gov.br

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

Guia de Requisitos e Obrigações Quanto a Privacidade e à Segurança da Informação

Programa de Privacidade e Segurança da Informação (PPSI)

Versão 3.2
Brasília, novembro de 2024

GUIA DE DE REQUISITOS E OBRIGAÇÕES QUANTO A PRIVACIDADE E À SEGURANÇA DA INFORMAÇÃO

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

Esther Dweck

Ministra

SECRETARIA DE GOVERNO DIGITAL

Rogério Souza Mascarenhas

Secretário de Governo Digital

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Leonardo Rodrigo Ferreira

Diretor de Privacidade e Segurança da Informação

COORDENAÇÃO-GERAL DE PRIVACIDADE

Julierme Rodrigues da Silva

Coordenador-Geral de Privacidade

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Segurança da Informação

Equipe Técnica de Elaboração

Denis Marcelo Oliveira

Julierme Rodrigues da Silva

Luiz Henrique do Espírito Santo Andrade

Tássio Correia da Silva

Wellington Francisco Pinheiro de Araújo

Equipe Técnica de Revisão - Versão 3.2

Adriano de Andrade Moura

Bruno Pierre Rodrigues de Sousa

Ivaldo Jeferson de Santana Castro

Raphael César Estevão

Rogério Vinicius Matos Rocha

Histórico de versões

Data	Versão	Descrição	Autor
11/12/2020	1.0	Primeira versão do Guia de Requisitos de Segurança da Informação e Privacidade em Contratações de Tecnologia da Informação.	Equipe Técnica de Elaboração
25/01/2021	2.0	Segunda versão do Guia de Requisitos de Segurança da Informação e Privacidade em Contratações de Tecnologia da Informação, considerando ajustes conforme nova versão da Instrução Normativa nº 1, de 4 de abril de 2019, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.	Equipe Técnica de Revisão
31/03/2023	3.0	Atualização para alinhamento com o Guia do Framework de Privacidade e Segurança da Informação, conforme destacado no Anexo II.	Equipe Técnica de Revisão
29/02/2024	3.1	Atualização da referência à Instrução Normativa da SGD para contratação de TIC, conforme destacado no Anexo II.	Equipe Técnica de Revisão
05/11/2024	3.2	Adequação do Modelo a Resolução CD/ ANPD Nº18, de 16 de julho de 2024	Equipe Técnica de Revisão

Sumário

1 Aviso preliminar e agradecimentos

O presente Guia, especialmente recomendado e dirigido aos órgãos e às entidades da Administração Pública Federal - APF, visa a auxiliar na Elaboração de um Termo de Referência para contratações de Soluções de Tecnologia da Informação e Comunicação (TIC) especificando Requisitos e Obrigações quanto à Privacidade e à Segurança da Informação, em atendimento ao previsto no art. 39 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), que estabelece que o operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria. Adicionalmente, a Elaboração de um Termo de Referência para contratação de Soluções de TIC contendo Requisitos e Obrigações quanto à Privacidade e à Segurança da Informação visa a atender, além da LGPD, a outros normativos vigentes sobre o tema de privacidade e segurança da informação.

Este documento é de autoria exclusiva da Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos e tem como referência fundamental o Guia do Framework de Privacidade e Segurança da Informação baseado em diversas publicações e documentos técnicos já existentes que são utilizados amplamente por profissionais da área de privacidade e segurança da informação. Destacam-se as publicações do Center for Internet Security (CIS), da International Organization for Standardization (ISO) e do National Institute of Standards and Technology (NIST). Com o objetivo de facilitar a difusão de conhecimentos sobre privacidade e segurança da informação, tais referências, quando escritas em línguas estrangeiras, foram traduzidas para o português pela equipe técnica da Diretoria de Privacidade e Segurança da Informação da Secretaria de Governo Digital.

Nesse cenário, a Secretaria de Governo Digital enfatiza que:

a) não representa, tampouco se manifesta em nome do CIS, da ISO e do NIST e vice-versa;
b) não se manifesta em nome de autoridades de privacidade e segurança da informação;
c) não é coautora das publicações internacionais abordadas;
d) não assume nenhuma responsabilidade administrativa, técnica ou jurídica por usos ou interpretações inadequadas, fragmentados ou parciais do presente modelo; e
e) caso o leitor deseje se certificar de que atende integralmente os requisitos das publicações das instituições mencionadas, deverá consultar diretamente as fontes oficiais de informação ofertadas por elas, que foram listadas na seção “Referências Bibliográficas” deste documento.

Finalmente, um agradecimento especial deve ser registrado ao CIS, à ISO, ao NIST e aos profissionais de privacidade e segurança da informação consultados, por suas valiosas contribuições para a comunidade e para elaboração deste documento.

Este Guia será atualizado frequentemente, de acordo com as novas diretrizes determinadas pelas autoridades em privacidade e segurança da informação ou segundo eventuais alterações que ocorram nos normativos vigentes relacionados a privacidade e segurança da informação e outras referências utilizadas neste documento.

2 Introdução

Este Guia tem por finalidade apresentar orientações com o intuito de auxiliar os órgãos e entidades da Administração Pública Federal, direta, autárquica e fundacional a especificar os Requisitos e Obrigações quanto à Privacidade e à Segurança da Informação em um Termo de Referência para contratações de Soluções de TIC no âmbito institucional.

Os Controles 15, 22 e 28 do Guia do Framework de Privacidade e Segurança da Informação (p. 54, 62 e 66) estabelecem que:

> **Controle 15: Gestão de Provedor de Serviços -** Com o objetivo de garantir a proteção das informações, sistemas e processos críticos da organização, estabeleça um processo para avaliar os provedores de serviços que operem e mantenham estes ativos da organização.
>
> **Controle 22: Políticas, Processos e Procedimentos -** Definir, desenvolver, divulgar, implementar e atualizar políticas, processos e procedimentos operacionais, internos e externos que regem as ações relativas à proteção de dados pessoais e privacidade, e controles para programas, sistemas de informação ou tecnologias que envolvam o tratamento de dados pessoais.
>
> **Controle 28: Supervisão em Terceiros -** A supervisão em terceiros visa garantir, através de meios contratuais ou outros, como políticas internas obrigatórias, que o terceiro destinatário implemente ações previstas pelo controlador no intuito de atender aos requisitos de conformidade com as leis e regulamentos de proteção de dados em vigor e requisitos de privacidade.

O presente Guia serve como um modelo prático a ser utilizado para auxiliar na adoção dos Controles 15, 22 e 28 do Guia do Framework de Privacidade e Segurança da Informação[1] v1 e respectivas evoluções desta versão (1.1, 1.2 etc.) elaborado e publicado pela SGD. As medidas dos Controles 15, 22 e 28 que estão contempladas por este Guia são respectivamente: 15.5 e 15.6, 22.4, 28.1, 28.2, 28.3, 28.4, 28.5, 28.6, 28.7, 28.8, 28.9, 28.10, 28.11, 28.12 e 28.13.

Este guia trata da inclusão de um passo adicional e necessário ao processo de elaboração dos artefatos inerentes a uma contratação de TIC. Este passo adicional consiste na incorporação dos Requisitos de Privacidade e Segurança da Informação nos instrumentos convocatórios (editais

[1] < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf >. Acesso em 15/04/2024

licitatórios) e contratos firmados com provedores/operadores para aquisição de produtos ou serviços de TIC, conforme destacado no passo 4 da **Figura 1**.

Figura 1 - Inclusão de Requisitos de Privacidade e Segurança da Informação

A Secretaria de Governo Digital (SGD) ressalta que, na época da elaboração deste Guia, tais orientações foram objeto de discussão e validação pelo Núcleo de Segurança da Informação das Plataformas de Governo Digital, composto por representantes da DATAPREV, Diretoria de Projetos da Secretaria Especial de Desburocratização, Gestão e Governo Digital (SEDGG) do Ministério da Economia, Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (DSI/GSI/PR), Secretaria Geral da PR, SERPRO e SGD/ME.

Destaca-se que aspectos inerentes à Lei Geral de Proteção de Dados Pessoais (LGPD), Lei 13.709 de 14 de agosto de 2018, foram abordados, em especial os que abrangem a implantação de mecanismos de gerenciamento de riscos e avaliação de impacto na privacidade, bem como diversos mecanismos de controle de privacidade, que constam em normas ABNT, conforme destacado na **Tabela 1**.

Cabe ressaltar que fica a cargo da equipe de planejamento da contratação identificar os requisitos aplicáveis às especificidades do objeto a ser contratado. Por este motivo, os requisitos, presentes neste guia, não possuem caráter obrigatório tampouco exaustivos.

Sugere-se a aplicabilidade, no que couber, das orientações contidas nos documentos destacados na **Tabela 1**, esclarecendo que em alguns casos fazemos referência explícita a alguns destes documentos.

DOCUMENTOS APLICÁVEIS			
01	ABNT NBR ISO/IEC 27001:2013: Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos.	**06**	ISO/IEC 29134:2017: Information Technology – Security techniques – Guidelines for privacy impact assessment.
02	ABNT NBR ISO/IEC 27002:2013: Tecnologia da Informação – Técnicas de segurança – Código de Prática para controles de segurança da informação.	**07**	ISO/IEC 29151:2017: Information Technology – Security techniques – Code of pratice for personally identifiable information protection.
03	ABNT NBR ISO/IEC 27005:2011: Tecnologia da Informação – Técnicas de segurança – Gestão de riscos de segurança da informação.	**08**	Guia de Boas Práticas LGPD
04	ABNT NBR ISO/IEC 27701:2019: Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão de privacidade da informação – Requisitos e diretrizes.	**09**	Legislação GSI: • PNSI; • Estratégia Nacional de Segurança Cibernética; • Glossário de Segurança da Informação; • Requisitos Mínimos de Segurança Cibernética que devem ser adotados no estabelecimento das redes 5G.
05	ABNT NBR ISO/IEC 31000:2018: Gestão de Riscos - Diretrizes	**10**	Guia do Framework de Privacidade e Segurança da Informação

Tabela 1 - Documentos Aplicáveis

Este Guia de Requisitos e Obrigações quanto à Privacidade e à Segurança da Informação foi estruturado em quatro seções, a saber:

- Requisitos gerais de estruturação de privacidade e segurança a serem adotados pela Contratada.
- Requisitos de Privacidade e Segurança da Informação.
- Ações de Responsabilidade da Contratada.
- Gestão do Contrato.

3 Requisitos Gerais de Estruturação de Privacidade e Segurança

Ao firmar um contrato de fornecimento de solução de TIC, ou mesmo em renovação contratual, o órgão contratante deve estabelecer, no que couber, requisitos gerais de estruturação de privacidade e segurança **(Figura 2)**, considerando que o tratamento de dados pessoais está sujeito à conformidade com a Lei 13.709/2018. Sugere-se, portanto, a aplicabilidade com comprovação pelo contratado, no que couber, das orientações contidas na norma ISO/IEC 29151:2017. Deve ser dada especial atenção ao item 15 da referida norma que discorre sobre a questão de relacionamento com controladores e operadores[2] que atuam no fornecimento de serviços sobre dados pessoais, como por exemplo, política de segurança da informação neste relacionamento, diretrizes para implantação da privacidade de dados pessoais, dados mínimos que devem estar contidos no contrato, abordagem de segurança dentro dos acordos, cadeia de suprimentos de TIC, entregas etc. Assim sendo, espera-se que **a empresa contratada apresente documentos comprobatórios referentes às exigências destacadas a seguir:**

Figura 2 - Requisitos gerais de estruturação de privacidade e segurança

[2] Lei 13.709/2018, Art. 5º - VI - Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

3.1 Política de Segurança da Informação (POSIN)

A empresa contratada deverá possuir uma **Política de Segurança da Informação (POSIN)**, ou equivalente, aderente ao disposto na IN GSI/PR nº 1, de 27 de maio de 2020, incluindo políticas ou normas para proteção de dados pessoais vigentes e atualizadas, com processo de revisão periódico formalizado e institucionalizado, de forma a garantir, dentre outros requisitos, o uso de sistemática e procedimentos de segurança da informação para assegurar não apenas a disponibilidade, a integridade, a confidencialidade e a autenticidade, mas também a consistência, a privacidade e a confiabilidade dos dados e informações tratados pela Solução de TIC;

3.2 Avaliação de impacto de privacidade

Realizar, em conjunto com a contratante, **avaliação de impacto na privacidade** relacionada à Solução de TIC, considerando o descrito pelo relatório de impacto à proteção de dados pessoais, conforme previsto na Lei nº 13.709/2018, quando da concepção de qualquer novo projeto, produto ou serviço;

3.3 Análise e avaliação de riscos

Realizar e apresentar à contratante periodicamente uma **análise/avaliação de riscos** da arquitetura de Solução de TIC, indicando os eventos de risco ao qual o sistema está exposto, baseada em prévia análise de vulnerabilidades dos ativos que compõem a Solução de TIC, resguardando os segredos de negócio, direitos autorais e direitos de propriedade intelectual aplicáveis, conforme metodologia indicada pela contratante;

3.4 Arquitetura, controles de privacidade e de segurança da informação e matriz de responsabilidades

Apresentar, em tempo determinado pela contratante:

a) Documentação que descreve a **arquitetura física e lógica** da Solução de TIC;
b) Uma descrição dos **controles de privacidade e segurança da informação** implementados em cada componente descrito na arquitetura física e lógica; e
c) A **matriz de responsabilidades** detalha a atribuição das responsabilidades pela privacidade e segurança da informação na organização. Ela identifica os gestores de serviços que lidam com dados pessoais e o(s) operador(es) de tratamento de dados, em relação ao objeto da contratação e aos itens descritos neste documento.

3.5 Continuidade operacional e contingência

Possuir e implementar um **Plano de Continuidade Operacional e um Plano de Contingência** relacionados ao objeto contratado, que garantam o nível requerido de continuidade para a segurança da informação durante uma situação adversa;

3.6 Gestão de incidentes

Possuir um processo de **Gestão de Incidentes** que registre os incidentes de privacidade e segurança da informação ocorridos e que contemple: 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; além de implementar e manter controles e procedimentos específicos para **detecção, tratamento e resposta a incidentes de segurança da informação e de privacidade**, de forma a reduzir o nível de risco ao qual o objeto do contrato e/ou a contratante estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela contratante;

3.7 Coleta e preservação de evidências

Implementar os controles necessários para **coleta e preservação de evidências** de incidentes de segurança da informação e privacidade;

3.8 Gestão de mudanças

Possuir e implementar processo de **gestão de mudanças** adequado para que mudanças na organização, nos processos de negócio e nos recursos de processamento da informação sejam controlados e não afetem a privacidade e a segurança da informação, reduzindo o nível de risco ao qual o objeto do contrato e/ou a contratante está exposta, considerando os critérios de aceitabilidade de riscos definidos pela contratante. No caso de contratação de sistemas de informação, se aplicável, considerar ainda na **gestão de mudanças** o processo referente a migração dos dados do sistema legado para o novo sistema;

3.9 Gestão de capacidade

Dispor possuir e implementar processo de **gestão de capacidade** e recursos para **redundância** de forma que a utilização dos recursos seja monitorada, ajustada e as projeções das necessidades de capacidade futura sejam avaliadas para garantir o desempenho dos ativos relacionados ao objeto do contrato, assegurando também a disponibilidade e recuperação de dados e informações, em conformidade com um plano de continuidade relacionado ao objeto contratado, que garanta o nível requerido de continuidade para a segurança da informação durante uma situação adversa;

3.10 Desenvolvimento seguro

Possuir e manter trilhas de qualidade e teste de software, e realizar **desenvolvimento seguro**, aderente ao que for disposto em dispositivos legais correlatos em publicações feitas pelo GSI/PR; determinado pela contratante:

a) Os dados pessoais utilizados em ambiente de TDH (teste, desenvolvimento e homologação) devem passar por um processo de **anonimização**;
b) A utilização dos dados pessoais em ambiente de TDH (teste, desenvolvimento e homologação), não anonimizados, deve **ser autorizada** pelo proprietário do ativo de informação;
c) A Contratada deve utilizar 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 no processo;
d) A aplicação desenvolvida pela Contratada deve ter funcionalidade para, ao **fornecer a base de informações** para órgãos de pesquisa, os dados pessoais sejam anonimizados ou pseudoanonimizados;
e) A Contratada deve possuir e implementar política de privacidade que atenda aos princípios da Lei Geral de Proteção de Dados Pessoais (LGPD), a ser homologada pelo órgão contratante, assegurando o adequado tratamento dos dados pessoais e principalmente sua **classificação em sensíveis e não sensíveis**, incluindo categorias de informações pessoais de saúde e informações pessoais financeiras
f) O Contratante e a Contratada realizarão a **avaliação de impacto na privacidade** relacionada à Solução de TIC, devendo considerar as informações levantadas pelo relatório de impacto da Contratada.

3.11 Segurança das redes corporativas

Implementar e manter controles e procedimentos específicos para **assegurar o nível adequado de segurança da informação às redes corporativas da Contratante e da Contratada**, de forma a reduzir o nível de risco ao qual a Solução de TIC e a contratante estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela contratante:

a) Implementar e manter controles e procedimentos específicos de Segurança Web, nos servidores da aplicação, ou na própria aplicação, para garantir o nível adequado de privacidade e segurança da informação.

3.12 Política de backup

Possuir e implementar política de backup das informações e dos registros de log da solução contratada, em conformidade com os dispositivos legais aplicáveis, a ser homologada pela contratante, que assegure a manutenção de cópias de segurança de todos os componentes de software dos sistemas, de suas bases de dados e da documentação associada, observando a técnica, os cuidados requeridos para cada caso, de modo a ser possível a plena recuperação de versões dos sistemas e dados salvaguardados em caso de falha ou por solicitação da contratante, reduzindo o nível de risco ao qual o objeto do contrato e/ou a contratante está exposta, considerando os critérios de aceitabilidade de riscos definidos pela contratante.

4 Requisitos de Privacidade e Segurança da Informação

A Equipe de Planejamento da Contratação deve estabelecer no que couber, ao definir os requisitos de privacidade e segurança da informação de que tratam as alíneas “f” do inciso I e “i” do inciso II do caput do art. 16 da IN SGD/ME nº 94/2022, que a Solução de TIC deve possuir os seguintes itens em destaque na **Figura 3**:

Figura 3 Requisitos de privacidade e segurança da informação

4.1 Controles criptográficos

Implementar e **manter controles criptográficos** para armazenamento, tráfego e tratamento da informação, de acordo com o nível de criticidade e grau de sigilo da informação definido pela contratante, observando a periodicidade e tempo de guarda legalmente estabelecidos ou definidos pela contratante.

4.2 Controle de acesso

Implementar **controles de acesso** baseados em uma política de controle de acesso para o objeto contratado, elaborada pela contratante em conjunto com a contratada, tendo em vista o princípio do menor privilégio, a privacidade e a segurança da informação, de forma a reduzir o nível de risco ao qual o objeto e a contratante estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela contratante. A política deve estabelecer, dentre outros critérios, que se deve conceder autorizações de acesso apenas quando realmente sejam necessárias para o desempenho de uma atividade específica, definindo também protocolos para cadastramento, mecanismo de controle de acesso (como, por exemplo, validação de formulário), habilitação, inabilitação, atualização de direitos de acesso e exclusão de usuário, além de

revisões periódicas da política. A política também deve definir situações e protocolos para acesso às informações sensíveis, necessidades de não repúdio, situações que requerem autenticação via duplo fator e acesso via certificado digital, nos casos em que a contratante julgar necessário.

4.3 Registro de eventos e incidentes de segurança

Implementar os controles necessários para o **registro de eventos e incidentes** de privacidade e segurança da informação.

4.4 Registro de eventos e rastreabilidade

Implementar e manter controles específicos para **registro de eventos e rastreabilidade** de forma a manter trilha de auditoria de privacidade e segurança da informação, aderente a disposto em dispositivo legal correlato publicado pelo GSI/PR, de forma a assegurar a rastreabilidade das ações de usuário por meio de logs de transações e de acesso aos sistemas, conforme especificação de requisitos, e gerá-los e disponibilizá-los à contratante para fins de auditorias e inspeções

4.5 Salvaguarda de logs

Implementar medidas de **salvaguarda para os logs** descritos no item anterior, bem como controles específicos para **registro das atividades dos administradores** e operadores dos sistemas relacionados ao objeto do contrato, de forma que esses não tenham permissão de exclusão ou desativação dos registros (log) de suas próprias atividades.

4.6 Compartilhamento, uso e proteção da informação

Contemplar procedimentos e controles adequados para compartilhamento, uso e proteção da informação e os casos de compartilhamento de informações com terceiro devem ser avaliados pela contratante, por intermédio da autoridade competente, a qual caberá autorizar a divulgação do mínimo de informações necessárias para cada compartilhamento, caso julgue apropriado, preservados os casos de sigilo previstos na legislação aplicável e de proteção de dados pessoais disposto pela Lei nº 13.709/2018.

4.7 Análise de vulnerabilidades

Executar periodicamente **análise de vulnerabilidades** na Solução de TIC, para detecção de vulnerabilidades técnicas e execução de medidas para seu saneamento ou contenção. Além disso, é necessário que haja um processo documentado para gestão de vulnerabilidades em soluções de TIC. Ele deverá ser revisado e atualizado periodicamente, principalmente quando ocorrerem mudanças na organização

4.8 Internet das coisas (IoT)

Implementar mecanismos de segurança da informação e privacidade relativos à **Internet das Coisas (IoT)** conforme critérios, diretrizes, princípios e métodos dispostos em dispositivo legal correlato publicado pelo GSI/PR.

5 Ações de responsabilidade da contratada

Nas descrições abaixo e conforme **Figura 4**, destacam-se itens relativos às responsabilidades que devem ser imputadas, no que couber, à empresa Contratada.

5.1 Recursos em versões comprovadamente seguras e atualizadas

Utilizar recursos de segurança da informação e de tecnologia da informação de qualidade, eficiência e eficácia reconhecidas e em **versões comprovadamente seguras e atualizadas**, de forma reduzir o nível de risco ao qual o objeto do contrato e/ou a contratante está exposta, considerando os critérios de aceitabilidade de riscos definidos pela contratante.

Figura 4 - Ações de Responsabilidade da Controlada

5.2 Reportar incidentes

Reportar de imediato à contratante incidentes que envolvam vazamento de dados, indisponibilidade ou comprometimento da informação relacionados à Solução de TIC. É necessário que a comunicação seja feita de forma tempestiva para que as providências sejam tomadas em tempo hábil de modo a solucionar o incidente ou amenizar seus efeitos.

5.3 Termo de compromisso e ciência

Implementar e manter controles e procedimentos específicos para assegurar completo e absoluto sigilo quanto a todos os dados e informações de que o preposto ou os demais empregados da contratada venham a tomar conhecimento em razão da execução do contrato, de forma a assegurar que seus empregados e outros profissionais sob sua direção e/ou controle respeitem o uso dos dados somente para as finalidades previstas em contrato e as restrições de uso dos ativos utilizado para desenvolvimento e/ou operação da Solução de TIC, cumprindo e

fazendo cumprir o disposto nos **Termo de Compromisso e Termo(s) de Ciência** firmados respectivamente, pelo representante legal e pelo(s) empregado(s) da contratada.

5.4 Descarte seguro

Definir e executar procedimento de **descarte seguro** dos dados pessoais ou sigilosos da contratante ao encerrar a execução do contrato ou mediante sua solicitação.

5.5 Revogação de privilégios

Comunicar à contratante, de imediato, a ocorrência de transferência, remanejamento ou demissão de funcionário, para que seja providenciada a **revogação de todos os privilégios** de acesso aos sistemas, informações e recursos da contratante, porventura colocados à disposição para realização dos serviços contratados.

5.6 Utilização de serviços terceiros

Informar e obter a anuência do órgão contratante sobre a **utilização de serviços de terceiros** (como Content Delivery Network, Youtube, Flicker etc.) para sustentar ou viabilizar o funcionamento da Solução de TIC.

5.7 Segurança física e do ambiente

Implementar e manter, em conjunto com a contratante, controles e procedimentos específicos para assegurar a **segurança física e do ambiente** de acesso às bases, informações, sistemas e demais ativos que compõem a Solução de TIC, de forma a prevenir qualquer tipo de ocorrência de evento de efeitos danosos ou prejudiciais ao funcionamento dos recursos de processamento das informações relacionadas à Solução de TIC, reduzindo assim o nível de risco ao qual o objeto do contrato e/ou a contratante estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela contratante.

5.8 Ambientes tecnológicos

Assegurar que os **ambientes tecnológicos** de desenvolvimento, teste, homologação e produção estejam segregados e possuam controles de privacidade e segurança da informação adequados a cada ambiente, de forma a reduzir o nível de riscos de acessos ou modificações não autorizadas.

5.9 Auditabilidade

Apresentar à contratante, sempre que solicitado, toda e qualquer informação e documentação que comprovem a implementação dos requisitos de privacidade e segurança da informação especificados na contratação, de forma a assegurar a **auditabilidade** do objeto contratado, bem como demais dispositivos legais aplicáveis.

5.10 Auditoria de privacidade e segurança da informação

Disponibilizar todos os recursos necessários, de forma tempestiva, para que a contratante, ou outra entidade por ela indicada, realize atividade continuada de **auditoria de privacidade e segurança da informação** relacionadas ao objeto do contrato.

5.11 Tratamento de incidentes de privacidade e segurança da informação

Realizar em conjunto com a contratante, ou com outros órgãos por ela indicados, **ações de tratamento de incidentes de privacidade e segurança da informação** relacionados ao objeto do contrato, bem como apoiar essas ações com o monitoramento e o envio de informações tempestivos.

5.12 Direito dos titulares

Implementar meios práticos para permitir que os titulares exerçam seu direito de gerenciamento dos dados pessoais.

6 Gestão de Contratos

Nas descrições abaixo e conforme **Figura 5**, destacam-se dispositivos que a Equipe de Planejamento da Contratação, ao elaborar o Modelo de Gestão do Contrato deve garantir que o contrato.

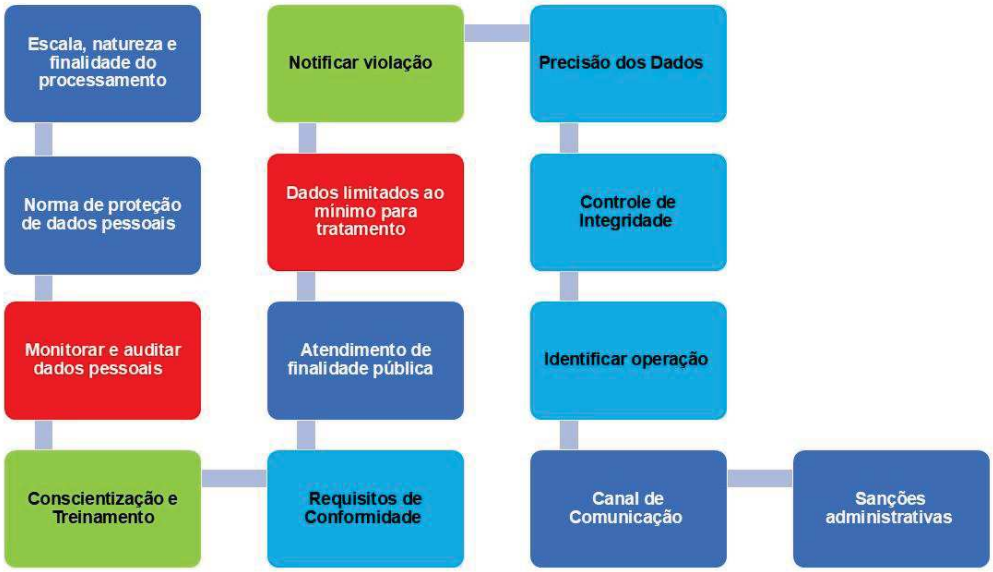

Figura 5 - Gestão de Contrato

6.1 Escala, natureza e finalidade do processamento

O Modelo de Gestão do Contrato, para contratos firmados com os operadores de dados pessoais, deve incluir cláusulas que contemplem, 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; conforme previsto pela Lei Geral de Proteção de Dados, Lei nº 13.709/2018.

6.2 Norma de proteção de dados pessoais

Dispositivo que garanta uma política ou norma de proteção de dados pessoais que aborde a finalidade da contratada perante o processamento de dados; a transparência com relação à coleta e processamento; a estrutura estabelecida para a proteção; regras para tomar decisões relacionadas a dados pessoais; critérios de aceitação de risco e compromisso de satisfazer os requisitos aplicáveis de proteção à privacidade.

6.3 Monitorar e auditar dados pessoais

Dispositivo para controle de proteção de dados pessoais que devem ser monitorados e auditados periodicamente para garantir que as operações que envolvam dados pessoais estejam em conformidade com as leis, regulamentos e termos contratuais aplicáveis.

6.4 Conscientização e treinamento

Dispositivo para implementação e manutenção de estratégia abrangente de conscientização e treinamento, destinada a garantir que os envolvidos entendam suas responsabilidades e os procedimentos de proteção de dados pessoais

6.5 Requisitos e conformidade

Dispositivo para o monitoramento contínuo das 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, comparando o desempenho em todo processo e também da organização, capaz de identificar vulnerabilidades e lacunas na política e na implementação e capaz de identificar modelos de sucesso.

6.6 Atendimento de finalidade pública

Dispositivo para que o tratamento de dados pessoais seja 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).

6.7 Dados limitados ao mínimo para tratamento

Dispositivo para que os dados coletados e seu processamento sejam limitados ao **mínimo necessário para atendimento da finalidade** do tratamento.

6.8 Notificar violação

Dispositivo que defina a obrigação do operador de dados pessoais **notificar** o Controlador em caso de ocorrência de **violação** de dados pessoais.

6.9 Precisão dos dados

Dispositivo que define que a contratada implemente medidas que **garantam e maximizem a precisão dos dados** pessoais coletados, antes de qualquer armazenamento ou processamento de dados pessoais.

6.10 Controle de integridade

Dispositivo que defina que os dados pessoais armazenados/retidos possuam controles de **integridade** permitindo identificar se os dados foram alterados sem permissão.

6.11 Identificar operação

Dispositivo que defina que as operações de processamento realizadas com dados pessoais sejam registradas de modo a **identificar a operação** realizada, quem realizou, data e hora.

6.12 Canal de comunicação

Dispositivo que defina 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 Contratada.

6.13 Sanções administrativas

Dispositivo que estipule **sanções** administrativas pelo descumprimento de cada um dos requisitos de segurança da informação e de privacidade especificados. No **Anexo I** deste guia são relacionadas as possíveis sanções que devem ser aplicadas em caso de descumprimento de cláusulas contratuais.

7 Referências Bibliográficas

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS: ABNT NBR ISO/IEC 27001:2013: **Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação - Requisitos.** Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002:2013: **Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação.** Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27005:2011: **Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.** Rio de Janeiro, 2011

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27701:2019: **Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes.** Rio de Janeiro, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 31000:2018: **Gestão de Riscos — Diretrizes.** Rio de Janeiro, 2018.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 09 set. 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Decreto nº 9.637, de 26 de dezembro de 2018. Política Nacional de Segurança da Informação – PNSI**. Disponível em: D9637 (planalto.gov.br) Acesso em: 09 set. 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Instrução Normativa nº 01, de 27 de maio de 2020. Brasília, DF, GSI/PR, 2020**. Disponível em: https://www.gov.br/gsi/pt-br/ssic/legislacao/copy_of_IN01_consolidada.pdf. Acesso em: Acesso em: 09 set. 2024.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações**. Instrução Normativa nº 04, de 26 de março de 2020. Brasília, DF, GSI/PR, 2020.** Disponível em: https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-4-de-26-de-marco-de-2020-250059468. Acesso em: 09 set. 2024.

BRASIL. Presidência da República. Subchefia para Assuntos Jurídicos. **Decreto nº 10.222 de 5 de fevereiro de 2020. Estratégia Nacional de Segurança Cibernética.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em: 09 set. 2020.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Portaria nº 93, de 26 de setembro de 2019. Glossário de Segurança da Informação**. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663. Acesso em: 09 set. 2024.

COMITÊ CENTRAL DE GOVERNANÇA DE DADOS - CCGD. **Guia de Boas Práticas LGPD**. Abril 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 09 set. 2024.

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE GOVERNO DIGITAL – DPSI/SGD. **Guia do Framework de Privacidade e Segurança da Informação. Março 2024**. Disponível em:https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf . Acesso em: 09 set. 2024.

INTERNATIONAL STANDARD. **ISO/IEC 29134:2017: Information technology – Security techniques – Guidelines for privacy impact assessment**. Genebra, 2017.

INTERNATIONAL STANDARD. **ISO/IEC 29151:2017: Information technology — Security techniques — Code of practice for personally identifiable information protection**. Genebra, 2017.

BRASIL. Ministério da Economia. Secretária de Governo Digital SGD/ME. **Instrução Normativa nº 94, de 23 de dezembro de 2022**. Disponível em: < https://www.gov.br/governodigital/pt-br/contratacoes/instrucao-normativa-sgd-me-no-94-de-23-de-dezembro-de-2022>. Acesso em: 09 set. 2024.

8 Anexo I

8.1 Sanções administrativas pelo descumprimento de requisitos

1. Tendo em vista a tabela de infrações destacada abaixo, a Equipe de Planejamento da Contratação deve, no que couber, estabelecer **percentual de multa (diária ou mensal) sobre o faturamento mensal ou valor total do contrato**, de acordo com o cronograma financeiro previsto para a contratação.
2. As infrações apresentadas neste Anexo, devem ser ajustadas de acordo com a realidade específica de cada contratação, desde que para cada requisito de segurança da informação especificado seja definida, no mínimo, uma infração correspondente.

Item de referência do Guia	Infração cometida
3.1	Não apresentar a POSIN - Política de Segurança da Informação.
3.2	Não apresentar o Relatório de Impacto à Proteção de Dados Pessoais – RIPD relacionado a solução de TIC.
3.3	Não apresentar o Relatório de Análise e Avaliação de Riscos de acordo com a periodicidade definida pela CONTRATANTE.
3.4	Não apresentar documentação, quando solicitada, que descreve a Arquitetura Física e Lógica do Objeto, Controles de Segurança da Informação e Matriz de Responsabilidades
3.4	Não apresentar descrição dos Controles de Segurança da Informação implementados em cada componente listado na Arquitetura Física e Lógica.
3.5	Não apresentar Plano de Continuidade Operacional e Plano de Contingência.
3.6	Não apresentar documento que evidencie o processo formal de Gestão de Incidentes.
3.7	Não apresentar documento que evidencie os controles implementados para Coleta e Preservação de Evidências de incidentes de segurança da informação e privacidade.
3.8	Não apresentar documento que evidencie o processo de Gestão de Mudanças.
3.9	Não apresentar documento que evidencie o processo de Gestão de Capacidade.
3.10	Não apresentar documentação que comprove estar em conformidade com Desenvolvimento Seguro presente em dispositivo legal correlato publicado pelo GSI/PR.

3.11	Não apresentar documentação que comprove estar em conformidade com nível adequado de Segurança da Informação das Redes Corporativas da Contratante e da Contratada.
3.12	Não apresentar documentação referente a Política de Backup.
4.1	Não apresentar documentação, referente aos Controles Criptográficos.
4.2	Não apresentar documento probatório que evidencie as Políticas e Controles de Acesso.
4.3	Não apresentar documentos de comprovação de Registros de Eventos e Incidentes de Segurança.
4.4	Não apresentar documentos de comprovação de Registros de Eventos e Rastreabilidade.
4.5	Não apresentar comprovação de Salvaguarda de Logs e registro das atividades de administradores e operadores.
4.6	Não apresentar documentos de comprovação de procedimentos e controles adequados para Compartilhamento, uso e proteção da informação.
4.7	Não apresentar documentos de comprovação de procedimentos periódicos de Análise de Vulnerabilidades.
4.8	Não apresentar documentação, quando solicitada, que evidencie a implementação de mecanismos relativos à Internet das Coisas (IoT) conforme critérios, diretrizes, princípios e métodos dispostos em dispositivo legal correlato publicado pelo GSI/PR.
5.1	Não apresentar documentação que evidencie a utilização de técnicas ou métodos apropriados de desenvolvimento seguro, com Versões Comprovadamente Seguras e Atualizadas.
5.2	Não apresentar documentação para Reportar de Incidentes.
5.3	Não apresentar Termos de Compromisso e Ciência.
5.4	Não apresentar documentação de que a Solução de TIC possui processamento que garante Descarte Seguro.
5.5	Não apresentar documentação das providências de Revogação de Privilégios quando solicitado.
5.6	Não obter anuência da CONTRATANTE sobre a Utilização de Serviços de Terceiros (como Content Delivery Network, Youtube, Flicker, etc.) para sustentar ou viabilizar o funcionamento da Solução de TIC.

5.7	Não apresentar documentos que comprovem procedimentos de Segurança Física e do Ambiente.
5.8	Não apresentar documentos que asseguram que os Ambientes Tecnológicos de desenvolvimento, teste, homologação e produção estejam segregados
5.9	Não apresentar documentação que comprovem a implementação dos requisitos de segurança da informação e privacidade especificados na contratação para assegurar a Auditabilidade do objeto contratado.
5.10	Não disponibilizar recursos para Auditoria de Segurança da Informação e Privacidade relacionadas ao objeto do contrato.
5.11	Não realizar em conjunto com a contratante, ou com outros órgãos por ela indicados, ações de Tratamento de Incidentes de Privacidade e Segurança da Informação relacionados ao objeto do contrato.
6.2	Não apresentar documentação que garanta política ou Norma de proteção de dados pessoais que aborde a finalidade da contratada perante o processamento de dados.
6.3	Não apresentar o processo para controle de proteção de dados pessoais que devem ser monitorados e auditados.
6.4	Não apresentar o processo de Conscientização e Treinamento dos envolvidos no processamento e proteção dos dados.
6.5	Não apresentar documentação de monitoramento contínuo das ações de proteção de dados pessoais para o cumprimento dos Requisitos de Conformidade.
6.6	Não apresentar documentação que comprove que o tratamento de dados pessoais é realizado para o Atendimento de sua Finalidade Pública.
6.7	Não apresentar documentação que comprove que o tratamento de dados está limitado ao mínimo necessário para atendimento da finalidade do tratamento.
6.8	Não notificar o Controlador em caso de ocorrência de violação de dados pessoais.
6.9	Não apresentar documentação que comprove que foram implementadas medidas que garantem e maximizam a Precisão dos Dados pessoais coletados.
6.10	Não apresentar documentação que comprove que os dados pessoais armazenados/retidos possuem Controles de Integridade.
6.11	Não apresentar documentação que define que as operações de processamento realizadas com dados pessoais são registradas identificando a operação realizada, quem realizou, data e hora

6.12	Não apresentar documentação que define o Canal de Comunicação.

9 Anexo II

Este anexo tem a finalidade de fornecer os destaques das mudanças inseridas nas versões do Guia de Requisitos e Obrigações quanto a Privacidade e a Segurança da Informação em comparação com o documento originalmente publicado em março de 2021.

Mudanças da Versão 3.2

As mudanças inseridas nesta versão em comparação com a anterior visam a adequação do Guia com a Resolução CD/ANPD Nº 18, de 16 de julho de 2024. Para isso, o item 1.4 foi ajustado para alinhar o documento às diretrizes da resolução mencionada.

Mudanças da Versão 3.1

Foi realizada a atualização na seção 2 para referenciar a nova IN SGD/ME nº 94/2022 em substituição a IN SGD/ME nº 1/2019, além de ter sido inserido como referência a medida 22.4 do Guia do Framework de Privacidade e Segurança da Informação v1.1.2 na introdução deste documento.

Mudanças da Versão 3.0

Primeiramente, ressalta-se que as mudanças inseridas nesta versão em comparação com a anterior visam a adequação com o Guia do Framework de Privacidade e Segurança da Informação v1 elaborado e publicado pela SGD em novembro de 2022.

Foram realizadas inclusões de: seção sobre aviso preliminar e agradecimentos; referência de que controle e medidas do Framework de Privacidade e Segurança da Informação são atendidos pelo Guia de Requisitos e Obrigações quanto a Privacidade e a Segurança da Informação; e remoção da seção sobre conclusão para padronização com os demais guias operacionais.

Além disso, foi realizada a inclusão de um tópico na seção 3 sobre direitos dos titulares, o alinhamento do texto com as medidas descritas nos Controles apresentadas no Guia do Framework, ajustes de figuras e o alinhamento da numeração das seções com o modelo do Guia do Framework de Privacidade e Segurança da Informação v1.