Guia de Avaliação de Riscos de Segurança e Privacidade

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Versão 1.0

Brasília, Novembro de 2020

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

Lei Geral de Proteção de Dados Pessoais

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
13/11/2020	1.0	Primeira versão do Guia de Avaliação de Riscos de Segurança e Privacidade.	Equipe Técnica de Elaboração

SUMÁRIO

INTRODUÇÃO

O objetivo deste Guia é fornecer aos responsáveis pelo tratamento de dados pessoais[1][2] no órgão ou entidade uma orientação para identificar lacunas de segurança da informação e de privacidade sobre os sistemas, contratos e processos da instituição.

O Guia foi construído a partir de uma experiência de pouco mais dois anos de análise de sistemas críticos, realizado na Secretaria de Governo Digital (SGD) da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia. As atividades inicialmente desempenhadas focaram na identificação de controles que elevassem a segurança da informação diante dos pilares de confidencialidade, integridade, disponibilidade e autenticidade no sistema a ser desenvolvido. À medida que o desenvolvimento avançava, houve a necessidade de realizar o monitoramento do sistema, e uma nova adição de controles para atender ao requisito foi realizada. Tal monitoramento implicou a associação com riscos de segurança. Caso os controles propostos não fossem implementados, consequentemente haveria um reflexo imediato na elevação dos níveis de riscos de segurança da informação para os riscos vinculados ao sistema crítico. Os novos controles introduzidos permitiam duas novas atividades: avaliar os controles estabelecidos no contrato, propondo revisões e adequações, e a avaliação do prestador de serviço sobre a abordagem de segurança da informação na estrutura organizacional interna. Ao fim, foi obtido um modelo de avaliação capaz de elevar a maturidade dos sistemas em segurança da informação.

Com a aproximação da entrada em vigor da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), realizou-se a adaptação do modelo de avaliação para atender a critérios de privacidade.

Ao longo do guia será discorrido sobre o embasamento teórico utilizado, organização dos temas segurança da informação e privacidade nos controles propostos e a avaliação dos riscos de segurança da informação e privacidade. Todas essas etapas não apenas servem como uma oportunidade de identificação de lacunas como também são insumos para a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), **detalhado** na seção 2.5 do Guia de Boas Práticas da LGPD (CCGD, 2020).

---

[1] Lei nº 13.709/2018, art. 5º, inciso X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

[2] Lei nº 13.709/2018, art. 5º, inciso I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

Importante reforçar que o tema deste guia - avaliação de riscos – é apenas uma das etapas do processo de gestão de riscos[3][4], conforme Figura 1, da norma ABNT NBR ISO/IEC 31000:2018. As demais etapas não são objeto de aprofundamento do documento.

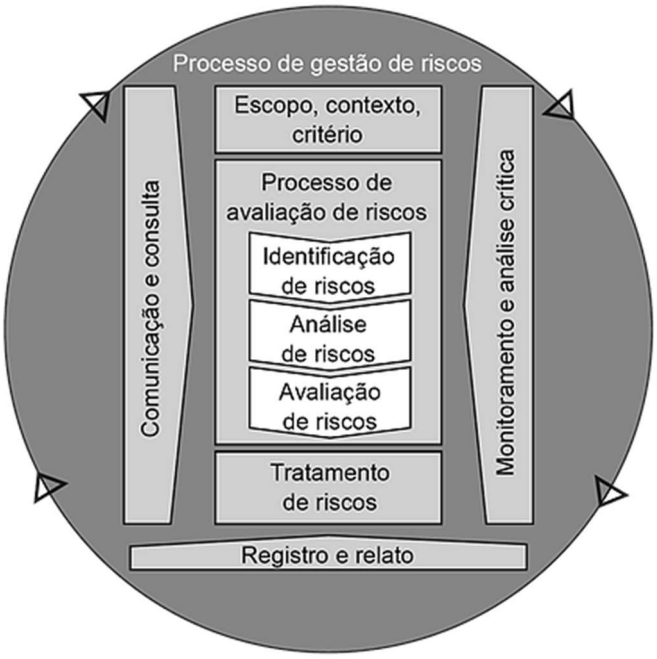

Figura 1. Processo de gestão de riscos (ABNT NBR ISO/IEC 31000:2018, seção 6)

O documento será atualizado à medida que novos ajustes forem necessários para acompanhar o amadurecimento dos processos de proteção e tratamentos de dados pessoais.

Ressalta-se que a instituição é livre para adequar todas as proposições deste guia a sua realidade.

[3] Gestão de Riscos - Atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos (ABNT NBR ISO/IEC 31000:2018).

[4] O processo de gestão de riscos envolve a aplicação sistemática de políticas, procedimentos e práticas para as atividades de comunicação e consulta, estabelecimento do contexto e avaliação, tratamento, monitoramento, análise crítica, registro e relato de riscos (ABNT NBR ISO/IEC 31000:2018).

1 - Guia de avaliação de riscos de segurança e privacidade

O Guia de avaliação de riscos de segurança e privacidade foi estruturado de modo a facilitar a reprodução e a adaptação do método proposto. As seções 1.1 a 1.4.2 versam sobre a organização e a seção 1.4.3 contempla o método definido para avaliação.

1.1 Dimensões

As dimensões agrupam os controles, de forma didática, em três contextos distintos: estrutura, sistema e privacidade.

Ao todo são 113 controles, ver Anexo I[5], distribuídos em 36 controles na dimensão Estrutura, 39 controles na dimensão Sistema e 38 controles na dimensão Privacidade. **Todas as dimensões tratam os temas segurança e privacidade**, mas dentro do contexto daquela dimensão, sendo a dimensão de privacidade direcionada especificamente à adequação legal à privacidade do tratamento de dados pessoais. Portanto, a organização por dimensão não vincula as medidas de segurança e privacidade (seção 1.2) a uma dimensão em particular, pois seu objetivo é relacioná-lo ao seu contexto do sistema, conforme pode ser observado nas próximas seções.

A seguir são apresentadas explicações sobre o que aborda cada dimensão do Anexo I.

1.1.1 Estrutura

Nesta dimensão são avaliados controles que tratam de aspectos estruturais do sistema (processos e infraestrutura que o sustentam), características de ambiente que expandem a análise, mas indispensável para identificar o estado atual da segurança e privacidade na organização responsável pelo tratamento de dados pessoais.

Exemplos de controles para Dimensão Estrutura:

Tabela 1. Exemplos de controles da Dimensão Estrutura (Anexo I).

Dimensão Estrutura	
ID	**Controle**
15	As mudanças são comunicadas para todas as partes interessadas?
16	Existe um prazo formalmente definido para o tratamento de vulnerabilidades técnicas relevantes identificadas?
18	Há um processo de análise e monitoramento de vulnerabilidades?

[5] O Anexo I, além de conter os 113 controles, foi organizado de modo que possa ser compartilhado entre vários setores da instituição na busca por respostas sobre a situação do(o) controle(s). Cada controle possui(em) referência(s) associada(s) que pode(m) ser checada(s) para melhor compreensão do tema.

1.1.2 Sistema

A dimensão Sistema tem alicerce no processo de *Security-by-Design*[6], ou seja, os controles de segurança propostos visam incorporar a segurança da informação durante todo o ciclo de vida do sistema, consequentemente auxiliam a redução da superfície de ataque para vulnerabilidades de sistema. A dimensão incluí temas como: desenvolvimento seguro, controles de acesso lógico, segurança web e outros.

É importante reforçar que a instituição é livre para alterar, incluir ou excluir os controles, adequando este documento à realidade e à criticidade do sistema. Há sistemas críticos que o duplo fator de autenticação[7] (ou o certificado digital) é de fundamental uso para elevar o nível de confiabilidade nas transações executadas no sistema, enquanto em outros casos com baixo risco (baixa probabilidade e baixo impacto) o seu uso pode ser dispensado. Portanto, identificar as lacunas e adaptar este documento à realidade do sistema é uma responsabilidade do controlador[8] e deve sempre estar relacionada à gestão de riscos institucional[9].

Exemplos de controles para Dimensão Sistema:

Tabela 2. Exemplos de controles da Dimensão Sistema (Anexo I).

Dimensão Sistema	
ID	**Controle**
48	O sistema em análise segue uma política de senha com definição de tamanho mínimo e formato?
55	O sistema implementa restrições/limitadores para sucessivas tentativas de acesso mal sucedidas?
66	É realizada análise estática e/ou análise dinâmica dos requisitos de segurança cibernética do sistema?

[6] *Security-by-Design* - é uma abordagem de desenvolvimento de software e hardware que visa minimizar as vulnerabilidades dos sistemas e reduzir a superfície de ataque em todas as fases do ciclo de vida de desenvolvimento de sistemas. Isso inclui a incorporação de especificações de segurança no projeto, avaliação de segurança contínua em cada fase e adesão às melhores práticas (Cyber Security Agency of Singapore, 2017).

[7] Um sistema de autenticação que requer mais de uma condição de autenticação distinta para realizar uma autenticação bem-sucedida (NIST, CSRC, Glossary, tradução nossa).

[8] Lei nº 13.709/2018, art. 5º, inciso VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

[9] Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016 - Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal.

1.1.3 Privacidade

Os controles de privacidade presentes nesta dimensão estão relacionados ao alcance da conformidade legal com à privacidade de tratamento de dados pessoais. Os controles permitirão que o controlador analise o sistema que trata dados pessoais e verifique se os requisitos de adequação à privacidade estão sendo atendidos.

O controle "Os dados coletados limitam-se ao mínimo necessário para atendimento da finalidade do tratamento?", por exemplo, motiva o controlador a revisitar as definições de negócio e averiguar se os dados coletados são excessivos ou não conforme o princípio de necessidade elencado no inciso III, art. 6º da LGPD: "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".

Exemplos de controles para Dimensão Privacidade:

Tabela 3. Exemplos de controles da Dimensão Privacidade (Anexo I).

Dimensão Privacidade	
ID	**Controle**
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?
81	A instituição 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?
105	No processamento de dados, é utilizado o mínimo necessário de dados pessoais para atingir a finalidade pretendida?

1.2 Medidas de Segurança e Privacidade

Esta seção descreve as medidas de segurança e privacidade e o objetivo dos controles presentes nelas. Ao todo são 23 medidas de segurança e privacidade divididas em 12 medidas de segurança e 11 medidas de privacidade. A divisão organiza os controles e facilita a compreensão do leitor. Ressalta-se que o avaliador pode adaptar os controles ou incluir novos controles para que a avaliação reflita a realidade do sistema.

As medidas utilizadas têm como referência as normas ABNT NBR ISO/IEC 27002:2013 (escopo de segurança da informação) e ISO/IEC 29100:2011 (escopo de privacidade).

Tabela 4. Exposição das medidas de segurança e os objetivos dos controles.

Medidas de Segurança (12)	**Descrição (Objetivo dos controles presentes na medida de segurança)**
Continuidade de Negócio	Manter a operação da atividade, apesar das adversidades enfrentadas.
Controles Criptográficos	Oferecer um meio seguro para as comunicações e armazenamento de registros (dados, informações e conhecimento).
Controles de Acesso Lógico	Limitar os acessos indevidos ao sistema.
Controles de Segurança em Redes, Proteção Física e do Ambiente	Evitar acessos indevidos às estruturas internas.
Cópia de Segurança	Realizar e manter cópias com temporariedade de execução e testes (simulações) de que os procedimentos adequados foram implantados e estão funcionais.
Desenvolvimento Seguro	Atender critérios de segurança da informação, desde a concepção do produto.
Gestão de Capacidade e Redundância	Manter a disponibilidade do serviço.
Gestão de Mudanças	Acompanhar as mudanças, comunicar aos interessados e identificar potenciais riscos.
Gestão de Riscos	Identificar, avaliar, gerenciar e monitorar os riscos identificados.
Registro de Eventos, Rastreabilidade e Salvaguarda de Logs	Registrar eventos com atributos de rastreabilidade e proteger de alteração e acessos indevidos.
Resposta a Incidente	Realizar a coleta, a preservação de evidências, o tratamento e a resposta à incidentes de segurança.
Segurança Web	Elevar os níveis de segurança (da camada de front-end[10]) nos serviços de acessos eletrônicos.

[10] Sítio eletrônico que é visto e utilizado diretamente pelo usuário (Cambridge Dictionary, tradução nossa).

Tabela 5. Exposição das medidas de privacidade e os objetivos dos controles.

Medidas de Privacidade (11)	**Descrição (Objetivo dos controles presentes na medida de privacidade)**
Abertura, Transparência e Notificação	Atender o princípio de transparência da LGPD (art. 6º, inciso VI[11]).
Compliance com a Privacidade	Atender a legislação de proteção de dados, monitorar e auditar a privacidade.
Consentimento e Escolha	Obter consentimento do titular (art. 7º, I), desde que não se enquadre nas demais hipóteses previstas pelo art. 7º e 11 da LGPD.
Controles de Acesso e Privacidade	Limitar acessos indevidos às operações de tratamento de dados pessoais (LGPD, art. 6º, Incisos VII[12] e VIII[13]).
Legitimidade e Especificação de Propósito	Realizar tratamento para propósitos legítimos, específicos, explícitos e informados ao titular (LGPD, art. 6º, I[14]).
Limitação da Coleta	Limitar a coleta ao mínimo necessário para a realização de suas finalidades (LGPD, art. 6º, III[15]).
Minimização dos Dados	Minimizar os dados utilizados no processamento (LGPD, art. 6º, III).
Participação Individual e Acesso	Assegurar que os direitos do titular dos dados pessoais são atendidos, a exemplo do livre acesso aos seus dados (LGPD, art. 6º, IV[16]).
Precisão e qualidade	Assegurar que os dados coletados são exatos e relevantes para o cumprimento da

[11] Lei nº 13.709/2018, art. 6º, Inciso VI - 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.

[12] Lei nº 13.709/2018, art. 6º, Inciso VII - 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.

[13] Lei nº 13.709/2018, art. 6º, Inciso VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

[14] Lei nº 13.709/2018, art. 6º, Inciso I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

[15] Lei nº 13.709/2018, art. 6º, Inciso III - 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.

[16] Lei nº 13.709/2018, art. 6º, Inciso IV - 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;

	finalidade do tratamento (LGPD, art. 6º, V[17]).
Responsabilização	Adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais (LGPD, art. 6º, X[18]).
Uso, Retenção e Limitação de Divulgação	Assegurar aos titulares os direitos fundamentais de liberdade, de intimidade e de privacidade nos termos da LGPD ao realizar o tratamento de dados pessoais.

1.3 Riscos

Os riscos elencados no RIPD (CCGD, 2020) foram influenciados e adaptados da norma ISO/IEC 29134:2017 que trata de técnicas de segurança para a avaliação de impacto à privacidade. Abaixo são descritos os 14 riscos utilizados na avaliação e seus respectivos escopos.

Tabela 6. Os 14 riscos propostos no guia de boas práticas da LGPD (CCGD, 2020) e o escopo de atuação.

ID	Riscos	Escopo do risco
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 (Ex.: perda do direito de acesso)	Garantia de atendimento dos direitos do titular, conforme descrito nos artigos 17 a 23 da LGPD. Art. 17. O titular dos dados pessoais tem direito a obter do controlador mediante requisição: I - confirmação da existência de tratamento;

[17] Lei nº 13.709/2018, art. 6º, Inciso V - 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;

[18] Lei nº 13.709/2018, art. 6º, Inciso X - 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.

		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; 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
5	Falha ou erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada etc.)	Dados de entrada que não são corretamente validados, operações de tratamento automatizadas de sistema que alteram de maneira indevida a composição do dado armazenado.
6	Informação insuficiente sobre a finalidade do tratamento	O tratamento de dados pessoais realizado de forma eletrônica ou documento em papel deve atender a uma finalidade e ser exposto de forma 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 reidentificados 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 da retenção dos dados pessoais para fins legais deve culminar com a

		exclusão e/ou descarte seguro(a) dos dados pessoais.
12	Roubo	Dados roubados nas dependências interna do controlador/operador[19], 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 esse requisito pode produzir informações com vinculações ou associações indevidas.

A título de esclarecimento, os riscos acima relacionados à disponibilidade são: perda, roubo e remoção. Caso ocorram, o titular de dados pode não conseguir acessar seus dados, por exemplo, e em consequência não exercer seus direitos. Dessa forma, caso os controles que mitiguem esses riscos não sejam implementados, haverá um impacto direto à disponibilidade.

1.4 Avaliação

A avaliação de riscos, conforme mencionada na seção introdutória, terá como base o modelo de Relatório de Impacto à Proteção de Dados Pessoais (RIPD) referenciado na seção 2.5 do Guia de Boas Práticas da LGPD (CCGD, 2020). As seções 1.4.1 e 1.4.2 retomam os principais conceitos tratados na seção 2.5 do Guia de Boas Práticas da LGPD de forma condensada, porém, não dispensa sua leitura para melhor compreensão e para mais detalhes sobre o tema.

A seção 1.4.3 detalha o método, pelas respostas atribuídas aos 113 controles propostos (aplicado, não aplicado e não se aplica), de avaliação do sistema. Ao final da seção, a partir da aplicação ou não dos controles propostos, o responsável pelo sistema

[19] Lei nº 13.709/2018, art. 5º, inciso VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

obtém o resultado da exposição aos riscos de segurança e privacidade aos quais o sistema está sujeito.

A validação do atendimento de um controle, identificação de aplicado, é de inteira responsabilidade do controlador na sua busca por respostas do operador.

Ressalta-se que a avaliação proposta neste documento não é um fim em si e sua adaptação contínua à realidade do sistema que trata dados pessoais é parte essencial do processo de avaliação. Leis, processos e culturas amadurecem constantemente e da mesma forma ocorre com o processo de avaliação de segurança da informação e da privacidade dos dados pessoais.

1.4.1 Avaliação de Riscos

Abaixo são resumidas as principais etapas do guia de boas práticas da LGPD para o tema avaliação de riscos.

A Tabela 7 exibe os parâmetros escalares, parâmetros que atribuem um valor gradual para cada uma das classificações (Baixo, Moderado e Alto). A Tabela 8, por sua vez, apresenta uma matriz que relaciona a probabilidade[20] (chance de algo acontecer) com o impacto[21] (resultado de um evento que afeta o objetivo). Ao multiplicar esses dois valores, obtém-se o nível de risco[22] (magnitude de um risco ou combinação de riscos).

Tabela 7. Parâmetros Escalares (CCGD, 2020).

CLASSIFICAÇÃO	VALOR
Baixo	5
Moderado	10
Alto	15

[20] Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente; ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).
[21] Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).
[22] Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

Tabela 8. Matriz de Probabilidade X Impacto (CCGD, 2020).

Probabilidade (P)			
15	75	150	225
10	50	100	150
5	25	50	75
	5	10	15
	Impacto (I)		

Tabela 9. Legenda de cores (CCGD, 2020).

Legenda (Cor)	Classificação do nível de risco
Verde	Baixo
Amarelo	Moderado
Vermelho	Alto

1.4.2 Fluxo das saídas

A avaliação descrita neste guia servirá de entrada e complemento a duas etapas do RIPD: identificar e avaliar os riscos, e identificar medidas para tratar os riscos. Elas estão descritas nas seções 2.5.2.6 e 2.5.2.7 do Guia de Boas Práticas da LGPD (CCGD, 2020).

A primeira etapa (identificar e avaliar os riscos), ou primeira avaliação, refletirá uma análise do cenário atual (diagnóstico) do sistema que trata dados pessoais, conforme exemplificado pela Tabela 10. Nela são apresentados os riscos e o nível de riscos diante da avaliação sobre os 113 controles selecionados.

A segunda etapa (identificar medidas para tratar os riscos), ou segunda avaliação, representa o tratamento efetivamente aplicado aos riscos por meio da implementação de controles, após a primeira avaliação. Ela contribui com as medidas complementares a serem definidas para o tratamento dos riscos. A Tabela 11 ilustra as medidas adotadas para prevenir ou mitigar o risco. Segundo o Guia de Boas Práticas da LGPD (CCGD, 2020), ao invés do preenchimento das medidas de segurança e privacidade, o campo de medidas poderia conter os controles aplicados e elevar o nível de detalhamento durante a documentação.

Tabela 10. Riscos e níveis de riscos referente ao tratamento de dados pessoais (CCGD, 2020).

ID	RISCO REFERENTE AO TRATAMENTO DE DADOS PESSOAIS	P	I	NÍVEL DE RISCO (P X I)
R01	Acesso não autorizado.	10	15	**150**
R02	Modificação não autorizada.	10	15	**150**
R03	Perda	5	15	**75**
R04	Roubo	5	15	**75**
R05	Remoção não autorizada.	5	15	**75**
R06	Coleção excessiva.	10	10	**100**
R07	Informação insuficiente sobre a finalidade do tratamento.	10	15	**150**
R08	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	10	15	**150**
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	5	15	**75**
R10	Compartilhar ou distribuir dados pessoais com terceiros fora da administração pública federal sem o consentimento do titular dos dados pessoais.	10	15	**150**
R11	Retenção prolongada de dados pessoais sem necessidade.	10	5	**50**
R12	Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	**75**
R13	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.).	5	15	**75**
R14	Reidentificação de dados pseudonimizados.	5	15	**75**

Legenda: P – Probabilidade; I – Impacto.

Tabela 11. Exemplos de medidas para lidar com os riscos (CCGD, 2020).

RISCO	MEDIDA(S)	EFEITO SOBRE RISCO	RISCO RESIDUAL			MEDIDA(S) APROVADA(S)
			P	I	(P X I)	
R01 Acesso não autorizado.	1. Controle de acesso Lógico. 2. Desenvolvimento seguro. 3. Segurança em Redes.	Reduzir	5	10	**50**	Sim

Legenda: P – Probabilidade; I – Impacto.

Além de fornecer informações para as duas etapas do RIPD citadas acima, outras informações desta avaliação permitem identificar necessidades de adequação em contratos com operadores de dados, medidas de segurança para expor no termo de uso e política de privacidade (princípio da transparência[23]), melhorar a segurança da informação e a privacidade de processos internos na instituição, bem como buscar a conformidade com a LGPD.

Figura 2. Benefícios da Avaliação de Riscos

1.4.3 Método

O método proposto neste documento parte de 4 premissas fundamentais para compreensão da estruturação do modelo de avaliação, são elas:

1. O sistema a ser avaliado inicia com nível de risco Alto (probabilidade Alta e impacto Alto), visto que os controles ainda não foram analisados para o sistema.
2. Os controles foram divididos e agrupados em características comuns e totalizam 113 controles (Anexo I deste documento). Esse agrupamento é chamado de medidas de segurança e privacidade. Ao todo são 23 medidas, 12 de segurança e 11 de privacidade.
    a. A tabela abaixo exibe as medidas de segurança e privacidade e a quantidade de controles que cada medida possui:

[23] Lei nº 13.709/2018, art. 6º, inciso VI - 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.

Tabela 12. Medidas de segurança e privacidade com total de controles

Medidas de Segurança e Privacidade (23)	Total de Controles (113)
Abertura, Transparência e Notificação	5
Compliance com a Privacidade	10
Consentimento e Escolha	1
Continuidade de Negócio	3
Controles Criptográficos	2
Controles de Acesso Lógico	10
Controle de Acesso e Privacidade	4
Controles de Segurança em Redes, Proteção Física e do Ambiente	5
Cópia de Segurança	8
Desenvolvimento Seguro	9
Gestão de Capacidade e Redundância	2
Gestão de Mudanças	5
Gestão de Riscos	5
Legitimidade e Especificação de Propósito	4
Limitação de Coleta	2
Minimização de Dados	2
Participação Individual e Acesso	2
Precisão e qualidade	2
Registro de Eventos, Rastreabilidade e Salvaguarda de Logs	7
Responsabilização	5
Resposta a Incidente	8
Segurança Web	9
Uso, Retenção e Limitação de Divulgação	3

3. Cada controle pode atuar de maneira diferente em relação a um determinado risco: 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.
4. O método estabelece pesos para os controles que representam um grau de importância em relação ao risco. A Tabela 13 expõe os pesos utilizados.

Tabela 13. Descrição dos pesos utilizados.

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

Em resumo, os controles agem mitigando e/ou prevenindo determinados riscos e, de acordo com sua importância (pesos), poderão reduzir mais ou menos a probabilidade (controles preventivos) e impacto (controles de mitigação). Para os controles que não se aplicam ao sistema avaliado, não há efeito na probabilidade ou no impacto dos riscos. Os anexos II.A, II.B e II.C exemplificam o modelo.

Para calcular o total de controles que atuam na probabilidade e impacto, soma-se os controles de prevenção (probabilidade) e os controles de mitigação (impacto). Por fim, controles de prevenção e mitigação são somados simultaneamente no grupo de prevenção e no grupo de mitigação. A Tabela 14 exemplifica a distribuição dos controles com base no risco de acesso não autorizado.

Tabela 14. Exemplificando a distribuição dos controles de prevenção e mitigação

Risco	Total de Controles	Total de Controles de Prevenção	Total de Controles de Mitigação	Total de Controles de Prevenção e Mitigação	Total de Controles que atuam na Probabilidade	Total de Controles que atuam no Impacto
Acesso não autorizado	20	8	7	5	(8+5) 13	(7+5) 12

Além da totalização dos tipos de controles, são contabilizados todos os controles aplicados, não aplicados e os que não se aplicam para cada um dos 14 riscos. Essa contabilização ocorre por meio da soma dos pesos vinculados aos controles para aquele risco específico.

As fórmulas abaixo buscam medir, a partir da entrada das respostas atribuídas aos controles (aplicado, não aplicado e não se aplica), o nível de risco (relação entre probabilidade e impacto, seção 1.4.1) para os riscos aos quais o sistema está exposto.

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. Posteriormente, realiza-se a subtração entre a soma de todos os pesos dos controles de prevenção do risco e a soma de todos os pesos dos controles de prevenção que "não se aplica" ao risco. Ao final, divide-se o primeiro pelo segundo. 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 daquele risco. A fórmula de cálculo para o impacto segue o mesmo raciocínio e difere apenas no tipo de controle avaliado (controles de mitigação).

Fórmulas de probabilidade e impacto

Cálculo da Probabilidade

- **Probabilidade** = Total de Pesos dos **Controles de Prevenção Aplicados** ao Risco / (Total de Pesos dos **Controles de Prevenção Associados** ao Risco – Total de Pesos dos **Controles de Prevenção Que Não se Aplica** ao Risco)

Cálculo do Impacto

- **Impacto** = Total de Pesos dos **Controles de Mitigação Aplicados** ao Risco / (Total de Pesos dos **Controles de Mitigação Associados** ao Risco – Total de Pesos dos **Controles de Mitigação Que Não se Aplica** ao Risco)

Antes da realização do cálculo do nível de risco (Tabela 8) é necessário adequar o resultado obtido com a probabilidade e o impacto, valor entre 0 e 1, em uma das classificações (Alta, Moderada e Baixa). A Tabela 15 é inspirada nos níveis de capacidade da seção 6.4.2 do Cobit 2019 e cria uma gradação dos níveis de classificação.

Tabela 15. Controles implementados X classificação

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

À medida que os controles são implementados, a classificação da probabilidade ou do impacto é reduzida. O impacto tem apenas duas classificações ao invés de três, pois leva em consideração a possibilidade de existência de peculiaridades do ambiente, tipos de dados pessoais tratados e legislações específicas aplicadas ao tratamento de dados. Dessa forma, optou-se por um único degrau de redução (de Alto para Moderado). Salienta-se novamente que o avaliador pode adaptar o método à realidade da instituição e pode inserir mais categorias ou mudar o método de acordo com seu critério.

A seguir, descreve-se o método de avaliação por meio de um exemplo simplificado dos controles. A Tabela 16 apresenta a matriz de riscos, os pesos e os tipos de controles que orientarão a obtenção do nível de risco para o sistema que trata dados pessoais.

As matrizes reais com todos os riscos, pesos e tipos de controles podem ser visualizados nos anexos II.A, II.B e II.C deste documento.

Tabela 16. Representação dos controles vinculados aos riscos, pesos e tipos

Risco	Controle 1	Controle 2	Controle 3	Controle 4	Controle 5	Controle 6	Controle 7	Controle 8	Controle 9	Controle 10
Acesso não autorizado	1			0,5	0,5		1	0,5		0,5
Coleção excessiva	1	1			1			1	1	

Tabela 17. Legenda Tipo de Controle

Tipo do controle
Mitigação
Prevenção
Mitigação e Prevenção
Controle não ativo

Exemplo de avaliação de riscos de segurança e privacidade:

Sistema XPTO

A tabela abaixo exibe as respostas para o sistema XPTO.

Análise	Controle 1	Controle 2	Controle 3	Controle 4	Controle 5	Controle 6	Controle 7	Controle 8	Controle 9	Controle 10
Resposta	Aplicado	Não Aplicado	Não se Aplica	Aplicado	Não Aplicado	Não se Aplica	Aplicado	Não Aplicado	Não se Aplica	Aplicado

Legenda	
Aplicado	Controle implementado
Não Aplicado	Controle não implementado
Não se Aplica	Controle não necessário para o sistema

As respostas são analisadas para cada risco individualmente, devido ao peso que o controle tem e a maneira que ele se comporta com o risco (prevenção ou mitigação, ou prevenção e mitigação).

Risco	Controle 1	Controle 2	Controle 3	Controle 4	Controle 5	Controle 6	Controle 7	Controle 8	Controle 9	Controle 10
Acesso não autorizado	Aplicado (1)	Não Aplicado	Não se Aplica	Aplicado (0,5)	Não Aplicado (0.5)	Não se Aplica	Aplicado (1)	Não Aplicado (0,5)	Não se Aplica	Aplicado (0,5)
Coleção excessiva	Aplicado (1)	Não Aplicado (1)	Não se Aplica	Aplicado	Não Aplicado (1)	Não se Aplica	Aplicado	Não Aplicado (1)	Não se Aplica (1)	Aplicado

Abaixo são contabilizados os pesos dos controles dentro de suas subdivisões:

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
Acesso não autorizado	3,5	2	2,5	1,5	0	0
Coleção excessiva	4	3	1	1	1	0

Aplicação das fórmulas:

- **Probabilidade** = Total de Pesos dos **Controles de Prevenção Aplicados** ao Risco / (Total de Pesos dos **Controles de Prevenção Associados** ao Risco – Total de Pesos dos **Controles de Prevenção Que Não se Aplica** ao Risco)

- **Impacto** = Total de Pesos dos **Controles de Mitigação Aplicados** ao Risco / (Total de Pesos dos **Controles de Mitigação Associados** ao Risco – Total de Pesos dos **Controles de Mitigação Que Não se Aplica** ao Risco)

1. Acesso não autorizado

   Probabilidade = 2,5 / (3,5 - 0) = 2,5 / 3,5 = 0,71

   Impacto = 1,5 / (2 - 0) = 1,5 / 2 = 0,75

2. Coleção excessiva

   Probabilidade = 1 / (4 - 1) = 1 / 3 = 0,33

   Impacto = 1 / (3 - 0) = 1 / 3 = 0,33

Resultado da avaliação:

Risco	Probabilidade (%)	Impacto (%)	Nível de risco
Acesso não autorizado	Moderada (71%)	Alto (75%)	Alto (150)
Coleção excessiva	Alta (33%)	Alto (33%)	Alto (225)

Para finalizar, destaca-se novamente que a avaliação de riscos é apenas uma das etapas de um processo de gestão de riscos que deve ser realizado na sua completude e acompanhado do amadurecimento dos controles definidos.

2 – FERRAMENTA PARA AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

2.1 Detalhes da ferramenta

A Secretaria de Governo Digital (SGD) está desenvolvendo uma ferramenta que materializa em formato eletrônico a automatização do método de avaliação deste documento. Os controles do Anexo I encontram-se em formato de questionário e a avaliação deve ser executada para cada sistema individualizado.

Após a avaliação do sistema é exibido para o usuário o nível de risco que ele está exposto. Os 14 riscos avaliados estão presentes na seção 2.5 do Guia de Boas Práticas da LGPD (CCGD, 2020).

Para ter acesso ao questionário entre em contato com o endereço eletrônico: cgsin@economia.gov.br. Na solicitação de acesso identifique-se com o seu nome, a instituição que pertence e o e-mail institucional para que o token de acesso à ferramenta possa ser encaminhado.

Apesar da ferramenta gerar uma avaliação de riscos do sistema analisado, reforça-se que cada sistema pode requerer controles de segurança e privacidade específicos que não podem ser abordados completamente por uma ferramenta única. Portanto, a avaliação de riscos de segurança e privacidade gerada a partir da ferramenta não prescindem da análise das equipes técnicas e do encarregado responsável, pois o sistema pode necessitar de controles específicos que não foram tratados pela ferramenta.

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 27005:2019**: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação. Rio de Janeiro, 2019.

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: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm >. Acesso em: 21 out. 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: 04 set. 2020.

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: < http://dsic.planalto.gov.br/assuntos/editoria-c/documentos-pdf-1/instrucao-normativa-no-1-de-27-de-maio-de-2020-1.pdf >. Acesso em: 24 out. 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: 26 out. 2020.

CYBER SECURITY AGENCY OF SINGAPORE (CSA). **Security-by-Design Framework Versão 1.0**. Singapura, 2017. Disponível em: < https://www.csa.gov.sg/-/media/csa/documents/legislation_supplementary_references/security_by_design_framework.pdf >. Acesso em: 26 out. 2020.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. ISACA **COBIT 2019** Framework: Introduction and Methodology. Schaumburg, 2018.

INTERNATIONAL STANDARD. **ISO/IEC 29100:2011**: Information technology — Security techniques — Privacy framework. Genebra, 2011.

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.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NIST Special Publication 800-53 revisão 5**: Security and Privacy Controls for Information Systems and Organizations. Gaithersburg, 2020.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST - Computer Security Resource Center – Glossary. Disponível em: < https://csrc.nist.gov/glossary >. Acesso em: 05 nov. 2020.

OPEN WEB APPLICATION SECURITY PROJECT. **OWASP Cheat Sheet Series**. Disponível em: < https://cheatsheetseries.owasp.org/index.html >. Acesso em: 23 out. 2020.

OPEN WEB APPLICATION SECURITY PROJECT. **OWASP Web Security Testing Guide versão 4.1**. Disponível em: < https://owasp.org/www-project-web-security-testing-guide/ >. Acesso em: 23 out. 2020.

Anexo I - Controles

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

Avaliação de Riscos de Segurança e Privacidade

CHECKLIST – *<Setor Responsável pelo levantamento>*

Orientações: Anexar evidências dos itens respondidos como **SIM (controle aplicado)**. Definir prazos e encaminhamentos para a implementação dos itens respondidos como **NÃO (controle não aplicado)**. Justificar os itens respondidos como **N/A** (não aplicável).

Plataforma: ***<Plataforma>***

Responsável pelo preenchimento:

ID	Dimensão Estrutura	Medida de Segurança e Privacidade	Resposta			Evidências / Prazos / Encaminhamentos	Referências
			Sim	Não	N/A		
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					Referências: NC nº 03/IN01/DSIC/GSIPR (item 5.3.7) e ABNT NBR ISO/IEC 27002:2013 (item 6.1.1)
2	Há **mecanismos para monitoramento** do uso dos recursos, de forma a atender as necessidades de capacidade futura e garantir o desempenho requerido das aplicações?	Gestão de Capacidade e Redundância					Referências: NC nº 10/IN01/DSIC/GSIPR (item 5.3.2) e ABNT NBR ISO/IEC 27002:2013 (12.1.3)
3	São implementados **mecanismos e procedimentos para mitigar ataques de negação de serviço**, tais como balanceamento de carga, proxy, firewall, etc.?	Continuidade de Negócio					Referências: NC nº 08/IN01/DSIC/GSIPR (Item 7.2) e ABNT NBR ISO/IEC 27002:2013 (13.1.2)

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

ID	Dimensão Estrutura	Medida de Segurança e Privacidade	Resposta			Evidências / Prazos / Encaminhamentos	Referências
			Sim	Não	N/A		
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					Referências: NC nº 06/IN01/DSIC/GSIPR e ABNT NBR ISO/IEC 27002:2013 (item 17.1)
5	A **Política de Segurança da Informação** já foi revisada para se adequar a medidas que objetivem a proteção de dados pessoais?	*Compliance* com Privacidade					Referências: ABNT NBR ISO/IEC 27701:2019 (item 6.2) (diretrizes adicionais para a implementação do controle 5.1.1, Políticas para segurança da informação, da ABNT NBR ISO/IEC 27002:2013)
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					Referências: ABNT NBR ISO/IEC 27701:2019 (item 6.5.2) (diretrizes adicionais para a implementação do controle 8.2.1, Classificação da informação, da ABNT NBR ISO/IEC 27002:2013)
7	O **local que processa as informações** é restrito somente ao pessoal autorizado?	Controles de Segurança em Redes, Proteção Física e do Ambiente					Referências: NC nº 10/IN01/DSIC/GSIPR (item 5.5.2) e ABNT NBR ISO/IEC 27002:2013 (item 11.1)

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

ID	Dimensão Estrutura	Medida de Segurança e Privacidade	Resposta			Evidências / Prazos / Encaminhamentos	Referências
			Sim	Não	N/A		
8	O trabalho nas **áreas seguras** é supervisionado?	Controles de Segurança em Redes, Proteção Física e do Ambiente					Referências: NC nº 07/IN01/DSIC/GSIPR (item 7) e ABNT NBR ISO/IEC 27002:2013 (item 11.1.2)
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					Referência: 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)
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					Referência: 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)

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

ID	Dimensão Estrutura	Medida de Segurança e Privacidade	Resposta			Evidências / Prazos / Encaminhamentos	Referências
			Sim	Não	N/A		
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					Referência: ABNT ISO/IEC 27002:2013 (item 14.2.4)
12	É realizado o **controle de mudanças em atualizações** de software e outros componentes das soluções de TIC?	Gestão de Mudanças					Referências: NC nº 13/IN01/DSIC/GSIPR (item 6) e ABNT NBR ISO/IEC 27002:2013 (item 14.2.2)
13	Mudanças são **planejadas e testadas**?	Gestão de Mudanças					Referências: NC nº 13/IN01/DSIC/GSIPR (item 6.3) e ABNT NBR ISO/IEC 27002:2013 (item 14.2.2)
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					Referências: NC nº 04/IN01/DSIC/GSIPR (6.2) e ABNT NBR ISO/IEC 27002:2013 (item 14.2.2)
15	As **mudanças são comunicadas** para todas as partes interessadas?	Gestão de Mudanças					Referências: NC nº 13/IN01/DSIC/GSIPR (item 6.3) e ABNT NBR ISO/IEC 27002:2013 (item 14.2.2)

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

ID	Dimensão Estrutura	Medida de Segurança e Privacidade	Resposta			Evidências / Prazos / Encaminhamentos	Referências
			Sim	Não	N/A		
16	Existe um **prazo** formalmente definido para o tratamento de vulnerabilidades técnicas relevantes identificadas?	Gestão de Mudanças					Referências: NC nº 04/IN01/DSIC/GSIPR (item 6.3.2) e ABNT NBR ISO/IEC 27002:2013 (item 12.6.1)
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?	Gestão de Riscos					Referências: NC nº 10/IN01/DSIC/GSIPR, ABNT NBR ISO/IEC 27002:2013 (item 12.6.1), ABNT NBR ISO/IEC 27701:2019 (item 7.2.8) e ISO/IEC 29151:2017 (item 8.1.2)
18	Há um **processo de análise e monitoramento** de vulnerabilidades?	Gestão de Riscos					Referências: NC nº 04/IN01/DSIC/GSIPR (item 6.6.2) e ABNT NBR ISO/IEC 27002:2013 (item 12.6.1)
19	Existe uma **equipe de detecção, tratamento e resposta a incidentes** de segurança cibernética (CSIRT)?	Resposta a Incidente					Referências: 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)

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

ID	Dimensão Estrutura	Medida de Segurança e Privacidade	Resposta			Evidências / Prazos / Encaminhamentos	Referências
			Sim	Não	N/A		
20	Existe um **canal apropriado para notificar os incidentes** de segurança da informação de forma rápida?	Resposta a Incidente					Referências: 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)
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					Referências: 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)
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					Referências: 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)
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					Referências: 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)

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

ID	Dimensão Estrutura	Medida de Segurança e Privacidade	Resposta			Evidências / Prazos / Encaminhamentos	Referências
			Sim	Não	N/A		
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					Referências: ABNT NBR ISO/IEC 27002:2013 (item 16.1) e ABNT NBR ISO/IEC 27701:2019 (item 6.13.1.5)
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					Referências: NC nº 21/IN01/DSIC/GSIPR (item 7) e ABNT NBR ISO/IEC 27002:2013 (item 16.1)
26	Os arquivos coletados como evidências são gravados em conjunto com o **arquivo com a lista dos resumos criptográficos**?	Resposta a Incidente					Referências: NC nº 21/IN01/DSIC/GSIPR (item 7) e ABNT NBR ISO/IEC 27002:2013 (item 16.1)
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					Referências: ABNT NBR ISO/IEC 27002:2013 (item 12.3)

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

ID	Dimensão Estrutura	Medida de Segurança e Privacidade	Resposta			Evidências / Prazos / Encaminhamentos	Referências
			Sim	Não	N/A		
28	Está estabelecida a **abrangência dos procedimentos de backup** para cada tipo de informação (por exemplo, completa ou diferencial)?	Cópia de Segurança					Referências: ABNT NBR ISO/IEC 27002:2013 (item 12.3) e ABNT NBR ISO/IEC 27701:2019 (item 6.9.3)
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					Referências: ABNT NBR ISO/IEC 27002:2013 (item 12.3) e ABNT NBR ISO/IEC 27701:2019 (item 6.9.3)
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?	Cópia de Segurança					Referências: ABNT NBR ISO/IEC 27002:2013 (item 12.3) e ABNT NBR ISO/IEC 27701:2019 (item 6.9.3)
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					Referências: ABNT NBR ISO/IEC 27002:2013 (item 12.3) e ABNT NBR ISO/IEC 27701:2019 (item 6.9.3)
32	É **exigida autorização** prévia da autoridade competente para liberação das credenciais de acesso para o gerenciamento dos sistemas que suportam o serviço?	Controles de Acesso Lógico					Referências: NC nº 07/IN01/DSIC/GSIPR e ABNT NBR ISO/IEC 27002:2013 (item 9.1.1)

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

ID	Dimensão Estrutura	Medida de Segurança e Privacidade	Resposta			Evidências / Prazos / Encaminhamentos	Referências
			Sim	Não	N/A		
33	Existe e é executado um **processo formal de desenvolvimento** de sistema seguro?	Desenvolvimento Seguro					Referências: NC nº 16/IN01/DSIC/GSIPR e ABNT NBR ISO/IEC 27002:2013 (item 14.2.1)
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					Referências: NC nº 16/IN01/DSIC/GSIPR e ABNT NBR ISO/IEC 27002:2013 (itens 12.1.4 e 14.2.1)
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					Referência: ABNT NBR ISO/IEC 27002:2013 (item 14.2.7)
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					Referências: NC nº 07/IN01/DSIC/GSIPR e ABNT NBR ISO/IEC 27002:2013 (item 14.2.6)

Informações adicionais:

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

ID	Dimensão Sistema	Medida de Segurança e Privacidade	Resposta			Evidências / Prazos / Encaminhamentos	Referências
			Sim	Não	N/A		
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					Referências: NC nº 04/IN01/DSIC/GSIPR e ABNT NBR ISO/IEC 27005:2019
38	Os recursos de segurança da informação e de tecnologia da informação encontram-se em **versões seguras, estáveis e atualizadas**?	Gestão de Riscos					Referência: ABNT NBR ISO/IEC 27002:2013 (item 12.6.1)
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					Referência: ABNT NBR ISO/IEC 27002:2013 (item 14.2)
40	Há **redundância dos recursos** de processamento da informação suficiente para atender aos requisitos de disponibilidade previstos em contrato?	Gestão de Capacidade e Redundância					Referência: ABNT NBR ISO/IEC 27002:2013 (item 12.1.3)
41	Foi elaborada uma **política de privacidade** para o serviço?	*Compliance* com a privacidade					Referências: ABNT NBR ISO/IEC 27701:2019 (item 6.2.1.1) e ISO/IEC 29151:2017 (A2)
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 a privacidade					Referências: Lei nº 13.709/2018, art. 10, Parágrafo 3º, Guia de Boas Práticas LGPD, seção 2.5 (CCGD, 2020) e ISO/IEC 29134:2017

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

ID	Dimensão Sistema	Medida de Segurança e Privacidade	Resposta			Evidências / Prazos / Encaminhamentos	Referências
			Sim	Não	N/A		
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					Referências: ABNT NBR ISO/IEC 27701:2019 (item 7.2.8)
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					Referências: NC nº 06/IN01/DSIC/GSIPR e ABNT NBR ISO/IEC 22301
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					Referências: 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)
46	Existe uma **frequência** estabelecida para geração dos backups?	Cópia de Segurança					Referências: ABNT NBR ISO/IEC 27002:2013 (item 12.3) e ABNT NBR ISO/IEC 27701:2019 (item 6.9.3)

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

ID	Dimensão Sistema	Medida de Segurança e Privacidade	Resposta			Evidências / Prazos / Encaminhamentos	Referências
			Sim	Não	N/A		
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					Referências: NC nº 21/IN01/DSIC/GSIPR e ABNT NBR ISO/IEC 27002:2013 (item 12.4.2)
48	O sistema em análise segue uma **política de senha** com definição de tamanho mínimo e formato?	Controles de Acesso Lógico					Referências: 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)
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					Referências: NC nº 07/IN01/DSIC/GSIPR, ABNT NBR ISO/IEC 27002:2013 (item 9)

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

ID	Dimensão Sistema	Medida de Segurança e Privacidade	Resposta			Evidências / Prazos / Encaminhamentos	Referências
			Sim	Não	N/A		
50	As informações das credenciais de acesso dos usuários são **transmitidas de forma protegida**?	Controles de Acesso Lógico					Referências: NC nº 07/IN01/DSIC/GSIPR, ABNT NBR ISO/IEC 27002:2013 (item 9)
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					Referência: ABNT NBR ISO/IEC 27002:2013 (item 9)
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?	Controles de Acesso Lógico					Referência: ABNT NBR ISO/IEC 27002:2013 (item 9.2.5)
53	Há mecanismos para encerramento (expirar) de qualquer sessão cuja **inatividade do usuário** exceda um período de tempo predeterminado?	Controles de Acesso Lógico					Referências: 16/IN01/DSIC/GSIPR (item 4.2) e ABNT NBR ISO/IEC 27002:2013 (itens 9.2.5 e 9.4.2)
54	Existem restrições de autenticação do usuário para **acesso simultâneo** a serviço(s), sistema(s) e/ou rede(s)?	Controles de Acesso Lógico					Referência: OWASP - Session Management Cheat Sheet
55	O sistema implementa restrições/limitadores para sucessivas tentativas de **acesso mal sucedidas**?	Controles de Acesso Lógico					Referência: ABNT NBR ISO/IEC 27002:2013 (item 9.4.2)

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

ID	Dimensão Sistema	Medida de Segurança e Privacidade	Resposta			Evidências / Prazos / Encaminhamentos	Referências
			Sim	Não	N/A		
56	As credenciais de acesso e logs são **armazenadas separadamente** dos dados das aplicações e dos sistemas?	Controles de Acesso Lógico					Referência: ABNT NBR ISO/IEC 27002:2013 (item 9.4.3)
57	O log registra **identificação do usuário**, incluindo administrador e acessos privilegiados?	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)
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)
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)
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)

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

ID	Dimensão Sistema	Medida de Segurança e Privacidade	Resposta			Evidências / Prazos / Encaminhamentos	Referências
			Sim	Não	N/A		
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)
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)
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)
64	Existem **controles de versão** para garantir a gestão dos códigos-fonte?	Desenvolvimento Seguro					Referências: NC nº 16/IN01/DSIC/GSIPR e ABNT NBR ISO/IEC 27002:2013 (item 14.2.1)
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)

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

ID	Dimensão Sistema	Medida de Segurança e Privacidade	Resposta			Evidências / Prazos / Encaminhamentos	Referências
			Sim	Não	N/A		
66	É realizada **análise estática e/ou análise dinâmica** dos requisitos de segurança cibernética do sistema?	Desenvolvimento Seguro					Referências: NC nº 16/IN01/DSIC/GSIPR (item 5) e ABNT NBR ISO/IEC 27002:2013 (itens 14.2.8 e 14.2.9)
67	O servidor da aplicação fornece opções de **protocolos criptográficos** para conexão em versões seguras, estáveis e atualizadas?	Segurança Web					Referência: ABNT NBR ISO/IEC 27002:2013 (item 10.1.2)
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)
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)
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)

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

ID	Dimensão Sistema	Medida de Segurança e Privacidade	Resposta			Evidências / Prazos / Encaminhamentos	Referências
			Sim	Não	N/A		
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)
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)
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)
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)
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)

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

ID	Dimensão Privacidade	Medida de Segurança e Privacidade	Resposta			Evidências / Prazos / Encaminhamentos	Referências
			Sim	Não	N/A		
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)
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)
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))?	Controles de Acesso e Privacidade					Referência: ISO/IEC 29151:2017 (item 9.2.3)
79	A instituição 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)
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)
81	A instituição 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)
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)

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

ID	Dimensão Privacidade	Medida de Segurança e Privacidade	Resposta			Evidências / Prazos / Encaminhamentos	Referências
			Sim	Não	N/A		
83	O compartilhamento ou transferência de dados pessoais é realizado por meio de um canal criptografado e de cifra recomendada pelos sítios especializados de segurança (Exemplo: https://www.ssllabs.com/ssltest/)?	Controles criptográficos					Referência: ISO/IEC 29151:2017 (item 13.2.2)
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)
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)

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

ID	Dimensão Privacidade	Medida de Segurança e Privacidade	Resposta			Evidências / Prazos / Encaminhamentos	Referências
			Sim	Não	N/A		
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)
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)
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)
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)
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)

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

ID	Dimensão Privacidade	Medida de Segurança e Privacidade	Resposta			Evidências / Prazos / Encaminhamentos	Referências
			Sim	Não	N/A		
91	Há uma política ou norma de proteção de dados pessoais que aborde a finalidade da instituição 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)
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)
93	É implementada e mantida uma estratégia abrangente de treinamento e conscientização, destinada a garantir que os envolvidos entendam suas responsabilidades e os procedimentos de proteção de dados pessoais?	*Compliance* com a Privacidade					Referência: ISO/IEC 29151:2017 (item A.11.5)
94	A instituição 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)

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

ID	Dimensão Privacidade	Medida de Segurança e Privacidade	Resposta			Evidências / Prazos / Encaminhamentos	Referências
			Sim	Não	N/A		
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)
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)
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)
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)
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)
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?	Abertura, Transparência e Notificação					Referência: ISO/IEC 29151:2017 (item A.4.2)

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

ID	Dimensão Privacidade	Medida de Segurança e Privacidade	Resposta			Evidências / Prazos / Encaminhamentos	Referências
			Sim	Não	N/A		
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)
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)
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)
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)

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

ID	Dimensão Privacidade	Medida de Segurança e Privacidade	Resposta			Evidências / Prazos / Encaminhamentos	Referências
			Sim	Não	N/A		
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)
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)
107	A instituição 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)
108	A instituição 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)
109	A instituição 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)
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)
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)

GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE

ID	Dimensão Privacidade	Medida de Segurança e Privacidade	Resposta			Evidências / Prazos / Encaminhamentos	Referências
			Sim	Não	N/A		
112	A instituição 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)
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 instituição?	Participação Individual e Acesso					Referência: ISO/IEC 29151:2017 (item A.10.3)

Anexo II.A – Dimensão Estrutura - Matriz de Pesos e tipos de controles por risco

Legenda	
Controle	Prevenção
Risco[24]	Mitigação
Controle não ativo para o Risco	Prevenção e Mitigação

ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1	1			0,5	0,5		1	1	1	1	0,5	0,5	0,5	1	0,5	1	1	1	1	1	1	1	1	1	1	0,5	0,5	0,5	0,5	0,5		1	1	1	1	1
2	1				0,5							1	1	1	1		0,5																			
3	1				0,5							0,5	1	1	1																					1
4	1			1	0,5	0,5	0,5	0,5				0,5	0,5	0,5	0,5		0,5										0,5	0,5	0,5	0,5	0,5		0,5			
5	1	0,5	0,5		0,5	0,5						1	1	1	1												0,5	1	1		0,5					
6	1				0,5							0,5	0,5	1	0,5		0,5																			
7	1			1	0,5		0,5	0,5	1	1	1	0,5	1	1	0,5	1	1	1	1	1	1	1	1	1	1	0,5	1	0,5	1	0,5		1	1	1	1	0,5
8	1	1	1	1	0,5		0,5	0,5	1	0,5	1	0,5	1	1	0,5	1	1	1	1	1	1	1	1	1	1	0,5	1	0,5	1	0,5	1	1	1	1	1	0,5
9	1				1							0,5	0,5	1	1																					
10	1			1	0,5		1	1	1	1	0,5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0,5	1	0,5	1	0,5		1	1	1	1	1
11	1				1							0,5	0,5	0,5	0,5		1										1	0,5			1						
12	1			1	0,5		1	1	1	1	0,5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0,5	1	0,5	1	0,5	1	1	1	1	1	1
13	1				0,5	1						0,5	0,5	1	1																					1
14	1				0,5	1						0,5	0,5	1	1																					1

[24] Ver Tabela 3 para identificar o risco tratado em cada linha.

Anexo II.B – Dimensão Sistema - Matriz de Pesos e tipos de controles por risco

ID	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
1	1	1	1			1	0,5	0,5	1	0,5	0,5	1	1	1	1	1	1	1	1	0,5	0,5	0,5	1	0,5	0,5	0,5	1	0,5	0,5	1	1	0,5	0,5	1	0,5	0,5	1	1	0,5
2					0,5	1	1																																
3						1	1																																
4				1	1	0,5	1	0,5		0,5			1	1	1		1	0,5											0,5	0,5	1	1	1	1	0,5	0,5	1	1	0,5
5						1	0,5			1																													
6					0,5	1	0,5																																
7	1	1	1			1	0,5	0,5	0,5	0,5	1	1	0,5	1	1	1	1	1	1		1	1	1	1	1	1	1	0,5	1	1	1	1	1	1	0,5	1	1	1	0,5
8	1	1	1	1		1	0,5	1	1	1	1	1	1	1	1	1	1	1	1	0,5	0,5	0,5	0,5	0,5	0,5	0,5	1	0,5	0,5	1	1	1	1	1	0,5	1	1	1	0,5
9						1	1		1																														
10	1	1	1			1	0,5	1	1	1	1	1	1	1	1	1	1	1	1		1	0,5	1	1	1	1	1	0,5	1	1	1	1	1	1	0,5	1	1	1	0,5
11					0,5	1	1																																
12	1	1	1			1	0,5	1	1	1	1	1	1	1	1	1	1	1	1	0,5	1	0,5	1	1	1	1	1	0,5	1	1	1	1	1	1	0,5	1	1	1	0,5
13					1	1	1										0,5	0,5			0,5	0,5	1	0,5															
14					0,5	1	1										0,5	0,5			0,5	0,5	1	0,5															

Anexo II.C - Dimensão Privacidade - Matriz de Pesos e tipos de controles por risco

ID	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113
1	1	1	1	1	1			1		0,5	1		1	1	0,5	0,5	0,5	0,5	0,5			0,5										1				0,5		
2											1		1	1	1	0,5	1	0,5	1		1	0,5	1	1	0,5				0,5	0,5								
3										1	1	1	1	1	1	0,5	1	0,5	0,5			1					1											
4						0,5				0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5		0,5	0,5			0,5	0,5	0,5		1				1				1	1
5											0,5		1	1	0,5	0,5	1	0,5	0,5			0,5						0,5					1	1				
6											0,5		0,5	0,5	0,5	0,5	0,5	0,5	0,5			0,5			1			1	1									
7	1	1	1	1				1		1	0,5		1	1	0,5	0,5	1	0,5	0,5			1										1			1	1		
8	1	1	1	1				1		0,5	0,5		1	1	0,5	0,5	1	0,5	0,5			1										1				1		
9						1					1		1	1	0,5	1	1	0,5	0,5			1										1						
10	1	1	1	1				1		1	1		1	1	0,5	0,5	1	0,5	0,5			1										1				1		
11											1		0,5	0,5	1	1	1	0,5	0,5			1			1				1									
12	1	1	1	1	1	1		1		1	1		1	1	0,5	0,5	1	0,5	0,5			1									1	1				1		
13									1	1	1		1	1	1	1	0,5	0,5	0,5	1		1			1				1							1		
14	1	1			1	1	1		1		1		1	1	1	1	0,5	0,5	0,5		1	1	1	1	0,5				0,5	1	1	1				1		