controles implementados)	Nível de Risco
11) Retenção prolongada de dados pessoais sem necessidade	Alto 29%	Alto 44%	Alto (225)

Figura 5.12 Resultado Risco 11 - Retenção prolongada de dados pessoais sem necessidade

Risco 12 - Roubo

Para o risco de roubo, o resultado foi que 52% dos controles de prevenção estão sendo aplicados, o que resulta em uma probabilidade considerada moderada como demonstrado na Figura 5.13. Já para os controles do tipo mitigação 45% dos controles estão aplicados fazendo o impacto ser considerado alto. Como resultado, o risco residual é alto.

Risco	Probabilidade (controles implementados)	Impacto (controles implementados)	Nível de Risco
12) Roubo	Moderado 52%	Alto 45%	Alto (150)

Figura 5.13 Resultado Risco 12 - Roubo

Risco 13 - Tratamento sem consentimento do titular

Para o risco de tratamento sem consentimento do titular dos dados pessoais, o resultado foi que 47% dos controles de prevenção estão sendo aplicados, o que resulta em uma probabilidade considerada alta (15) como demonstrado na Figura 5.14. Já para os controles do tipo mitigação 67% dos controles estão aplicados fazendo o impacto ser considerado moderado (10). Como resultado, o risco residual é alto (150).

Risco	Probabilidade (controles implementados)	Impacto (controles implementados)	Nível de Risco
13) Tratamento sem consentimento do titular dos dados pessoais (caso o tratamento não esteja previsto em legislação ou regulação pertinente)	Alto 47%	Moderado 67%	Alto (150)

Figura 5.14 Resultado Risco 13 - Tratamento sem consentimento do titular

Risco 14 - Vinculação ou associação indevida

Para o risco de vinculação ou associação indevida direta ou indireta, dos dados pessoais ao titular, o resultado foi que 46% dos controles de prevenção estão sendo aplicados, o que resulta em uma probabilidade considerada alta como demonstrado na Figura 5.15. Já para os controles do tipo mitigação 41% dos controles estão aplicados fazendo o impacto ser considerado alto. Como resultado, o risco residual é alto.

Risco	Probabilidade (controles implementados)	Impacto (controles implementados)	Nível de Risco
14) Vinculação ou associação indevida direta ou indireta, dos dados pessoais ao titular	Alto 46%	Alto 41%	Alto (225)

Figura 5.15 Resultado Risco 14 - Vinculação ou associação indevida

5.4 Sugestões de implementação de controles

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 presentes na Figura 5.16 devem ser implementados e resulta em um risco residual considerado "Moderado":

Matriz de Pesos da Análise			
Risco	Probabilidade (controles implementados)	Impacto (controles implementados)	Nível de Risco
1) Acesso não autorizado	Moderado 65,3%	Moderado 56,6%	Moderado (100)
2) Coleção excessiva	Moderado 70%	Moderado 82,4%	Moderado (100)
3) Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais	Moderado 64,3%	Moderado 70%	Moderado (100)
4) Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso)	Moderado 71,4%	Moderado 55%	Moderado (100)
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.)	Moderado 66,7%	Moderado 54,2%	Moderado (100)
6) Informação insuficiente sobre a finalidade do tratamento	Moderado 60%	Moderado 75%	Moderado (100)
7) Modificação não autorizada	Moderado 64,5%	Moderado 51,6%	Moderado (100)
8) Perda	Moderado 60,5%	Moderado 60%	Moderado (100)
9) Reidentificação de dados pseudonimizados	Moderado 62,9%	Moderado 70,6%	Moderado (100)
10) Remoção não autorizada	Moderado 65,7%	Moderado 53,3%	Moderado (100)
11) Retenção prolongada de dados pessoais sem necessidade	Moderado 55,2%	Moderado 66,7%	Moderado (100)
12) Roubo	Moderado 61,3%	Moderado 57%	Moderado (100)
13) Tratamento sem consentimento do titular dos dados pessoais (caso o tratamento não esteja previsto em legislação ou regulação pertinente)	Moderado 66,7%	Moderado 66,7%	Moderado (100)
14) Vinculação ou associação indevida direta ou indireta, dos dados pessoais ao titular	Moderado 67,5%	Moderado 58,8%	Moderado (100)

Figura 5.16 Primeiro Cenário - Risco Residual Moderado

1. **Controle**: 5 - Compliance com privacidade
   Pergunta: A empresa possui Política de Segurança da Informação? Ela já foi revisada para se adequar a medidas que objetivem a proteção de dados pessoais? Deve estar estabelecido a previsão de revisão periódica e 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.
   Origem: ABNT NBR ISO/IEC 27701:2019 (item 6.2)

2. **Controle**: 18 - Gestão de Riscos
   Pergunta: Há um processo de análise e monitoramento de vulnerabilidades?
   Origem: ABNT NBR ISO/IEC 27002:2013 (item 14.2.2)

3. **Controle**: 27 - Cópia de Segurança
   Pergunta: Há uma política ou norma de backup que aborde os procedimentos operacionais que padronizam os processos de geração de cópias de segurança e recuperação de arquivos, assim como os processos de controle de acesso, armazenamento, movimenta-

ção e descarte das mídias que contêm cópias de segurança?
Origem: ABNT NBR ISO/IEC 27002:2013 (item 12.3)

4. **Controle**: 42 - Gestão de Riscos
   Pergunta: Há um processo de análise e monitoramento de vulnerabilidades?
   Origem: ABNT NBR ISO/IEC 27002:2013 (item 14.2.2)

5. **Controle**: 89 - Compliance com a Privacidade
   Pergunta: O desenvolvimento dos sistemas é orientado à proteção da privacidade dos dados pessoais (Privacy by Design)?
   Origem: ISO/IEC 29151:2017 (item 14.2.10)

6. **Controle**: 91 - Compliance com a Privacidade
   Pergunta: Há uma política ou norma de proteção de dados pessoais que aborde a finalidade da empresa perante o processamento de dados; a transparência com relação à coleta e processamento de dados pessoais; a estrutura estabelecida para a proteção de dados pessoais; regras para tomar decisões em questões de proteção de dados pessoais; critérios de aceitação de risco de privacidade; compromisso de satisfazer os requisitos aplicáveis de proteção à privacidade?
   Origem: ISO/IEC 29151:2017 (item 14.2.10)

7. **Controle**: 99 - Limitação da Coleta
   Pergunta: É realizada uma análise periódica sobre os dados coletados, se eles continuam limitados ao mínimo necessário para o atendimento a finalidade?
   Origem: ISO/IEC 29151:2017(item A.5) e ANPD 3.2.2 (p. 44)

O segundo cenário consiste na aplicação do primeiro cenário juntamente com controles adicionais, de modo a que o risco residual seja considerado 'Baixo'. Portanto, os controles da Figura 5.17 devem ser implementados.

Matriz de Pesos da Análise			
Risco	Probabilidade (controles implementados)	Impacto (controles implementados)	Nível de Risco
1) Acesso não autorizado	Baixo 93,1%	Baixo 90,6%	Baixo (25)
2) Coleção excessiva	Baixo 92,5%	Baixo 100%	Baixo (25)
3) Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais	Baixo 89,3%	Baixo 100%	Baixo (25)
4) Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso)	Baixo 97,1%	Baixo 95%	Baixo (25)
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.)	Baixo 87,9%	Baixo 91,7%	Baixo (25)
6) Informação insuficiente sobre a finalidade do tratamento	Baixo 95%	Baixo 100%	Baixo (25)
7) Modificação não autorizada	Baixo 91,6%	Baixo 90,3%	Baixo (25)
8) Perda	Baixo 93%	Baixo 92%	Baixo (25)
9) Reidentificação de dados pseudonimizados	Baixo 88,6%	Baixo 88,2%	Baixo (25)
10) Remoção não autorizada	Baixo 96%	Baixo 93,3%	Baixo (25)
11) Retenção prolongada de dados pessoais sem necessidade	Baixo 89,7%	Baixo 100%	Baixo (25)
12) Roubo	Baixo 90,1%	Baixo 88,4%	Baixo (25)
13) Tratamento sem consentimento do titular dos dados pessoais (caso o tratamento não esteja previsto em legislação ou regulação pertinente)	Baixo 93,9%	Baixo 100%	Baixo (25)
14) Vinculação ou associação indevida direta ou indireta, dos dados pessoais ao titular	Baixo 90%	Baixo 88,2%	Baixo (25)

Figura 5.17 Segundo Cenário - Risco Residual Baixo

1. **Controle**: 1 - Responsabilização
   Pergunta: 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?
   Origem: ABNT NBR ISO/IEC 27002:2013 (item 6.1.1)

2. **Controle**: 4 - Continuidade de Negócio
   Pergunta: 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?
   Origem: ABNT NBR ISO/IEC 27002:2013 (item 17.1)

3. **Controle**: 12 - Gestão de Mudanças
   Pergunta: É realizado o controle de mudanças em atualizações de software e outros

componentes das soluções de TIC, assegurando que estes estejam atualizados?
Origem: ABNT NBR ISO/IEC 27002:2013 (item 14.2.2) e CIS Controls v8 (item 12.1)

4. **Controle**: 33 - Desenvolvimento Seguro
Pergunta: Existe e é executado um processo formal de desenvolvimento de sistema seguro? Trate de itens como: padrões de design de aplicação seguro, práticas de codificação seguras, treinamento de desenvolvedor, gestão de vulnerabilidade, segurança de código de terceiros e procedimentos de teste de segurança de aplicação.
Origem: ABNT NBR ISO/IEC 27002:2013 (item 14.2.1) e CIS Controls v8 (item 16.10)

5. **Controle**: 38 - Gestão de Riscos
Pergunta: Os recursos de segurança da informação e de tecnologia da informação encontram-se em versões seguras, estáveis e atualizadas?
Origem: ABNT NBR ISO/IEC 27002:2013 (item 12.6.1)

6. **Controle**: 4 - Gestão contínua de vulnerabilidades
Pergunta: As atualizações do sistema operacional e de aplicações em ativos corporativos são realizadas por meio da gestão automatizada de patches de forma mensal ou com mais frequência?
Origem: CIS Controls v8 (item 7.3) e (item 7.4)

5.5 Comentários dos Colaboradores

Nesta seção, são apresentados os comentários dos colaboradores que participaram da avaliação do método GARSP-SGD. Suas perspectivas e *insights* oferecem uma visão abrangente sobre a eficácia do método e os potenciais benefícios que ele pode proporcionar.

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 testes de segurança executados por terceiros como uma maneira de melhorar o método de 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 Lei Geral de Proteção de Dados (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: Quanto aos potenciais benefícios que o método de avaliação de riscos pode oferecer à 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 Lei Geral de Proteção de Dados e sua capacidade de difundir conceitos de segurança em startups.

> Visto que o método aplicado tem base na Lei Geral de Proteção de Dados, 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: Ele identificou benefícios, incluindo 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 de avaliação de riscos são: 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 noticias, por exemplo, que evidenciam os impactos que falhas na segurança causam na vida das pessoas.

Esses comentários refletem as percepções dos colaboradores sobre o método de avaliação de riscos e fornecem *insights* valiosos sobre sua eficácia e possíveis melhorias.

CAPÍTULO 6

Conclusão

6.1 Contribuições

Nesse trabalho, foi aplicado o de avaliação de riscos do Guia de Avaliação de Riscos de Segurança da Informação e Privacidade (GARSP-SGD) em uma aplicação de governança de dados de uma *startup*. Após um questionário com colaboradores, foi possível avaliar o risco do sistema. Dos 14 riscos de segurança da informação e privacidade elencados pelo método, 13 estão com o risco em nível Alto. 1 está com o risco em nível moderado. Considerando a realidade de uma *startup* de pequeno porte, a análise de risco reflete as dificuldades enfrentadas por esse tipo de organização na implementação de controles de segurança da informação e privacidade. Isso se deve principalmente à falta de recursos financeiros e de pessoal especializado. Após a análise, foram sugeridos controles que pudessem diminuir o nível de risco na *startup*, ao todo foram 7 controles selecionados para o nível moderado e mais 6 controles para o nível baixo. Com a implementação desses 13 controles é possível alcançar um nível de risco mais baixo para a aplicação.

O trabalho oferece uma série de contribuições significativas. Em primeiro lugar, promove a adoção de métodos desenvolvidos por órgãos do Governo Federal alinhados com a Lei Geral de Proteção de Dados no setor privado. Além disso, oferece orientações valiosas para aprimorar a segurança da informação e a privacidade em *startups*, identificando riscos específicos a que essas empresas estão expostas. Também destaca os desafios enfrentados por *startups* ao implementar controles de segurança, dadas as restrições financeiras e de recursos humanos. Além disso, aumenta a conscientização tanto dos gestores quanto dos funcionários, destacando oportunidades de aprimoramento na segurança da informação e no tratamento de dados pessoais. Adicionalmente, este trabalho estimula discussões sobre questões cruciais relacionadas à segurança da informação e à privacidade nessas organizações. Por fim, 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.

6.2 Limitações

É importante destacar que, uma vez que o sistema avaliado não foi originalmente desenvolvido com base em controles de segurança da informação e privacidade, a ausência desses controles e o resultado de alto risco são compreensíveis. Isto ocorre, pois os controles são eram requisitos do projeto e os controles abordados pelo método de avaliação de riscos 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 as seguintes limitações. 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 dos controles, avaliando em cada etapa o nível de risco num processo contínuo e interativo. Essas questões são cruciais para uma avaliação de riscos completa e eficaz em uma empresa, especialmente com o objetivo de envolver a alta administração no processo, o que é um fator-chave para o sucesso.

6.3 Trabalhos futuros

Como trabalhos futuros pode-se avaliar os controles mais ideais para startups em um 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, essa aplicação forneceria uma interface gráfica com as seguintes funcionalidades: gestão de controles (inserir, editar e modificar controles), modificar pesos, aplicar os cálculos de risco de forma automatizada e guardar histórico das análises de riscos, exportar análises em diferentes formatos (CSV, Excel e PDF). Painéis de dados podem ser criados para apoiar os gestores na tomada de decisão e acompanhar a implementação dos controles.

APÊNDICE A

Lista de Controles do Guia de avaliação de Riscos SGD

Tabela A.1: Lista final de controles utilizados na avaliação de risco.

ID	Origem	Código	Controle	Grupo	Referência Original	Controle Startups
1	Guia SGD	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) e ABNT NBR ISO/IEC 27002:2013 (item 6.1.1)	SIM
2	Guia SGD	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) e ABNT NBR ISO/IEC 27002:2013 (item 12.1.3) e NBR ISO/IEC 27002:2005 (A.10.3.1)	SIM
3	Guia SGD	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) e ABNT NBR ISO/IEC 27002:2013 (13.1.2) e CIS Controls v8 (item 4.4) e ANPD 3.2.3 (p. 54)	SIM
4	Guia SGD	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 e ABNT NBR ISO/IEC 27002:2013 (item 17.1) e NBR ISO/IEC 27002:2005 (A.14.1.1)	SIM
5	Guia SGD	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) e ANPD 3.1.1 (p. 24)	SIM
6	Guia SGD	6	Os dados pessoais encontram-se classificados em sensíveis e não sensíveis, incluindo categorias de informações pessoais de saúde, informações pessoais financeiras, entre outras?	Legitimidade e especificação de propósito	ABNT NBR ISO/IEC 27701:2019 (item 6.5.2)	NAO
7	Guia SGD	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) e ABNT NBR ISO/IEC 27002:2013 (item 11.1) e NBR ISO/IEC 27002:2005 (A.9.1.1) e NBR ISO/IEC 27002:2005 (A.9.1.2)	SIM
8	Guia SGD	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) e ABNT NBR ISO/IEC 27002:2013 (item 11.1.2) e NBR ISO/IEC 27002:2005 (A.9.1.1) e NBR ISO/IEC 27002:2005 (A.9.1.2)	SIM
9	Guia SGD	9	A rede corporativa é segmentada em domínios lógicos (limitando aos funcionários o acesso às redes e aos serviços de rede especificamente autorizados a usar), de acordo com cada rede local, atendendo às necessidades de fornecimento de serviço público e proteção da rede corporativa?	Controles de Segurança em Redes, Proteção Física e do Ambiente	Requisitos mínimos de segurança da informação aos órgãos da Administração Pública federal (GSI/PR, 2.2 Orientações Técnicas, 2017) e ABNT NBR ISO/IEC 27002:2013 (item 13.1.3)	NAO
10	Guia SGD	10	O acesso externo aos sistemas é provido de meios de segurança que protegem a confidencialidade e integridade dos dados trafegados, tais como o uso de VPN?	Controles de Segurança em Redes, Proteção Física e do Ambiente	Requisitos mínimos de segurança da informação aos órgãos da Administração Pública federal (GSI/PR, 2.2 Orientações Técnicas, 2017) e ABNT ISO/IEC 27002:2013 (item 13.1.1)	SIM

Tabela A.1: Lista final de controles utilizados na avaliação de risco.

ID	Origem	Código	Controle	Grupo	Referência Original	Controle Startups
11	Guia SGD	11	Existem e são executados processos periódicos de cópias de segurança das configurações e sistemas operacionais dos switches e roteadores?	Controles de Segurança em Redes, Proteção Física e do Ambiente	ABNT ISO/IEC 27002:2013 (item 14.2.4)	NAO
12	Guia SGD	12	É realizado o controle de mudanças em atualizações de software e outros componentes das soluções de TIC, assegurando que estes estejam atualizados?	Gestão de Mudanças	NC nº 13/IN01/DSIC/GSIPR (item 6) e ABNT NBR ISO/IEC 27002:2013 (item 14.2.2) e CIS Controls v8 (item 12.1)	SIM
13	Guia SGD	13	Mudanças são planejadas e testadas?	Gestão de Mudanças	NC nº 13/IN01/DSIC/GSIPR (item 6.3) e ABNT NBR ISO/IEC 27002:2013 (item 14.2.2) e NBR ISO/IEC 27002:2005 (A.10.2)	SIM
14	Guia SGD	14	Há uma avaliação de impactos potenciais, riscos e consequências, incluindo impactos de segurança cibernética, quando da identificação de necessidade de mudanças?	Gestão de Mudanças	NC nº 04/IN01/DSIC/GSIPR (6.2) e ABNT NBR ISO/IEC 27002:2013 (item 14.2.2) e NBR ISO/IEC 27002:2005 (A.10.2)	SIM
15	Guia SGD	15	As mudanças são comunicadas para todas as partes interessadas?	Gestão de Mudanças	NC nº 13/IN01/DSIC/GSIPR (item 6.3) e ABNT NBR ISO/IEC 27002:2013 (item 14.2.2) e NBR ISO/IEC 27002:2005 (A.10.2)	SIM
16	Guia SGD	16	Existe um prazo formalmente definido para o tratamento de vulnerabilidades técnicas relevantes identificadas?	Gestão de Mudanças	NC nº 04/IN01/DSIC/GSIPR (item 6.3.2) e ABNT NBR ISO/IEC 27002:2013 (item 12.6.1)	SIM
17	Guia SGD	17	Há inventários completos e atualizados dos ativos corporativos, hardware, software e provedores de serviço, com as informações necessárias para identificar os diferentes itens com suas respectivas características?	Gestão de Riscos	NC nº 10/IN01/DSIC/GSIPR e ABNT NBR ISO/IEC 27002:2013 (item 12.6.1) e ABNT NBR ISO/IEC 27701:2019 (item 7.2.8) e ISO/IEC 29151 (item 8.1.2) e CIS Controls v8 (item 15.1) e NBR ISO/IEC 27002:2005 (A.7.1.1) e NBR ISO/IEC 27002:2005 (A.7.1.2) e NBR ISO/IEC 27002:2005 (A.7.1.3)	SIM
18	Guia SGD	18	Há um processo de análise e monitoramento de vulnerabilidades?	Gestão de Riscos	NC nº 13/IN01/DSIC/GSIPR (item 6.3) e ABNT NBR ISO/IEC 27002:2013 (item 14.2.2) e Guia Boas Práticas ANPD (item 3.2.4), OWASP Proactive Controls (C2)	SIM
19	Guia SGD	19	Existe uma equipe de detecção, tratamento e resposta a incidentes de segurança cibernética (CSIRT)?	Resposta a Incidente	NC nº 05/IN01/DSIC/GSIPR, ABNT NBR ISO/IEC 27002:2013 (item 16.1) e ABNT NBR ISO/IEC 27701:2019 (item 6.13) e CIS Controls v8 (item 17.1) e ANPD 3.1.2 (p. 29)	SIM
20	Guia SGD	20	Existe um canal apropriado para notificar os incidentes de segurança da informação de forma rápida?	Resposta a Incidente	NC nº 05/IN01/DSIC/GSIPR, ABNT NBR ISO/IEC 27002:2013 (item 16.1) e ABNT NBR ISO/IEC 27701:2019 (item 6.13) e CIS Controls v8 (item 17.2) e ANPD 3.1.2 (p. 29)	SIM
21	Guia SGD	21	Existem formalmente e são executados procedimentos específicos para resposta aos incidentes, contemplando: a definição de incidente; o escopo da resposta; quando e por quem as autoridades devem ser contatadas; papéis, responsabilidades e autoridades; avaliação de impacto do incidente; medidas para reduzir a probabilidade e mitigar o impacto do incidente; descrição da natureza dos dados pessoais afetados; as informações sobre os titulares de dados pessoais envolvidos; procedimentos para determinar se um aviso para indivíduos afetados e outras entidades designadas (por exemplo, órgãos reguladores) é necessário?	Resposta a Incidente	NC nº 08/IN01/DSIC/GSIPR (item 7), ABNT NBR ISO/IEC 27002:2013 (item 16.1) e ABNT NBR ISO/IEC 27701:2019 (item 6.13) e CIS Controls v8 (item 17.3) e ANPD 3.1.2 (p. 29)	SIM
22	Guia SGD	22	Os ativos de informação estão configurados de forma a registrar todos os eventos relevantes de segurança da informação, contendo, pelo menos, a identificação inequívoca do usuário, a natureza do evento, a data, hora e fuso horário, o identificador do ativo de informação, as coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento?	Resposta a Incidente	NC nº 21/IN01/DSIC/GSIPR (item 6), ABNT NBR ISO/IEC 27002:2013 (item 12.4.1) e ABNT NBR ISO/IEC 27701:2019 (item 6.9.4)	SIM
23	Guia SGD	23	Há um sistema para monitoramento de aplicações, alertas e vulnerabilidades utilizado para auxiliar na detecção e tratamento de incidentes de segurança cibernética (IPS, IDS, etc.)?	Resposta a Incidente	NC nº 08/IN01/DSIC/GSIPR (item 7), NC nº 21/IN01/DSIC/GSIPR (item 6) e ABNT NBR ISO/IEC 27002:2013 (item 16.1)	SIM
24	Guia SGD	24	O plano de comunicação foi atualizado para incluir os contatos que devem ser notificados, caso haja uma violação de privacidade, ou para reportar detalhes de processamento, como contatos com a autoridade de proteção de dados e/ou grupos diretamente relacionados?	Resposta a Incidente	ABNT NBR ISO/IEC 27002:2013 (item 16.1) e ABNT NBR ISO/IEC 27701:2019 (item 6.13.1.5)	SIM

Tabela A.1: Lista final de controles utilizados na avaliação de risco.

ID	Origem	Código	Controle	Grupo	Referência Original	Controle Startups
25	Guia SGD	25	Nos casos em que seja inviável preservar as mídias de armazenamento em razão da necessidade de pronto restabelecimento do serviço afetado, o agente responsável pelo CSIRT coleta e armazena cópia dos arquivos afetados pelo incidente, tais como: logs, configurações do sistema operacional, arquivos do sistema de informação, e outros julgados necessários, mantendo-se a estrutura de diretórios original, bem como os "metadados" desses arquivos, como data, hora de criação e permissões; registrando em relatório a impossibilidade de preservar as mídias afetadas e listando todos os procedimentos adotados?	Resposta a Incidente	NC nº 21/IN01/DSIC/GSIPR (item 7) e ABNT NBR ISO/IEC 27002:2013 (item 16.1)	NAO
26	Guia SGD	26	Os arquivos coletados como evidências são gravados em conjunto com o arquivo com a lista dos resumos criptográficos?	Resposta a Incidente	NC nº 21/IN01/DSIC/GSIPR (item 7) e ABNT NBR ISO/IEC 27002:2013 (item 16.1)	NAO
27	Guia SGD	27	Há uma política ou norma de backup que aborde os procedimentos operacionais que padronizam os processos de geração de cópias de segurança e recuperação de arquivos, assim como os processos de controle de acesso, armazenamento, movimentação e descarte das mídias que contêm cópias de segurança?	Cópia de Segurança	ABNT NBR ISO/IEC 27002:2013 (item 12.3) e ABNT NBR ISO/IEC 27701:2019 (item 6.9.3) e ANPD 3.2.2 (p. 49)	SIM
28	Guia SGD	28	Está estabelecida a abrangência dos procedimentos de backup para cada tipo de informação (por exemplo, completa ou diferencial)?	Cópia de Segurança	ABNT NBR ISO/IEC 27002:2013 (item 12.3) e ABNT NBR ISO/IEC 27701:2019 (item 6.9.3) e ANPD 3.2.2 (p. 49)	SIM
29	Guia SGD	29	É definido a abrangência dos testes de backup e sua periodicidade, de forma que os testes sejam planejados observando as dependências e relacionamentos entre sistemas, considerando inclusive os ambientes de continuidade de negócios, com o objetivo de minimizar a possibilidade de que a ausência de sincronismo entre os dados inviabilize ou dificulte sua recuperação?	Cópia de Segurança	ABNT NBR ISO/IEC 27002:2013 (item 12.3) e ABNT NBR ISO/IEC 27701:2019 (item 6.9.3) e ANPD 3.2.2 (p. 49) e CIS Controls v8 (item 11.1)	SIM
30	Guia SGD	30	As mídias que contêm cópias de segurança são armazenadas em uma localidade remota ("off-site"), a uma distância suficiente que garanta sua integridade e disponibilidade contra possíveis danos advindos de um desastre ocorrido no sítio primário?	Cópia de Segurança	ABNT NBR ISO/IEC 27002:2013 (item 12.3) e ABNT NBR ISO/IEC 27701:2019 (item 6.9.3) e ANPD 3.2.2 (p. 49) e CIS Controls v8 (item 11.4)	SIM
31	Guia SGD	31	O período de retenção das cópias de segurança e os requisitos de releitura são predefinidos, levando-se em consideração os requisitos de negócio, contratuais, regulamentares ou legais?	Cópia de Segurança	ABNT NBR ISO/IEC 27002:2013 (item 12.3) e ABNT NBR ISO/IEC 27701:2019 (item 6.9.3) e ANPD 3.2.2 (p. 49)	SIM
32	Guia SGD	32	É exigida autorização de prévia de autoridade competente para liberação de credenciais em sistemas, bancos de dados e serviços de segurança (VPN) que suportam o serviço, seja para atividade fim ou para atividade de desenvolvimento?	Controles de Acesso Lógico	NC nº 07/IN01/DSIC/GSIPR e ABNT NBR ISO/IEC 27002:2013 (item 9.1.1) e CIS Controls v8 (item 3.3) e CIS Controls v8 (item 6.1) e CIS Controls v8 (item 6.2)	SIM
33	Guia SGD	33	Existe e é executado um processo formal de desenvolvimento de sistema seguro? Trate de itens como: padrões de design de aplicação seguro, práticas de codificação seguras, treinamento de desenvolvedor, gestão de vulnerabilidade, segurança de código de terceiros e procedimentos de teste de segurança de aplicação.	Desenvolvimento Seguro	NC nº 16/IN01/DSIC/GSIPR e ABNT NBR ISO/IEC 27002:2013 (item 14.2.1) e CIS Controls v8 (item 16.10)	SIM
34	Guia SGD	34	As áreas de desenvolvimento, teste, homologação e produção são segregadas a fim de reduzir as possibilidades de modificação ou uso indevido dos recursos de processamento da informação, com controles de segurança adequados para cada ambiente?	Desenvolvimento Seguro	NC nº 16/IN01/DSIC/GSIPR e ABNT NBR ISO/IEC 27002:2013 (itens 12.1.4 e 14.2.1)	NAO
35	Guia SGD	35	Em caso de desenvolvimento de sistemas de informação por terceiros, o proprietário do ativo da informação supervisiona o processo do planejamento até a implantação?	Desenvolvimento Seguro	ABNT NBR ISO/IEC 27002:2013 (item 14.2.7)	NAO
36	Guia SGD	36	Quando há a cópia dos dados de produção para os ambientes de desenvolvimento, teste e homologação, há autorização do proprietário do ativo de informação?	Desenvolvimento Seguro	NC nº 07/IN01/DSIC/GSIPR e ABNT NBR ISO/IEC 27002:2013 (item 14.2.6)	NAO
37	Guia SGD	37	É realizada periodicamente uma análise/avaliação de riscos da arquitetura da Solução de TIC, indicando os eventos de risco e seus respectivos níveis de risco ao qual o sistema está exposto, baseada em prévia análise de vulnerabilidades dos ativos que compõem a Solução de TIC?	Gestão de Riscos	NC nº 04/IN01/DSIC/GSIPR e ABNT NBR ISO/IEC 27005:2019	SIM
38	Guia SGD	38	Os recursos de segurança da informação e de tecnologia da informação encontram-se em versões seguras, estáveis e atualizadas?	Gestão de Riscos	ABNT NBR ISO/IEC 27002:2013 (item 12.6.1)	SIM

Tabela A.1: Lista final de controles utilizados na avaliação de risco.

ID	Origem	Código	Controle	Grupo	Referência Original	Controle Startups
39	Guia SGD	39	O responsável pelo sistema acompanha junto aos fabricantes o período de obsolescência do produto, para evitar que os componentes tornem-se expostos a vulnerabilidades sem correção?	Gestão de Riscos	ABNT NBR ISO/IEC 27002:2013 (item 14.2)	NAO
40	Guia SGD	40	Há redundância dos recursos de processamento da informação suficiente para atender aos requisitos de disponibilidade previstos em contrato?	Gestão de Capacidade e Redundância	ABNT NBR ISO/IEC 27002:2013 (item 12.1.3) e NBR ISO/IEC 27002:2005 (A.10.3.1)	SIM
41	Guia SGD	41	Foi elaborada uma política de privacidade para o serviço?	Compliance com privacidade	ABNT NBR ISO/IEC 27701:2019 (item 6.2.1.1) e ISO/IEC 29151:2017 (A2)	SIM
42	Guia SGD	42	Existe Relatório de Impacto à Proteção de Dados Pessoais, conforme previsto na Lei 13.709 de 14 de agosto de 2018, relacionado à solução de TIC?	Compliance com Privacidade	Lei nº 13.709/2018, art. 10, Parágrafo 3º, Guia de Boas Práticas LGPD, seção 2.5 (CCGD, 2020) e ISO/IEC 29134:2017	NAO
43	Guia SGD	43	Há um inventário completo e atualizado dos dados pessoais, contendo os agentes de tratamento (controlador e operador), encarregado, descrição do fluxo de tratamento dos dados pessoais (como são coletados, armazenados, processados, retidos e eliminados), abrangência da área geográfica do tratamento (nacional, estadual, municipal), finalidade do tratamento dos dados pessoais, categoria dos dados pessoais (identificação pessoal, financeiros, características pessoais, outros), categoria de dados sensíveis, dados pessoais compartilhados e transferência internacional?	Legitimidade e especificação de propósito	ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)	SIM
44	Guia SGD	44	São realizados, em intervalos de tempo predefinidos, simulações e/ou testes planejados, levando-se em consideração as menores indisponibilidades e impactos possíveis nos processos de negócio, de forma que seja possível identificar falhas que venham a comprometer qualquer parte do processo de continuidade, com vistas a promover revisões e atualizações periódicas dos Planos relacionados?	Controles de Continuidade de Negócio	NC nº 06/IN01/DSIC/GSIPR e ABNT NBR ISO/IEC 22301:2013	NAO
45	Guia SGD	45	Há utilização de criptografia para a proteção dos dados sensíveis ou críticos armazenados em dispositivos móveis, mídias removíveis ou em banco de dados?	Controles Criptográficos	ABNT NBR ISO/IEC 27002:2013 (item 10.1.1) e ABNT NBR ISO/IEC 27701:2019 (item 6.5.3 e item 6.7) e Guia Boas Práticas ANPD (item 3.2.2) e OWASP Proactive Controls (C8)	SIM
46	Guia SGD	46	Existe uma frequência estabelecida para geração dos backups?	Cópia de Segurança	ABNT NBR ISO/IEC 27002:2013 (item 12.3) e ABNT NBR ISO/IEC 27701:2019 (item 6.9.3) e ANPD 3.2.2 (p. 49)	SIM
47	Guia SGD	47	São realizadas cópias de segurança dos logs de acordo com períodos de retenção, que consideram os requisitos de negócio, contratuais, regulamentares ou legais?	Cópia de Segurança	NC nº 21/IN01/DSIC/GSIPR e ABNT NBR ISO/IEC 27002:2013 (item 12.4.2)	SIM
48	Guia SGD	48	O sistema em análise segue uma política de senha com definição de tamanho mínimo e formato?	Controles de Acesso Lógico	NC nº 07/IN01/DSIC/GSIPR, Requisitos mínimos de segurança da informação aos órgãos da Administração Pública federal (GSI/PR, 2.2 Orientações Técnicas, 2017), ABNT NBR ISO/IEC 27002:2013 (item 9) e ANPD 3.1.3 (p. 36)	SIM
49	Guia SGD	49	As informações das credenciais de acesso dos usuários estão gravadas em recursos de tecnologia da informação protegidos e sob a forma criptografada?	Controles de Acesso Lógico	NC nº 07/IN01/DSIC/GSIPR e ABNT NBR ISO/IEC 27002:2013 (item 9) e Guia Boas Práticas ANPD (item 3.2.3) e OWASP Proactive Controls (C8)	SIM
50	Guia SGD	50	As informações das credenciais de acesso dos usuários são transmitidas de forma protegida?	Controles de Acesso Lógico	NC nº 07/IN01/DSIC/GSIPR e ABNT NBR ISO/IEC 27002:2013 (item 9) e ANPD 3.2.3 (p. 53)	SIM
51	Guia SGD	51	Um mecanismo de recuperação de senha está implementado de forma a assegurar a recuperação da senha de maneira segura, sem fornecimento de senha por parte da aplicação, e que obrigue a alteração de senha do usuário no primeiro acesso?	Controles de Acesso Lógico	ABNT NBR ISO/IEC 27002:2013 (item 9.2.4) e OWASP - Web Security Testing Guide v4.1 (item Testing for Weak Password Change or Reset Functionalities) e OWASP Proactive Controls (C6)	SIM
52	Guia SGD	52	Uma análise crítica de direitos de acesso é realizada em um período de tempo previamente definido ou a qualquer momento depois de qualquer mudança nos direitos de usuários ou para verificação de incidentes de segurança? Essas mudanças são registradas em um inventário de contas para controle?	Controles de Acesso Lógico	ABNT NBR ISO/IEC 27002:2013 (item 9.2.5) e OWASP Proactive Controls (C7) e CIS Controls v8 (item 6.1) e CIS Controls v8 (item 6.2) e NBR ISO/IEC 27002:2005 (A.11.2.4)	SIM
53	Guia SGD	53	Há mecanismos para encerramento (expirar) de qualquer sessão cuja inatividade do usuário exceda um período de tempo predeterminado?	Controles de Acesso Lógico	16/IN01/DSIC/GSIPR (item 4.2) e ABNT NBR ISO/IEC 27002:2013 (itens 9.2.5 e 9.4.2)	SIM
54	Guia SGD	54	Existem restrições de autenticação do usuário para acesso simultâneo a serviço(s), sistema(s) e/ou rede(s)?	Controles de Acesso Lógico	OWASP - Session Management Cheat Sheet	SIM

Tabela A.1: Lista final de controles utilizados na avaliação de risco.

ID	Origem	Código	Controle	Grupo	Referência Original	Controle Startups
55	Guia SGD	55	O sistema implementa restrições/limitadores para sucessivas tentativas de acesso mal-sucedidas?	Controles de Acesso Lógico	ABNT NBR ISO/IEC 27002:2013 (item 9.4.2)	NAO
56	Guia SGD	56	As credenciais de acesso e logs são armazenadas separadamente dos dados das aplicações e dos sistemas?	Controles de Acesso Lógico	ABNT NBR ISO/IEC 27002:2013 (item 9.4.3) e CIS Controls v8 (item 8.1)	SIM
57	Guia SGD	57	O log registra identificação do usuário, incluindo administrador e acessos privilegiados?	Registro de Eventos e Rastreabilidade	Referências: NC nº 21/IN01/DSIC/GS IPR (6.3) e ABNT NBR ISO/IEC 27002:2013 (item 12.4.1) e OWASP Proactive Controls (C9) e CIS Controls v8 (item 8.1)	SIM
58	Guia SGD	58	O log registra endereço IP ou outro atributo que permita a identificação de onde o usuário efetuou o acesso?	Registro de Eventos e Rastreabilidade	Referências: NC nº 21/IN01/DSIC/GSIPR (6.3) e ABNT NBR ISO/IEC 27002:2013 (item 12.4.1) e OWASP Proactive Controls (C9) e CIS Controls v8 (item 8.1) e CIS Controls v8 (item 8.1)	SIM
59	Guia SGD	59	O log registra as ações executadas pelos usuários?	Registro de Eventos e Rastreabilidade	Referências: NC nº 21/IN01/DSIC/GSIPR (6.5) e ABNT NBR ISO/IEC 27002:2013 (item 12.4.1) e OWASP Proactive Controls (C9) e CIS Controls v8 (item 8.1)	SIM
60	Guia SGD	60	O log registra data e hora do evento com alguma fonte de tempo sincronizada?	Registro de Eventos e Rastreabilidade	Referências: NC nº 21/IN01/DSIC/GSIPR (6.3) e ABNT NBR ISO/IEC 27002:2013 (item 12.4.1) e OWASP Proactive Controls (C9) e CIS Controls v8 (item 8.1)	SIM
61	Guia SGD	61	Os logs gerados são protegidos, quando da geração, contra edição e exclusão?	Registro de Eventos e Rastreabilidade	Referências: NC nº 21/IN01/DSIC/GSIPR (7.5) e ABNT NBR ISO/IEC 27002:2013 (item 12.4.2) e OWASP Proactive Controls (C9), CIS Controls v8 (item 8.1)	SIM
62	Guia SGD	62	Os logs são protegidos contra o acesso indevido?	Registro de Eventos e Rastreabilidade	Referências: NC nº 21/IN01/DSIC/GSIPR (7.5) e ABNT NBR ISO/IEC 27002:2013 (item 12.4.2) e OWASP Proactive Controls (C9) e CIS Controls v8 (item 8.1)	SIM
63	Guia SGD	63	Requisitos de segurança são identificados e considerados em todas as fases do projeto do sistema?	Desenvolvimento Seguro	Referências: NC nº 16/IN01/DSIC/GSIPR e ABNT NBR ISO/IEC 27002:2013 (item 14.2.1) e OWASP Proactive Controls (C1)	SIM
64	Guia SGD	64	Existem controles de versão para garantir a gestão dos códigos-fonte?	Desenvolvimento Seguro	Referências: NC nº 16/IN01/DSIC/GSIP R e ABNT NBR ISO/IEC 27002:2013 (item 14.2.1)	NAO
65	Guia SGD	65	As mensagens de erro do sistema não revelam detalhes da sua estrutura interna?	Desenvolvimento Seguro	Referências: NC nº 16/IN01/DSIC/GSIPR (item 5) e ABNT NBR ISO/IEC 27002:2013 (item 14.1.3) e OWASP Proactive Controls (C10)	SIM
66	Guia SGD	66	É realizada análise estática e/ou análise dinâmica dos requisitos de segurança cibernética do sistema?	Desenvolvimento Seguro	Referências: NC nº 16/IN01/DSIC/GS IPR (item 5) e ABNT NBR ISO/IEC 27002:2013 (itens 14.2.8 e 14.2.9)	NAO
67	Guia SGD	67	O servidor da aplicação fornece opções de protocolos criptográficos para conexão em versões seguras, estáveis e atualizadas? Nas comunicações, utilizar conexões cifradas (com uso de TLS/HTTPS) ou aplicativos com criptografia fim a fim.	Segurança Web	Referência: ABNT NBR ISO/IEC 27002:2013 (item 10.1.2) e ANPD 3.2.3 (p. 53)	SIM
68	Guia SGD	68	O servidor da aplicação tem configurado o cabeçalho HTTP com X-XSS-Protection para evitar que usuários de navegadores antigos sejam vulneráveis a ataques de Cross-site Scripting (XSS)?	Segurança Web	Referência: OWASP - Cross Site Scripting Prevention Cheat Sheet (item X-XSS-Protection Header)	NAO
69	Guia SGD	69	O servidor da aplicação tem configurado o cabeçalho HTTP com X-Frame-Options para evitar que usuários caiam em ataques de clickjacking?	Segurança Web	Referência: OWASP - Web Security Testing Guide v4.1 (item Server side protection: X- Frame-Options)	NAO
70	Guia SGD	70	O servidor da aplicação tem configurado o cabeçalho HTTP com HTTP Strict-Transport- Security (HSTS) para garantir que todo o tráfego de dados ocorra criptografado?	Segurança Web	Referência: OWASP - Web Security Testing Guide v4.1 (item Test HTTP Strict Transport Security) e Guia Boas Práticas ANPD (item 3.2.3) e OWASP Proactive Controls (C8)	NAO

Tabela A.1: Lista final de controles utilizados na avaliação de risco.

ID	Origem	Código	Controle	Grupo	Referência Original	Controle Startups
71	Guia SGD	71	O servidor da aplicação implementa políticas (Content Security Policy (CSP)) que validam a renderização da página e protegem contra ataques de injeção de conteúdo como Cross-Site Scripting (XSS)?	Segurança Web	Referência: OWASP Cheat Sheet Series (item Content Security Policy Cheat Sheet)	NAO
72	Guia SGD	72	O servidor da aplicação implementa o X-Content- Type-Options para evitar que navegadores como Internet Explorer e Chrome interpretem o conteúdo da página e execute o dado como código?	Segurança Web	Referência: OWASP Cheat Sheet Series (item REST Security Cheat Sheet)	NAO
73	Guia SGD	73	Os cookies da aplicação são enviados para o usuário apenas através de conexões criptografadas (flag SECURE)?	Segurança Web	Referência: OWASP - Web Security Testing Guide v4.1 (item Testing for Sensitive Information Sent via Unencrypted Channels)	NAO
74	Guia SGD	74	A aplicação está configurada para que os cookies não possam ser acessíveis via comando JavaScript, evitando assim ataques cross-site scripting (XSS) (flag HTTPOnly)?	Segurança Web	Referência: OWASP - Web Security Testing Guide v4.1 (item Testing for Cookies Attributes)	NAO
75	Guia SGD	75	O servidor da aplicação está configurado com o cabeçalho Subresource Integrity (SRI) para proteger contra invasores que modifiquem o conteúdo de bibliotecas JavaScript hospedadas em redes de entrega de conteúdo (CDNs)?	Segurança Web	Referência: OWASP Cheat Sheet Series (item Third Party JavaScript Management Cheat Sheet)	NAO
76	Guia SGD	76	As permissões de acesso (incluir, consultar, alterar, excluir) dos usuários que executam a operação de processamento de dados pessoais se limitam ao mínimo necessário para realizar o processamento?	Controles de Acesso e Privacidade	Referência: ISO/IEC 29151:2017 (item 9.2.3)	NAO
77	Guia SGD	77	O acesso para realizar as operações de tratamento de dados pessoais é provido ao número mínimo de indivíduos necessários para executar as operações de tratamento?	Controles de Acesso e Privacidade	Referência: ISO/IEC 29151:2017 (item 9.2.3)	SIM
78	Guia SGD	78	Meios de autenticação forte são providos para o processamento dos dados pessoais, em especial os dados sensíveis (dados de saúde e demais dados previstos pelo art.5º, II da LGPD))? Exemplo: autenticação de múltiplos fatores.	Controles de Acesso e Privacidade	Referência: ISO/IEC 29151:2017 (item 9.2.3) e ANPD 3.1.3 (p. 41)	SIM
79	Guia SGD	79	A empresa controla por meio de um processo formal a concessão de direitos de acesso privilegiado para o processamento de dados?	Controles de Acesso e Privacidade	Referência: ISO/IEC 29151:2017 (item 9.2.4)	NAO
80	Guia SGD	80	Os dados pessoais utilizados em ambiente de TDH (teste, desenvolvimento e homologação) passaram por um processo de anonimização?	Uso, retenção e limitação de divulgação	Referência: ISO/IEC 29151:2017 (item 12.1.5)	NAO
81	Guia SGD	81	A empresa utiliza técnicas ou métodos apropriados para garantir exclusão ou destruição segura de dados pessoais (incluindo originais, cópias e registros arquivados), de modo a impedir sua recuperação?	Uso, retenção e limitação de divulgação	Referência: ISO/IEC 29151:2017 (item 8.3.3) e CIS Controls v8 (item 3.5)	SIM
82	Guia SGD	82	Ao fornecer a base de informações para órgãos de pesquisa, os dados pessoais são anonimizados ou pseudoanonimizados?	Uso, retenção e limitação de divulgação	Referência: ISO/IEC 29151:2017 (item A.6)	NAO
83	Guia SGD	83	O compartilhamento ou transferência de dados pessoais é realizado por meio de um canal criptografado e de cifra recomendada?	Controles criptográficos	Referência: ISO/IEC 29151:2017 (item 13.2.2) e ANPD 3.2.3 (p. 53)	SIM
84	Guia SGD	84	No compartilhamento de dados com terceiro operador ou órgãos públicos, são documentadas as informações de limitação do tratamento dos dados pessoais ao mínimo necessário para atendimento do fornecimento do serviço e dispositivo legal?	Responsabilização	Referência: ISO/IEC 29151:2017 (item 13.2.5)	NAO
85	Guia SGD	85	Acordos de confidencialidade, termos de responsabilidade, termos de sigilo são assinados com os órgãos e operadores de dados pessoais? É importante que os termos e acordos informem a respeito dos itens a seguir, mas a eles não se limitem: tipos de tratamento de dados pessoais a serem realizados por quem irá receber os dados; ações requeridas quando do encerramento do compartilhamento, como destruição dos dados, responsabilidade e ações dos signatários para evitar a divulgação não autorizada dos dados pessoais; base legal para o compartilhamento; direito de auditar e monitorar as atividades que envolvem os dados pessoais; processo para notificar ou relatar vazamentos; violações ou divulgações não autorizadas dos dados pessoais; ações a serem tomadas diante da violação do acordo; e outras medidas possíveis.	Responsabilização	Referência: ISO/IEC 29151:2017 (item 13.2.5)	SIM

Tabela A.1: Lista final de controles utilizados na avaliação de risco.

ID	Origem	Código	Controle	Grupo	Referência Original	Controle Startups
86	Guia SGD	86	Os contratos firmados com os operadores contêm cláusulas que contemplam, não se limitando a: uma declaração adequada sobre a escala, natureza e finalidade do processamento contratado; relatar casos de violação de dados, processamento não autorizado ou outro não cumprimento dos termos e condições contratuais; medidas aplicáveis na rescisão do contrato, especialmente no que diz respeito à exclusão segura de dados pessoais; impedimento de tratamento de dados pessoais por subcontratados, exceto por aprovação do controlador?	Responsabilização	Referência: ISO/IEC 29151:2017 (item 15.1.2) e ANPD 3.1.3 (p. 31)	SIM
87	Guia SGD	87	O compartilhamento e a transferência de dados pessoais com terceiros, operadores ou órgãos públicos são registrados, incluindo quais dados pessoais foram divulgados, a quem, a que horas e com que finalidade?	Responsabilização	Referência: ISO/IEC 29151:2017 (item A.7.4)	SIM
88	Guia SGD	88	O desenvolvimento dos sistemas tem como base os riscos e as medidas de segurança identificadas no RIPD (Relatório de Impacto de Proteção à Dados Pessoais)?	Compliance com a Privacidade	Referência: ISO/IEC 29151:2017 (item 14.1.2)	NAO
89	Guia SGD	89	O desenvolvimento dos sistemas é orientado à proteção da privacidade dos dados pessoais (Privacy by Design)?	Compliance com a Privacidade	Referência: ISO/IEC 29151:2017 (item 14.2.10)	NAO
90	Guia SGD	90	Os contratos firmados com os operadores de dados pessoais contêm cláusulas que asseguram o tratamento de dados pessoais conforme previsto pela Lei Geral de Proteção de Dados?	Compliance com a Privacidade	Referência: ISO/IEC 29151:2017 (item 15.1.2) e ANPD 3.1.3 (p. 31)	SIM
91	Guia SGD	91	Há uma política ou norma de proteção de dados pessoais que aborde a finalidade da empresa perante o processamento de dados; a transparência com relação à coleta e processamento de dados pessoais; a estrutura estabelecida para a proteção de dados pessoais; regras para tomar decisões em questões de proteção de dados pessoais; critérios de aceitação de risco de privacidade; compromisso de satisfazer os requisitos aplicáveis de proteção à privacidade?	Compliance com a Privacidade	Referência: ISO/IEC 29151:2017 (item A.2) e ANPD 3.2.2 (p. 44)	SIM
92	Guia SGD	92	Os controles de proteção de dados pessoais são monitorados e auditados periodicamente para garantir que as operações que envolvam dados pessoais estejam em conformidade com as leis, regulamentos e termos contratuais aplicáveis?	Compliance com a Privacidade	Referência: ISO/IEC 29151:2017 (item A.11.4)	NAO
93	Guia SGD	93	É implementada e mantida uma estratégia abrangente de treinamento e conscientização, destinada a garantir que os envolvidos (funcionários, usuários e desenvolvedores) entendam suas responsabilidades e os procedimentos de proteção de dados pessoais?	Compliance com a Privacidade	Referência: ISO/IEC 29151:2017 (item A.11.5) e ANPD 3.1.2 (p. 26) e CIS Controls v8 (item 14.1)	SIM
94	Guia SGD	94	A empresa monitora continuamente as ações de proteção de dados pessoais, a fim de determinar o progresso no cumprimento dos requisitos de conformidade com a proteção de dados pessoais e dos controles de proteção de dados pessoais, comparar o desempenho em toda a organização, identificar vulnerabilidades e lacunas na política e na implementação e identificar modelos de sucesso?	Compliance com a Privacidade	Referência: ISO/IEC 29151:2017 (itens A.11.1 e A.13.1)	NAO
95	Guia SGD	95	O controlador obtém consentimento (LGPD, art 7º, I) do titular de dados para o tratamento de dados pessoais que não se enquadre nas demais hipóteses previstas pelo art. 7º e 11 da LGPD?	Consentimento e Escolha	Referência: ISO/IEC 29151:2017 (item A.3.1)	NAO
96	Guia SGD	96	O tratamento de dados pessoais é realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público? (embasamento legal)	Legitimidade e especificação de propósito	Referência: ISO/IEC 29151:2017 (item A.4.1)	NAO
97	Guia SGD	97	As transferências internacionais de dados pessoais são realizadas de acordo com o disposto pelo art. 33 da Lei 13.709/2018 (LGPD)?	Legitimidade e especificação de propósito	Referência: ISO/IEC 29151:2017 (item A.13.2)	NAO
98	Guia SGD	98	Os dados coletados limitam-se ao mínimo necessário para atendimento da finalidade do tratamento?	Limitação da Coleta	Referência: ISO/IEC 29151:2017 (item A.5) e ANPD 3.2.2 (p. 44)	SIM
99	Guia SGD	99	É realizada uma análise periódica sobre os dados coletados, se eles continuam limitados ao mínimo necessário para o atendimento a finalidade?	Limitação da Coleta	Referência: ISO/IEC 29151:2017(item A.5) e ANPD 3.2.2 (p. 44)	SIM
100	Guia SGD	100	A finalidade do tratamento é comunicada ao titular dos dados pessoais, mesmo no caso de execução de políticas públicas e competência legal, antes que as informações sejam coletadas ou usadas?	Limitação da Coleta	Referência: ISO/IEC 29151:2017 (item A.4.2) e ANPD 3.2.2 (p. 44)	SIM
101	Guia SGD	101	No contrato, há a obrigação do operador de dados pessoais notificar o Controlador em caso de ocorrência de violação de dados pessoais?	Abertura, Transparência e Notificação	Referência: ISO/IEC 29151:2017 (item A.7.3) e ANPD 3.1.3 (p. 31)	SIM

Tabela A.1: Lista final de controles utilizados na avaliação de risco.

ID	Origem	Código	Controle	Grupo	Referência Original	Controle Startups
102	Guia SGD	102	Os terceiros operadores de dados informaram no contrato sobre a utilização de subcontratos para processar dados pessoais?	Abertura, Transparência e Notificação	Referência: ISO/IEC 29151:2017 (item A.7.5) e ANPD 3.1.3 (p. 31)	SIM
103	Guia SGD	103	Os titulares de dados pessoais são notificados de alterações na forma de tratamento de dados?	Abertura, Transparência e Notificação	Referência: ISO/IEC 29151:2017 (item A.9.1)	SIM
104	Guia SGD	104	São fornecidas aos titulares de dados pessoais informações claras e facilmente acessíveis sobre as políticas, procedimentos, práticas do controlador de dados pessoais em relação ao manuseio de dados pessoais (dados coletados, processamento efetuado, finalidade a ser alcançada com o processamento, com quem compartilha e a finalidade, capacidade de consentir compartilhamento específicos), como os dados são protegidos, dados de comunicação com o encarregado, entre outras informações de importância a transparência e publicidade?	Abertura, Transparência e Notificação	Referência: ISO/IEC 29151:2017 (item A.9.2)	SIM
105	Guia SGD	105	No processamento de dados, é utilizado o mínimo necessário de dados pessoais para atingir a finalidade pretendida?	Minimização dos dados	Referência: ISO/IEC 29151:2017 (item A.6)	SIM
106	Guia SGD	106	É avaliada a necessidade de permitir que operadores e administradores de banco de dados usem linguagens de consulta, que habilitam recuperação maciça automatizada de bases de dados que contêm dados pessoais?	Minimização dos dados	Referência: ISO/IEC 29151:2017 (item A.9.4.2)	NAO
107	Guia SGD	107	A empresa revisa periodicamente as medidas de segurança aplicadas nos ativos que realizam o tratamento de dados pessoais (coleta, retenção, processamento, compartilhamento e eliminação)?	Desenvolvimento Seguro	Referência: ISO/IEC 29151:2017 (item A.6)	NAO
108	Guia SGD	108	A empresa implementa processos para que o tratamento dos dados pessoais seja preciso, completo, atualizado, adequado e relevante para a finalidade de uso?	Precisão e Qualidade	Referência: ISO/IEC 29151:2017 (item A.8)	NAO
109	Guia SGD	109	A empresa implementa medidas que garantam e maximizem a precisão dos dados pessoais coletados, antes de qualquer armazenamento ou processamento de dados pessoais?	Precisão e Qualidade	Referência: ISO/IEC 29151:2017 (item A.8)	NAO
110	Guia SGD	110	Os dados pessoais armazenados/retidos possuem controles de integridade permitindo identificar se os dados foram alterados sem permissão?	Cópia de Segurança	Referência: ISO/IEC 29151:2017 (item A.8)	NAO
111	Guia SGD	111	As operações de processamento realizadas com dados pessoais são registradas de modo a identificar a operação realizada, quem realizou, data e hora?	Registro de Eventos e Rastreabilidade	Referência: ISO/IEC 29151:2017 (item A.8)	NAO
112	Guia SGD	112	A empresa permite aos titulares dos dados pessoais, quando permitido pela legislação aplicável, a capacidade de acessar e revisar seus dados pessoais para elevar a integridade e precisão das informações?	Participação Individual e Acesso	Referência: ISO/IEC 29151:2017 (item A.10.1)	NAO
113	Guia SGD	113	Há um canal de comunicação ativo, seguro e autenticado para o recebimento de reclamações e manter um ponto de contato para receber e responder a reclamações, preocupações ou perguntas dos titulares sobre o tratamento de dados pessoais realizados pela empresa?	Participação Individual e Acesso	Referência: ISO/IEC 29151:2017 (item A.10.3)	NAO
114	CIS v8	4.1	Foi estabelecido um processo de configuração segura para ativos corporativos (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos não computacionais/IoT; e servidores), software (sistemas operacionais e aplicações) e dispositivos de rede?	Configuração segura de ativos corporativos e software	CIS Controls v8 (item 4.1)	SIM
115	CIS v8	4.6	Os ativos e softwares corporativos são gerenciados com segurança? Por exemplo: gestão de configuração por meio de version-controlled-infrastructure-as-code e acesso a interfaces administrativas por meio de protocolos de rede seguros, como Secure Shell (SSH) e Hypertext Transfer Protocol Secure (HTTPS)?	Configuração segura de ativos corporativos e software	CIS Controls v8 (item 4.2)	SIM
116	CIS v8	4.7	As contas padrão nos ativos e software corporativos, como root, administrador e outras contas de fornecedores pré-configuradas são gerenciadas com segurança? Exemplos de implementações podem incluir: desativar contas padrão, torná-las inutilizáveis, assim como trocar as senhas.	Configuração segura de ativos corporativos e software	CIS Controls v8 (item 4.7) e ANPD 3.1.3 (p. 37)	SIM
117	CIS v8	5.4	Apenas as contas de administador dedicadas possuem privilégios de administrador nos ativos corporativos? Realize atividades gerais de computação, como navegação na Internet, e-mail e uso do pacote de produtividade, a partir da conta primária não privilegiada do usuário.	Gestão de contas	CIS Controls v8 (item 5.4)	SIM

Tabela A.1: Lista final de controles utilizados na avaliação de risco.

ID	Origem	Código	Controle	Grupo	Referência Original	Controle Startups
118	CIS v8	7.3	As atualizações do sistema operacional e de aplicações em ativos corporativos são realizadas por meio da gestão automatizada de patches de forma mensal ou com mais frequência?	Gestão contínua de vulnerabilidades	CIS Controls v8 (item 7.3) e CIS Controls v8 (item 7.4)	SIM
119	CIS v8	9.1	Apenas navegadores e clientes de e-mail suportados plenamente têm permissão para executar na empresa, usando apenas a versão mais recente dos navegadores e clientes de e-mail fornecidos pelo fornecedor?	Proteções de e-mail e navegador Web	CIS Controls v8 (item 9.1)	SIM
120	CIS v8	9.2	São utilizados os serviços de filtragem de DNS em todos os ativos corporativos para bloquear o acesso a domínios mal-intencionados conhecidos?	Proteções de e-mail e navegador Web	CIS Controls v8 (item 9.2)	SIM
121	CIS v8	10.1	Todos os ativos corporativos possuem software anti-malware instalados e mantidos?	Defesas contra malware	CIS Controls v8 (item 10.1) e CIS Controls v8 (item 10.2)	SIM
122	CIS v8	10.2	A funcionalidade de execução e reprodução automática para mídias removíveis está desabilitada nos ativos corporativos?	Defesas contra malware	CIS Controls v8 (item 10.3)	SIM
123	ANPD	30	O termo de confidencialidade (non-disclosure agreement - NDA) é assinado pelos funcionários da empresa para que estes se comprometam a não divulgar informações confidenciais que envolvam dados pessoais?	Gerenciamento de contratos	ANPD 3.1.3 (p. 30)	SIM
124	ANPD	38	É vedado o compartilhamento de contas ou de senhas entre funcionários, visto que isso é um vetor crítico de vulnerabilidade de segurança da informação?	Controle de acesso	ANPD 3.1.3 (p. 38)	SIM
125	ANPD	39	Os usuários de um sistema possuem o menor nível de acesso necessário para a realização de suas atividades? Funções de alto nível, tais como as de administrador de sistema, devem ser restringidas apenas àqueles funcionários que necessitem exercer esse papel e sejam capazes de assumir essa responsabilidade. Esse é o princípio do menor privilégio (need to know)	Controle de acesso	ANPD 3.1.3 (p. 39)	SIM
126	ANPD	46	São aplicadas técnicas de técnicas de pseudonimização em dados armazenados sensíveis que dificultem a identificação do titular? Um exemplo dessa técnica é a criptografia.	Segurança dos dados pessoais armazenados	ANPD 3.2.2 (p. 46) e ANPD 3.2.3 (p. 55)	SIM
127	ANPD	48	São adotadas medidas para evitar a transferência de dados pessoais de estações de trabalho para dispositivos de armazenamento externo, como pendrives, discos rígidos externos, dentre outros, tendo em vista o risco de se perder a guarda dos dados pessoais transferidos? Caso essa operação seja imprescindível, sugere-se a adoção de controles adicionais a esses dispositivos externos, como inventariá-los, cifrar os dados e armazená-los em locais seguros.	Segurança dos dados pessoais armazenados	ANPD 3.2.2 (p. 47)	SIM
128	OWASP	C2	São utilizadas bibliotecas e frameworks de fontes confiáveis que são ativamente mantidades e utilizadas por muitas aplicações? Crie e mantenha um catálogo com todas as bibliotecas de terceiros e proativamente mantenha atualizado.	Desenvolvimento Seguro	OWASP Proactive Controls (C2)	SIM
129	OWASP	C3	As bases de dados possuem mecanismos ativo de proteção como permitir consultar seguras via parametrização de consultas, configuração segura ativa em todos os bancos de dados, autenticação seja feita por canais seguros de comunicação (criptografados)?	Proteção de dados	OWASP Proactive Controls (C3)	SIM
130	OWASP	C4	Técnicas de codificação (Encoding) e escape dos dados são utilizadas para evitar ataques do injeção?	Segurança Web	OWASP Proactive Controls (C4)	SIM
131	OWASP	C5	A aplicação checa se os dados recebidos estão sintaticamente e semanticamente corretos antes de serem utilizados de qualquer forma? Ex. uso de expresões regulares no input dos dados.	Segurança Web	OWASP Proactive Controls (C5)	SIM
132	ANPD	3.1.3 (p. 32) e 3.2.2 (p. 51)	É estabelecido com fornecedores de TI terceiros, contratos que incluam dentre outras, cláusulas de segurança da informação que assegurem a adequada proteção de dados pessoais?	Gerenciamento de contratos	ANPD 3.1.3 (p. 32) e ANPD 3.2.2 (p. 51)	SIM
133	ANPD	3.1.3 (p. 35)	É implementado um sistema de controle de acesso aplicável a todos os usuários, com níveis de permissão na proporção da necessidade de trabalhar com o sistema e de acessar dados pessoais? Esse sistema pode, por exemplo, permitir a criação, aprovação, revisão e exclusão de contas dos usuários.	Controle de acesso	ANPD 3.1.3 (p. 35)	SIM
134	ANPD	3.2.2 (p. 50)	Todas as mídias que contenham dados pessoais são formatadas antes do descarte? Quando isso não for possível, como em CDs, DVDs, papel e de mídia portátil, sugere-se que seja realizada a destruição física da mídia.	Segurança dos dados pessoais armazenados	ANPD 3.2.2 (p. 50)	SIM

Tabela A.1: Lista final de controles utilizados na avaliação de risco.

ID	Origem	Código	Controle	Grupo	Referência Original	Controle Startups
135	ANPD	3.2.2 (p. 60)	Os dispositivos móveis de uso privado não são usados para fins de uso institucional? Caso não seja possível implementar medidas de segurança equivalentes às da organização, recomenda-se que dispositivos móveis pessoais não sejam utilizados para fins institucionais.	Medidas relacionadas ao uso de dispositivos móveis	ANPD 3.2.2 (p. 60)	SIM
136	ANPD	3.3 (p. 62)	A empresa atualmente implementa e monitora a funcionalidade de remoção remota de dados pessoais em dispositivos móveis, tanto institucionais quanto pessoais, como parte das medidas de segurança da informação?	Medidas relacionadas ao uso de dispositivos móveis	ANPD 3.3 (p. 62)	SIM
137	ANPD	3.4 (p. 66)	Os contrato de aquisição de serviços de nuvem possuem acordo de nível de serviço contemplando a segurança dos dados armazenados?	Medidas relacionadas ao serviço em nuvem	ANPD 3.4 (p. 66)	SIM
138	ANPD	3.4 (p. 67)	O serviço oferecido pelo provedor do serviço em nuvem atende os requisitos de segurança da informação estabelecidos pela empresa?	Medidas relacionadas ao serviço em nuvem	ANPD 3.4 (p. 67)	SIM
139	ANPD	3.4 (p. 68)	São utilizadas técnicas de autenticação multifator, como por exemplo, aplicativos autenticadores ou SMS para acesso aos serviços em nuvem relacionados a dados pessoais?	Medidas relacionadas ao serviço em nuvem	ANPD 3.4 (p. 68)	SIM
140	NBR ISO/IEC 27002:2005	A.10.1	A organização possui procedimentos operacionais documentados e acessíveis, abrangendo atividades como inicialização e desligamento de sistemas, geração de cópias de segurança, manutenção de equipamentos, tratamento de mídias e segurança da informação? Esses procedimentos incluem instruções para configuração de sistemas, processamento de informações, agendamento de tarefas, tratamento de erros, contatos de suporte, recuperação em caso de falha, gerenciamento de trilhas de auditoria e registros de sistemas, além de procedimentos de monitoramento? A direção autoriza mudanças nesses procedimentos, considerando-os como documentos formais? A organização busca uniformidade no gerenciamento de sistemas de informação, utilizando os mesmos procedimentos, ferramentas e utilitários quando possível?	Avaliar riscos da integração de novas soluções	NBR ISO/IEC 27002:2005 (A.10.1)	SIM

Referências Bibliográficas

[1] DIGITAL, S. de G. *Guia de Avaliação de Riscos de Segurança e Privacidade*. 2020. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-e-modelos>. Acesso em: 31 mar. 2023. (document), 1.3, 1.4, 2.3, 2.3.2, 2.3, 2.3.2, 2.1, 2.3.3, 2.2, 2.3, 3.1, 5.2

[2] SECURITY, C. for I. *CIS Controls version 8*. 2021. Disponível em: <https://www.cisecurity.org/controls/cis-controls-list/>. (document), 2.2.2, 2.1, 3.1

[3] DADOS, A. A. N. de Proteção de. *Guia de Tratamento para Agentes de Pequeno Porte*. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf>. Acesso em: 03 abr. 2023. (document), 2.2.3, 2.2, 3.1

[4] NEXO. *Banco Central comunica vazamento de dados de 160 mil chaves Pix*. 2022. Disponível em: <https://www.nexojornal.com.br/extra/2022/01/21/Banco-Central-comunica-vazamento-de-dados-de-160-mil-chaves-Pix>. Acesso em: 27 mar. 2023. 1.1

[5] MáXIMO, W. *Banese sofre falha de segurança e invasores acessam chaves Pix*. 2021. Disponível em: <https://agenciabrasil.ebc.com.br/economia/noticia/2021-09/banese-sofre-falha-de-seguranca-e-invasores-acessam-chaves-pix?ref=thehack.com.br>. Acesso em: 27 mar. 2023. 1.1

[6] ALECRIM, E. *Ministério da Saúde expõe dados de 243 milhões de pessoas*. 2020. Disponível em: <https://tecnoblog.net/noticias/2020/12/02/ministerio-saude-expoe-dados-243-milhoes-pessoas/>. Acesso em: 27 mar. 2023. 1.1

[7] CERT.BR; NIC.BR; CGI.BR. *Fascículo: Vazamento de dados*. 2021. Disponível em: <https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf>. Acesso em: 27 mar. 2023. 1.1

[8] IBM. *Cost of a Data Breach Report 2022*. 2022. Disponível em: <https://www.ibm.com/reports/data-breach>. Acesso em: 30 mar. 2023. 1.1

[9] BISSO, R. et al. 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*, v. 3, n. 1, 2020. 1.1

[10] ALMEIDA, S. d. C. D. d.; SOARES, T. A. Os impactos da lei geral de proteção de dados-lgpd no cenário digital. *Perspectivas em Ciência da Informação*, SciELO Brasil, v. 27, p. 26–45, 2022. 1.1, 2.1

[11] SERASA. *Pesquisa LGPD: Como as empresas se preparam para anteder à nova regulamentação*. 2020. Disponível em: <https://www.serasaexperian.com.br/images-cms/wp-content/uploads/2020/11/03225812/White-Paper-Serasa-Experian-LGPD-Como-as-Empresas-se-prepararam.pdf>. Acesso em: 31 mar. 2023. 1.1

[12] FUTSÆTER, N. *Best practices and motivational factors for information security in startups: An exploratory case study of four Norwegian tech startups*. Dissertação (Mestrado) — NTNU, 2019. 1.2

[13] CISO. *Ser pequena não significa que a empresa nunca sofrerá um ataque*. 2022. Disponível em: <https://www.cisoadvisor.com.br/ser-pequena-nao-significa-que-a-empresa-nunca-sofrera-um-ataque/>. Acesso em: 01 abr. 2023. 1.2

[14] 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*. Rio de Janeiro, RJ, Brasil: ABNT, 2011. 1.2, 2.3

[15] BRASIL. *Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais*. 2018. Disponível em: <https://www.planalto.gov.br/ccivil$_0$3/$_a$to2015 − 2018/2018/lei/l13709.htm>.*Acessoem* : 31*mar.*2023. 2.1, 2.1.1, 2.1.3, 2.3.1

[16] DADOS, C. C. de Governança de. *Guia de Boas Práticas - Lei Geral de Proteção de Dados*. 2020. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia$_l$gpd.pdf>.*Acessoem* : 31*mar.*2023. 2.1.1

[17] SêMOLA, M. *Gestão da segurança da informação*. [S.l.]: Elsevier Brasil, 2014. v. 2. 2.2, 2.2.1, 2.2.1, 2.2.1, 2.2.1

[18] Associação Brasileira de Normas Técnicas (ABNT). *ABNT NBR ISO/IEC 27002:2013 - Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de ativos de segurança da informação*. Rio de Janeiro, RJ, Brasil: ABNT, 2013. 2.2, 2.2.1

[19] NETO, P.; ARAUJO, W. *Segurança da Informação*. [S.l.]: Editora UFPB, 2019. 2.2, 2.3

[20] DANTAS, M. L. *Segurança da Informação: Uma Abordagem Focada em Gestão de Riscos*. [S.l.]: Livro Rápido, 2011. 2.2

[21] UNIãO, B. T. de Contas da. *Boas Práticas em Segurança da Informação*. Quarta. Brasília: TCU, 2012. 2.2

[22] FERNANDES, J. H. C. Introdução à gestão de riscos de segurança da informação. *Brasília: UNB*, 2009. 2.2.1, 2.3

[23] OWASP. *OWASP Proactive Controls*. 2018. Disponível em: <https://owasp.org/www-project-proactive-controls/>. Acesso em: 31 mar. 2023. 2.2.4, 3.1

[24] NETTO, A. d. S.; 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*, SciELO Brasil, v. 4, p. 375–397, 2007. 2.4.1

[25] NETO, G.; ALENCAR, G.; QUEIROZ, A. Proposta de modelo de segurança simplificado para pequenas e médias empresas. p. 299–306, 2015. 2.4.2, 3.1

[26] KAILA, U.; NYMAN, L. Information security best practices: First steps for startups and smes. *Technology Innovation Management Review*, Talent First Network, v. 8, n. 11, p. 32–42, 2018. 2.4.3

[27] VENTURA, F. *Netshoes paga 500 mil em danos morais após vazamento de dados*. 2019. Disponível em: <https://tecnoblog.net/noticias/2019/02/05/netshoes-acordo-mpdft-vazamento-dados/>. Acesso em: 27 mar. 2023.