Guia de Requisitos e de Obrigações quanto a Segurança da Informação e Privacidade

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Versão 2.0

Brasília, Março de 2021

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

MINISTÉRIO DA ECONOMIA

Paulo Roberto Nunes Guedes

Ministro

SECRETARIA ESPECIAL DE DESBUROCRATIZAÇÃO, GESTÃO E GOVERNO DIGITAL

Caio Mario Paes de Andrade

Secretário Especial de Desburocratização, Gestão e Governo Digital

SECRETARIA DE GOVERNO DIGITAL

Luis Felipe Salin Monteiro

Secretário de Governo Digital

DEPARTAMENTO DE GOVERNANÇA DE DADOS E INFORMAÇÕES

Mauro Cesar Sobrinho

Diretor do Departamento de Governança de Dados e Informações

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

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 Elaboração

SUMÁRIO

INTRODUÇÃO

O objetivo deste guia é fornecer orientações básicas às instituições públicas para a especificação de requisitos mínimos necessários de Segurança da Informação e Privacidade em contratações de Soluções de Tecnologia da Informação (TIC). Ressaltamos que no processo de elaboração dos artefatos inerentes a uma contratação de TIC este guia trata de um passo adicional acrescido ao referido processo, conforme destacado no passo 4 da **Figura 1** a seguir, que é a inclusão dos Requisitos de Segurança da Informação e Privacidade na contratação de produto ou serviço de TIC.

Figura 1 – Inclusão de Requisitos de Segurança de Informação e Privacidade

A Secretaria de Governo Digital (SGD) ressalta que 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 (ME), 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 análise de impacto na privacidade dos dados pessoais, bem como diversos mecanismos de controle de privacidade, que constam em normas ABNT, conforme destacado na Fig 2. Documentos Aplicáveis.

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. Este

guia de requisitos de Segurança da Informação e Privacidade em contratações de Tecnologia da Informação foi estruturado em quatro capítulos, a saber:

• O Capítulo 1 - Requisitos gerais de estruturação de segurança e privacidade a serem adotados pela Contratada;

• O Capítulo 2 - Requisitos de Segurança da Informação e Privacidade;

• O Capítulo 3 - Ações de Responsabilidade da Contratada;

• O Capítulo 4 - Gestão do Contrato

Sugere-se a aplicabilidade, no que couber, das orientações contidas nos documentos referenciados no item deste guia, Bibliografia (Documentos Aplicáveis - **Figura 2**), esclarecendo que em alguns casos fazemos sua referência explícita.

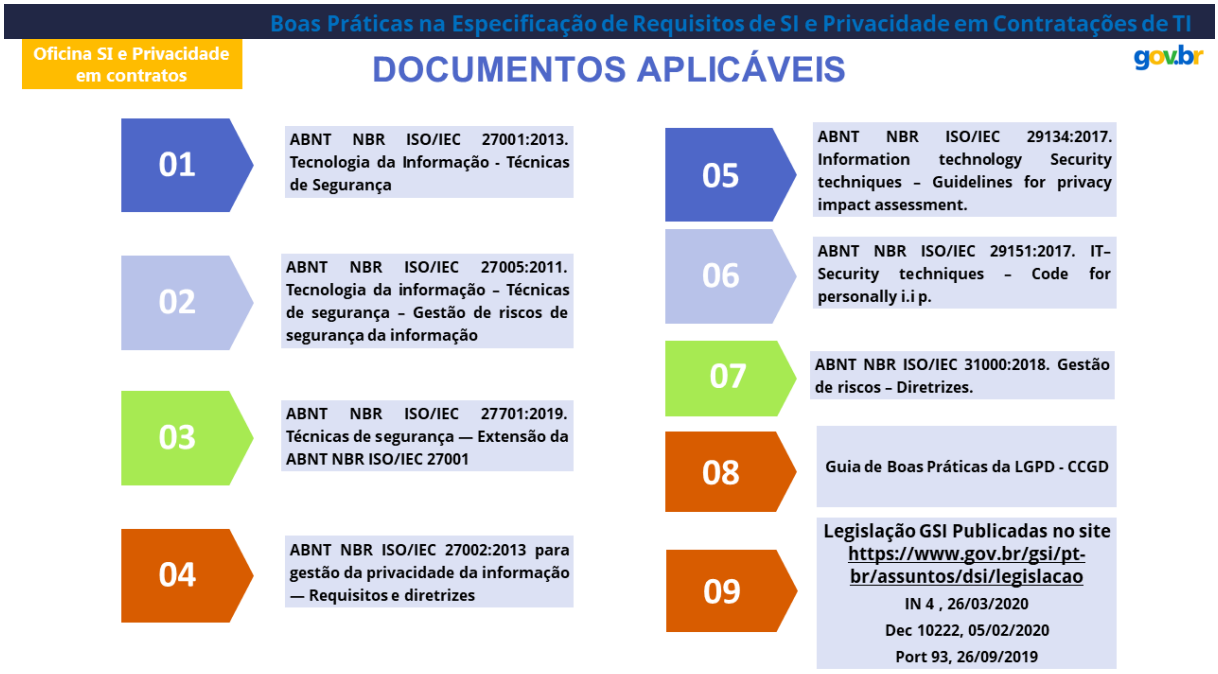

Figura 2 – Documentos Aplicáveis

Este guia será atualizado e ampliado periodicamente com objetivo de mantê-lo alinhado às diretrizes e normativos vigentes.

1 REQUISITOS GERAIS DE ESTRUTURAÇÃO DE SEGURANÇA E PRIVACIDADE

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 segurança e privacidade (**Figura 3**), 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[1] 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 3 - Requisitos gerais de estruturação de segurança e privacidade

[1] 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.

1.1 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 ;

1.2 Análise de Impacto na Privacidade de Dados Pessoais

Realizar, em conjunto com a contratante, **análise de impacto na privacidade dos dados pessoais** 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;

1.3 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;

1.4 Arquitetura, Controles de Segurança 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 segurança da informação** e privacidade implementados em cada componente descrito na arquitetura física e lógica; e

c) **Matriz de responsabilidades** descrevendo a atribuição das responsabilidades pela segurança da informação na organização, pela privacidade (encarregado), identificação dos gestores de serviços com dados pessoais, operador(es) de tratamento de dados, relacionada ao objeto da contratação e com relação aos itens aqui descritos.

1.5 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;

1.6 Gestão de Incidentes

Possuir um processo de **Gestão de Incidentes** que registre os incidentes de segurança da informação e privacidade 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;

1.7 Coleta e preservação de evidências

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

1.8 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 segurança da informação e privacidade, 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;

1.9 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;

1.10 Desenvolvimento Seguro

Possuir e manter trilhas de qualidade e teste de software, e realizar **desenvolvimento seguro**, aderente ao disposto em dispositivo legal correlato publicado pelo GSI/PR;

1.10.1 Os dados pessoais utilizados em ambiente de TDH (teste, desenvolvimento e homologação) devem passar por um processo de **anonimização;**

1.10.2 A utilização dos dados pessoais em ambiente de TDH (teste, desenvolvimento e homologação), não anonimizados, deve **ser autorizada** pelo proprietário do ativo de informação;

1.10.3 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;

1.10.4 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;

1.10.5 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;

1.10.6 O Contratante e a Contratada realizarão a **análise de impacto** na proteção dos dados pessoais relacionada à Solução de TIC, devendo considerar as informações levantadas pelo relatório de impacto da Contratada.

1.11 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;

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

1.12 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.

2 REQUISITOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

A Equipe de Planejamento da Contratação deve estabelecer no que couber, ao definir os requisitos de segurança da informação e privacidade de que trata a alínea "i" do inciso II do caput do art. 16 da IN SGD/ME nº 1/2019, que a Solução de TIC deve possuir os seguintes itens em destaque na **Figura 4:**

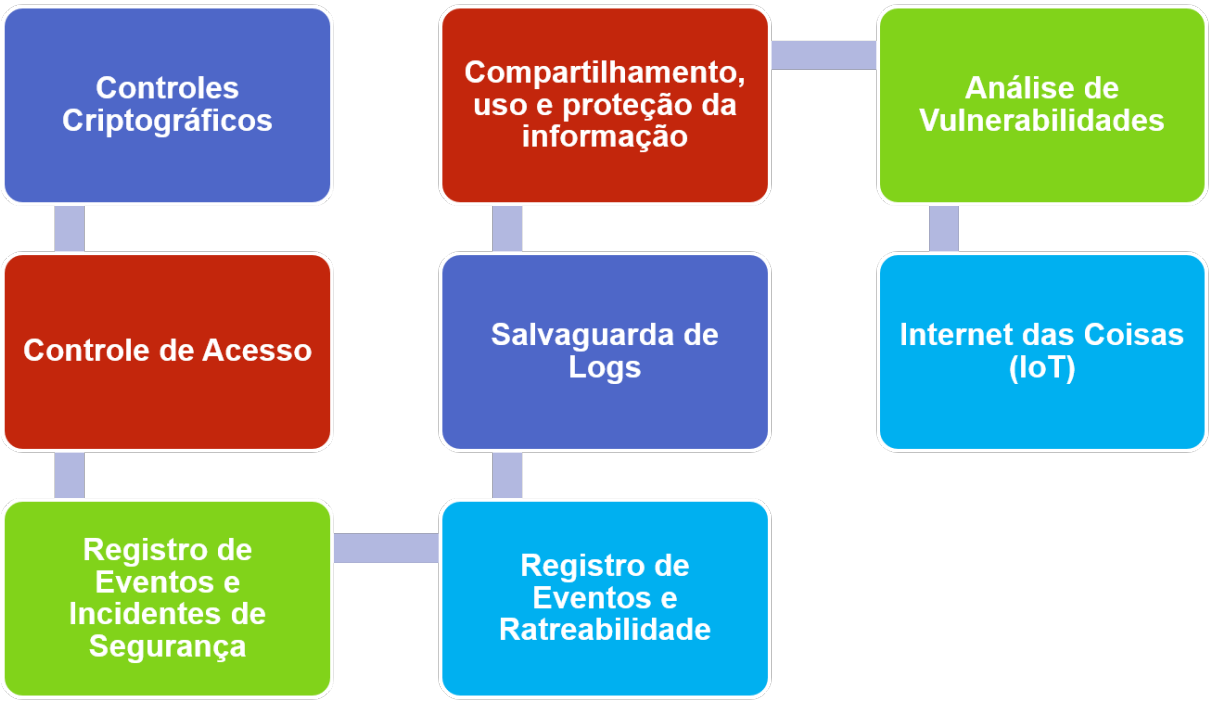

Figura 4 - Requisitos de Segurança da Informação e Privacidade

2.1 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.

2.2 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 segurança da informação e a privacidade, 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 à 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.

2.3 Registro de Eventos e Incidentes de Segurança

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

2.4 Registro de Eventos e Rastreabilidade

Implementar e manter controles específicos para **registro de eventos e rastreabilidade** de forma a manter trilha de auditoria de segurança da informação e privacidade, 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.

2.5 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.

2.6 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.

2.7 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.

2.8 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.

3 AÇÕES DE RESPONSABILIDADE DA CONTRATADA

Nas descrições abaixo e conforme **Figura 5**, destacam-se itens relativos às responsabilidades que devem ser imputadas, no que couber, à empresa Contratada.

Figura 5 - Ações de Responsabilidade da Contratada

3.1 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.

3.2 Reportar Incidentes

Reportar de imediato à contratante incidentes que envolvam vazamento de dados, indisponibilidade ou comprometimento da informação relacionados à Solução de TIC.

3.3 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.

3.4 Descarte Seguro

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

3.5 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.

3.6 Utilização de Serviços de 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.

3.7 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.

3.8 Ambientes Tecnológicos

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

3.9 Auditabilidade

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

3.10 Auditoria de segurança da informação e privacidade

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

3.11 Tratamento de incidentes de segurança da informação e privacidade

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

4 GESTÃO DO CONTRATO

Nas descrições abaixo e conforme **Figura 6**, destacam-se dispositivos que a Equipe de Planejamento da Contratação, ao elaborar o Modelo de Gestão do Contrato deve garantir que o contrato contenha.

Figura 6 – Gestão do Contrato

4.1 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.

4.2 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.

4.3 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.

4.4 Treinamento e concientização

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

4.5 Requisitos de 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.

4.6 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).

4.7 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.

4.8 Notificar violação

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

4.9 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.

4.10 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

4.11 Identificar operação

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

4.12 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.

4.13 Sanções administrativas

Dispositivo que estipule **sanções** administrativas pelo descumprimento de cada um dos requisitos de segurança da informação e de privacidade especificados.

No **Anexo A** deste guia são relacionadas as possíveis sanções que devem ser aplicadas em caso de descumprimento de cláusulas contratuais.

5 CONCLUSÃO

5.1 Importância e Relevância

Constata-se ser de extrema relevância a adoção de Requisitos de Segurança da Informação e Privacidade de Dados Pessoais bem como a respectiva gestão contratual com abordagem específica desse aspecto, quando da contratação de produtos e/ou serviços de TIC, pelos órgãos da administração pública.

5.2 Benefícios esperados

Espera-se, portanto, que o presente guia contribua para uma complementação e consolidação necessária ao estabelecimento de requisitos funcionais de produto e/ou serviços de TIC. Consideramos que tal ação representa um marco importante para o aprimoramento das ações contratuais que visam assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que serão tratadas neste tipo de aquisição no âmbito da administração pública.

5.3 Abrangência deste Guia

Este guia não pretende ser exaustivo em suas recomendações, ficando a cargo das equipes de planejamento de contratação, com os respectivos responsáveis pelas especificações operacionais e funcionais, a verificação de conformidade com os produtos e/ou serviços desejados. Dessa forma, espera-se mitigar as possibilidades de lacuna que vierem a existir para a segurança da informação e privacidade de dados pessoais da aquisição em processo de contratação.

5.4 Recomendações Finais

Conforme já citado anteriormente, é de suma importância a leitura das orientações contidas nos documentos referenciados no item Referências Bibliográficas deste guia, face procederem de órgão normativo e de relevância nas questões de padronização de metodologias e procedimentos.

Lembramos mais uma vez que este documento será atualizado e ampliado periodicamente com objetivo de mantê-lo alinhado às diretrizes e normativos vigentes.

ANEXO A

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
1.1	Não apresentar a POSIN - Política de Segurança da Informação.
1.2	Não apresentar o Relatório de Impacto à Proteção de Dados Pessoais – RIPD relacionado a solução de TIC.
1.3	Não apresentar o relatório de análise e avaliação de riscos de acordo com a periodicidade definida pela CONTRATANTE.
1.4	Não apresentar documentação, quando solicitada, que descreve a arquitetura física e lógica do objeto, controles de segurança da informação e matriz de responsabilidades
1.5	Não apresentar descrição dos controles de segurança da informação implementados em cada componente listado na arquitetura física e lógica.
1.5	Não apresentar Plano de Continuidade Operacional e Plano de Contingência.
1.6	Não apresentar documento que evidencie o processo formal de Gestão de Incidentes.
1.7	Não apresentar documento que evidencie os controles implementados para coleta e preservação de evidências de incidentes de segurança da informação e privacidade.
1.8	Não apresentar documento que evidencie o processo de Gestão de Mudanças.
1.9	Não apresentar documento que evidencie o processo de Gestão de Capacidade.

1.10	Não apresentar documentação que comprove estar em conformidade com desenvolvimento seguro presente em dispositivo legal correlato publicado pelo GSI/PR.
1.11	Não apresentar documentação que comprove estar em conformidade com nível adequado de segurança da informação às redes corporativas da Contratante e da Contratada.
1.12	Não apresentar documentação referente a política de backup.
2.1	Não apresentar documentação, referente aos controles criptográficos.
2.2	Não apresentar documento probatório que evidencie as políticas e controles de acesso.
2.3	Não apresentar documentos de comprovação de registros de eventos e incidentes.
2.4	Não apresentar documentos de comprovação de registros de eventos e rastreabilidade.
2.5	Não apresentar comprovação de salvaguarda de logs e registro das atividades de administradores e operadores.
2.6	Não apresentar documentos de comprovação de procedimentos e controles adequados para compartilhamento, uso e proteção da informação.
2.7	Não apresentar documentos de comprovação de procedimentos periódicos de análise de vulnerabilidades.
2.8	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.
3.1	Não apresentar documentação que evidencie a utilização de técnicas ou métodos apropriados de desenvolvimento seguro, com versões comprovadamente seguras e atualizadas.
3.2	Não apresentar documentação de reporte de incidentes.
3.3	Não apresentar Termos de Compromisso e Ciência.
3.4	Não apresentar documentação de que a Solução de TIC possui processamento que garante descarte seguro.
3.5	Não apresentar documentação de das providências de revogação de privilégios quando solicitado.

3.6	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.
3.7	Não apresentar documentos que comprovem procedimentos de segurança física e do ambiente.
3.8	Não apresentar documentos que asseguram que os ambientes tecnológicos de desenvolvimento, teste, homologação e produção estejam segregados
3.9	Não apresentar documentação que comprovem a implementação dos requisitos de segurança da informação e privacidade especificados na contratação.
3.10	Não disponibilizar recursos para auditoria de segurança da informação e privacidade relacionadas ao objeto do contrato.
3.11	Não realizar em conjunto com a contratante, ou com outros órgãos por ela indicados, ações de tratamento de incidentes de segurança da informação e privacidade relacionados ao objeto do contrato.
4.2	Não apresentar documentação que garanta política ou norma de proteção de dados pessoais que aborde a finalidade da contratada perante o processamento de dados.
4.3	Não apresentar o processo para controle de proteção de dados pessoais que devem ser monitorados e auditados.
4.4	Não apresentar o processo de treinamento e conscientização dos envolvidos no processamento e proteção dos dados.
4.5	Não apresentar documentação de monitoramento contínuo das ações de proteção de dados pessoais.
4.6	Não apresentar documentação que comprove que o tratamento de dados pessoais é realizado para o atendimento de sua finalidade pública.
4.7	Não apresentar documentação que comprove que o tratamento de dados está limitado ao mínimo necessário para atendimento da finalidade do tratamento.
4.8	Não notificar o Controlador em caso de ocorrência de violação de dados pessoais.
4.9	Não apresentar documentação que comprove que foram implementadas medidas que garantem e maximizam a precisão dos dados pessoais coletados.
4.10	Não apresentar documentação que comprove que os dados pessoais armazenados/retidos possuem controles de integridade.
4.11	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

4.12	Não apresentar documentação que define o canal de comunicação.

Referências Bibliográficas

ABNT NBR ISO/IEC 27001:2013. Tecnologia da Informação - Técnicas de Segurança

ABNT NBR ISO/IEC 27005:2011. Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

ABNT NBR ISO/IEC 27701:2019. Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001

ABNT NBR ISO/IEC 27002:2013 para gestão da privacidade da informação — Requisitos e diretrizes.

ABNT NBR ISO/IEC 29134:2017. Information technology – Security techniques – Guidelines for privacy impact assessment.

ABNT NBR ISO/IEC 29151:2017. Information technology – Security techniques – Code of practice for personally identifiable information protection.

ABNT NBR ISO/IEC 31000:2018. Gestão de riscos - Diretrizes.

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: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm >.

Acesso em: dezembro 2020.

COMITÊ CENTRAL DE GOVERNANÇA DE DADOS - CCGD. **Guia de Boas Práticas LGPD**. Abril 2020. Disponível em: < https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd >.

Acesso em: dezembro 2020.

LEGISLAÇÃO GSI/PR

Disponível em: < https://www.gov.br/gsi/pt-br/assuntos/dsi/legislacao >

Acesso em: dezembro 2020

PORTARIA Nº 93, DE 26 DE SETEMBRO DE 2019 - Glossário de Segurança da Informação

INSTRUÇÃO NORMATIVA Nº 4, DE 26 DE MARÇO DE 2020 - Segurança Cibernética em redes 5G

DECRETO Nº 10.222, DE 5 DE FEVEREIRO DE 2020 - Estratégia Nacional de Segurança Cibernética.