

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

“Expedir Certidão de Movimentos Migratórios”

Brasília, 31 de agosto de 2023

POLÍCIA FEDERAL

Histórico de Revisões

Data	Versão	Descrição	Autor
13/12/2021	1.0	Conclusão da primeira versão do relatório	AADM Yara Aquino
20/12/2021	2.0	Revisão do relatório após análise do controlador, operador e encarregado.	DPF André Zaca Furquim
31/08/2023	3.0	Revisão do relatório após análise do controlador, operador e encarregado.	DPF Caio Bortone Ramos Ribeiro

POLÍCIA FEDERAL

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - RIPD

OBJETIVO

O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Referência: Art. 5º, XVII da Lei 13.709/2018 (LGPD).

1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador

Polícia Federal

Operador

Polícia Federal

Encarregado

DPF Rinaldo de Souza

E-mail Encarregado

dpa@pf.gov.br

Telefone Encarregado

2024-8527

2 – NECESSIDADE DE ELABORAR O RELATÓRIO

- 2.1. Tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais (LGPD, art. 4º, § 3º).

3 – DESCRIÇÃO DO TRATAMENTO

Processo: Expedir Certidão de Movimentos Migratórios.

3.1 – NATUREZA DO TRATAMENTO

3.1.1. Descrição do fluxo do tratamento dos dados pessoais:

1 - O interessado (brasileiro, estrangeiro ou imigrante) procura uma das unidades da Polícia Federal e solicita a emissão de certidão de movimentos migratórios, na qual são reproduzidos os registros de movimentos de entrada e saída mantidos no banco de dados do Sistema de Tráfego Internacional - STI;

2 - O pedido é realizado com a apresentação de documento que identifique o interessado, demonstra ser titular dos dados buscados ou que detém poder para buscar dados de terceiros, oportunidade em que poderão ser apresentados outros documentos de identificação com o

POLÍCIA FEDERAL

intuito de comprovar vínculos familiares.

3.1.2. Fonte de dados utilizada para obtenção dos dados pessoais: Documento de identificação do requerente da certidão e, eventualmente, de outros documentos que identificam os titulares dos dados buscados por terceiros.

3.1.3. Não são compartilhados dados pessoais com outras Instituições.

3.1.4. O operador que realiza o tratamento de dados pessoais é a Polícia Federal, na fase de Coleta.

3.1.5. As medidas de segurança atualmente adotadas são: Política de Segurança; Gestão de Riscos; Segurança nas Operações; Organização da Segurança; Classificação da Informação; Proteção Física e do Ambiente; Gestão de Mudanças; Continuidade de Negócio; Tratamento e Resposta a Incidentes; Controles de Coleta e Preservação de Evidências; Controles Criptográficos; Cópia de Segurança; Controle de Acesso Lógico; Registro de Eventos e Rastreabilidade; Compartilhamento, Uso e Proteção da Informação; Desenvolvimento Seguro; Segurança em Redes.

3.2 – ESCOPO DO TRATAMENTO

3.2.1. Os dados pessoais tratados pelo processo abrangem:

- Informações de identificação pessoal: Nome, tipo de documento, número do documento, classificação migratória, sexo, data de nascimento, nacionalidade e foto do documento de viagem.

- Informações de identificação atribuídas por instituições governamentais: Documento de identificação.

- Detalhes pessoais: Sexo, data de nascimento e nacionalidade.

- Situação de Imigração: Classificação migratória em cada movimento de entrada e saída consignado na certidão.

- Viagens e deslocamentos: Data de entrada e saída do Brasil.

- Outros: Endereço eletrônico.

3.2.2. A quantidade de dados pessoais tratados é de aproximadamente 10 dados pessoais e 0 dados sensíveis. A frequência de tratamento dos dados pessoais é: A emissão de certidão é realizada após comparecimento do interessado em unidade da PF em horário de expediente.

3.2.3. O processo não realiza retenção de dados.

3.2.4. O número de titulares afetados pelo tratamento de dados é variável, podendo atingir números da escala nacional e até mesmo internacional.

3.2.5. A abrangência da área geográfica do tratamento dos dados é Nacional.

3.3 – CONTEXTO DO TRATAMENTO

A Polícia Federal é responsável pelo recebimento dos pedidos de certidão de movimento migratório realizados pelos interessados ou seus procuradores.

Os dados pessoais são obtidos a partir dos documentos pessoais de viagem apresentados pelos indivíduos. De forma secundária, se necessário, poderão ser obtidos dados adicionais a partir de registros próprios do órgão.

POLÍCIA FEDERAL

O procedimento é o mesmo no caso de crianças, adolescentes e quaisquer outros grupos, representados ou assistidos pelos responsáveis.

O tipo de tratamento realizado sobre os dados é condizente com a expectativa dos titulares dos dados pessoais, uma vez que o dado pessoal não é tratado de maneira diversa do que é determinado em leis e regulamentos, e comunicado pela instituição ao titular de dados.

Pode ser detectado como “avanço relevante da instituição em tecnologia ou segurança que contribui para a proteção dos dados pessoais” a facilitação da obtenção de certidão de movimentos migratórios por meio não presencial, desde que exista prévio registro de endereço de e-mail pessoal do interessado junto à Polícia Federal. Neste caso, a resposta é encaminhada exclusivamente para o e-mail previamente cadastrado.

3.4 – FINALIDADE DO TRATAMENTO

3.4.1. Garantir que os dados pessoais (registros de entrada e saída do Brasil) sejam fornecidos somente a seus titulares ou a quem de direito.

3.4.2. Os resultados pretendidos para o titular de dados são: Ter acesso a seu histórico migratório e utilizar a certidão para fazer prova de suas entradas e saídas do Brasil.

3.4.3. Os benefícios esperados para o órgão, entidade ou para a sociedade como um todo são: Fornecimento de dados mantidos pela Administração Pública quando necessário a seu titular.

4 – PARTES INTERESSADAS CONSULTADAS

As partes interessadas consultadas foram os próprios Gestores e Chefes das áreas do referido Processo/Serviço, além de seus respectivos Diretores.

Importante relatar que o registro das opiniões dos gestores não será informado, pois poderia comprometer segredo organizacional e fragilizaria a segurança da informação, além do que poderia violar um dos princípios expressos da Constituição Federal de 1988, tal qual, o da Eficiência.

5 – NECESSIDADE E PROPORCIONALIDADE

5.1 – FUNDAMENTAÇÃO LEGAL

5.1.1. A hipótese legal para tratamento de dados pessoais é o art. 4º, inciso III, alíneas a) e d) da LGPD.

5.1.2. A necessidade do tratamento de dados desse processo é respaldada pela previsão legal constante no Artigo 144, §1º da Constituição Federal, Código de Processo Penal, Lei nº. 12.850/2013 Lei nº. 12.830/2013.

5.2 – QUALIDADE E MINIMIZAÇÃO DOS DADOS

O tratamento de dados pessoais realizado pela PF é condizente e proporcional às finalidades dos dados coletados e armazenados em todas as suas atividades, limitando-se ao estritamente necessário para a efetiva realização das atribuições legais desse órgão. Por isso são adotados controles físicos e lógicos, bem como medidas administrativas e processos para proteger os dados pessoais de acessos não autorizados ou da sua utilização ilegal, com a identificação e pronta

POLÍCIA FEDERAL

responsabilização dos servidores e demais colaboradores que por ventura venham a fazer mau uso das informações às quais têm acesso para exercício de seu mister. Há registro de logs dos usuários e de atividades de todos os tratamentos de dados realizados, que ficam armazenados por prazo mínimo de 5 (cinco) anos. Ademais, qualquer tratamento de dados é fundamentado em determinado processo administrativo, evitando que acessos não autorizados aconteçam, bem como garantindo que o tratamento dos dados será o mínimo necessário, ao permitir um controle das ações do agente.

5.3 – MEDIDAS PARA ASSEGURAR CONFORMIDADE DO OPERADOR

razão da necessária restrição de acesso às informações pessoais, impostas pelo direito fundamental à intimidade e à vida privada, bem como pelas novas legislações que reforçam a necessidade de dados pessoais sensíveis, o acesso às informações armazenadas e tratadas nos sistemas da Polícia Federal somente é autorizado a servidores Policiais Federais, mediante confirmação da autorização pela chefia imediata, pelas áreas gestoras e assinatura de termos que reforçam o compromisso funcional de manutenção de sigilo das informações, nos quais seja declarada a ciência inequívoca da legislação sobre o tratamento de informações pessoais de terceiros, cuja divulgação possa causar dano a intimidade, vida privada, honra e imagem das pessoas, assim como de informações sigilosas, cuja divulgação possa causar risco ou dano à segurança da sociedade ou do Estado, por força do disposto no art. 61 do Decreto nº 7.724/2012, que regulamenta a Lei nº 12.527/2011. Ademais, as ações da Polícia Federal ainda se submetem a regra do art. 20 do Código de Processo Penal que determina que a Autoridade Policial tome todas as medidas de salvaguarda para garantir o sigilo necessário ao inquérito policial.

5.4 – MEDIDAS PARA ASSEGURAR DIREITOS DO TITULAR DOS DADOS

O Sistema Eletrônico do Serviço de Informação ao Cidadão (e-SIC) e a Ouvidoria da Polícia Federal (Plataforma Fala.BR) são disponibilizados para que os titulares dos dados pessoais possam demandar as solicitações diretamente à Polícia Federal. Ressalta-se que o tratamento previsto no presente RIPD se enquadra na exceção prevista no art. 4º, inciso III, alíneas a) e d) da LGPD. Ademais, a ANPD poderá solicitar a qualquer momento o RIPD à Polícia Federal, bem como emitir opiniões técnicas ou recomendações sobre o presente tratamento de dados. (Art. 4º, § 3º da LGPD).

A Polícia Federal está a todo momento submetida ao Controle Externo do Ministério Público, nos termos do art. 129 da Constituição Federal. O exercício de tal controle permite ao MP a requisição de quaisquer informações sobre o exercício da atividade policial, além de livre acesso às dependências da PF. Ainda como consequência dessa previsão constitucional e nos termos do Código de Processo Penal, investigações conduzidas pela PF são encaminhadas ao Poder Judiciário e ao Ministério Público no prazo máximo de 30 dias após o seu início, devendo ainda retornar a esses órgãos para o exercício do controle em prazo por eles definidos.

Além do controle externo realizado pelo MP e pelo Judiciário, nos autos da investigação criminal, existe o controle interno da Corregedoria da Polícia Federal, presente em todas as unidades da federação, que submete as investigações da Polícia Federal a uma auditoria interna, toda vez que ocorre a remessa de uma investigação ao Judiciário e ao MP. Ainda, nos termos da Súmula Vinculante 14, do STF, qualquer investigado e/ou seu advogado tem acesso integral aos autos da investigação, de modo que o próprio titular do direito possa exercer, diretamente ou por intermédio de seu procurador, o regular exercício do controle da atividade policial no tocante a ele.

POLÍCIA FEDERAL

Ainda a respeito do controle interno e externo, a Corregedoria da Polícia Federal, além da regular auditoria já mencionada, exerce poder disciplinar e de investigação administrativa e criminal caso seja identificada qualquer violação das normas anteriormente descritas por qualquer servidor da Polícia Federal.

5.5 – SALVAGUARDAS PARA AS TRANSFERÊNCIAS INTERNACIONAIS DE DADOS

5.5.1. Este Processo não realiza qualquer tipo de transferência internacional de dados.

6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Id	Risco referente ao tratamento de dados pessoais	P	I	Nível de Risco (P x I)
R01	Acesso não autorizado.	10	10	100
R02	Modificação não autorizada.	5	10	50
R03	Perda.	5	15	75
R04	Roubo.	5	15	75
R05	Remoção não autorizada.	5	15	75
R06	Coleção excessiva.	5	10	50
R07	Informação insuficiente sobre a finalidade do tratamento.	5	10	50
R08	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	5	15	75
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 sem o consentimento do titular dos dados pessoais.	10	15	150
R11	Retenção prolongada de dados pessoais sem necessidade.	5	10	50
R12	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	75
R13	Falha/erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com dado equivocado, ausência de validação dos dados de entrada, etc.).	5	5	25
R14	Reidentificação de dados pseudonimizados.	5	5	25

POLÍCIA FEDERAL

7 – MEDIDAS PARA TRATAR OS RISCOS

Risco	Medida(s)	Efeito sobre o Risco ¹	Risco Residual ²			Medida(s) ³ Aprovada(s)
			P	I	Nível (P x I)	
Acesso não autorizado.	1 - Política de Segurança;	Reduzir	5	10	50	Sim
	2 - Gestão de Riscos;					
	3 - Segurança nas Operações;					
	4 - Organização da Segurança;					
	5 - Classificação da Informação;					
	6 - Proteção Física e do Ambiente;					
	7 - Gestão de Mudanças;					
	8 - Continuidade de Negócio;					
	9 - Tratamento e Resposta a Incidentes;					
	10 - Controles de Coleta e Preservação de Evidências;					
	11 - Controles Criptográficos;					
	12 - Cópia de Segurança;					
	13 - Controle de Acesso Lógico;					
	14 - Registro de Eventos e Rastreabilidade;					
	15 - Compartilhamento, Uso e Proteção da Informação;					
	16 - Desenvolvimento Seguro;					
	17 - Segurança em redes;					
Modificação não autorizada.	1 - Política de Segurança;	Aceitar	5	10	50	Sim
	2 - Gestão de Riscos;					
	3 - Segurança nas Operações;					
	4 - Organização da					

POLÍCIA FEDERAL

	Segurança; 5 - Classificação da Informação; 6 - Proteção Física e do Ambiente; 7 - Gestão de Mudanças; 8 - Continuidade de Negócio; 9 - Tratamento e Resposta a Incidentes; 10 - Controles de Coleta e Preservação de Evidências; 11 - Controles Criptográficos; 12 - Cópia de Segurança; 13 - Controle de Acesso Lógico; 14 - Registro de Eventos e Rastreabilidade; 15 - Compartilhamento, Uso e Proteção da Informação; 16 - Desenvolvimento Seguro; 17 - Segurança em redes;					
Perda.	1 - Política de Segurança; 2 - Gestão de Riscos; 3 - Segurança nas Operações; 4 - Organização da Segurança; 5 - Classificação da Informação; 6 - Proteção Física e do Ambiente; 7 - Gestão de Mudanças; 8 - Continuidade de Negócio; 9 - Tratamento e Resposta a Incidentes; 10 - Controles de Coleta e Preservação de Evidências; 11 - Controles Criptográficos; 12 - Cópia de Segurança;	Reduzir	5	10	50	Sim

POLÍCIA FEDERAL

	13 - Controle de Acesso Lógico; 14 - Registro de Eventos e Rastreabilidade; 15 - Compartilhamento, Uso e Proteção da Informação; 16 - Desenvolvimento Seguro; 17 - Segurança em redes;					
Roubo.	1 - Política de Segurança; 2 - Gestão de Riscos; 3 - Segurança nas Operações; 4 - Organização da Segurança; 5 - Classificação da Informação; 6 - Proteção Física e do Ambiente; 7 - Gestão de Mudanças; 8 - Continuidade de Negócio; 9 - Tratamento e Resposta a Incidentes; 10 - Controles de Coleta e Preservação de Evidências; 11 - Controles Criptográficos; 12 - Cópia de Segurança; 13 - Controle de Acesso Lógico; 14 - Registro de Eventos e Rastreabilidade; 15 - Compartilhamento, Uso e Proteção da Informação; 16 - Desenvolvimento Seguro; 17 - Segurança em redes;	Reduzir	5	10	50	Sim
Remoção não autorizada.	1 - Política de Segurança; 2 - Gestão de Riscos; 3 - Segurança nas Operações;	Reduzir	5	10	50	Sim

POLÍCIA FEDERAL

	4 - Organização da Segurança; 5 - Classificação da Informação; 6 - Proteção Física e do Ambiente; 7 - Gestão de Mudanças; 8 - Continuidade de Negócio; 9 - Tratamento e Resposta a Incidentes; 10 - Controles de Coleta e Preservação de Evidências; 11 - Controles Criptográficos; 12 - Cópia de Segurança; 13 - Controle de Acesso Lógico; 14 - Registro de Eventos e Rastreabilidade; 15 - Compartilhamento, Uso e Proteção da Informação; 16 - Desenvolvimento Seguro; 17 - Segurança em redes;					
Coleção excessiva.	1 - Política de Segurança; 2 - Gestão de Riscos; 3 - Segurança nas Operações; 4 - Organização da Segurança; 5 - Classificação da Informação; 6 - Proteção Física e do Ambiente; 7 - Gestão de Mudanças; 8 - Continuidade de Negócio; 9 - Tratamento e Resposta a Incidentes; 10 - Controles de Coleta e Preservação de Evidências; 11 - Controles Criptográficos;	Aceitar	5	10	50	Sim

POLÍCIA FEDERAL

	12 - Cópia de Segurança; 13 - Controle de Acesso Lógico; 14 - Registro de Eventos e Rastreabilidade; 15 - Compartilhamento, Uso e Proteção da Informação; 16 - Desenvolvimento Seguro; 17 - Segurança em redes;					
Informação insuficiente sobre a finalidade do tratamento.	1 - Política de Segurança; 2 - Gestão de Riscos; 3 - Segurança nas Operações; 4 - Organização da Segurança; 5 - Classificação da Informação; 6 - Proteção Física e do Ambiente; 7 - Gestão de Mudanças; 8 - Continuidade de Negócio; 9 - Tratamento e Resposta a Incidentes; 10 - Controles de Coleta e Preservação de Evidências; 11 - Controles Criptográficos; 12 - Cópia de Segurança; 13 - Controle de Acesso Lógico; 14 - Registro de Eventos e Rastreabilidade; 15 - Compartilhamento, Uso e Proteção da Informação; 16 - Desenvolvimento Seguro; 17 - Segurança em redes;	Aceitar	5	10	50	Sim
Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja	1 - Política de Segurança; 2 - Gestão de Riscos; 3 - Segurança nas Operações;	Reduzir	5	10	50	Sim

POLÍCIA FEDERAL

previsto em legislação ou regulação pertinente).	4 - Organização da Segurança;					
	5 - Classificação da Informação;					
	6 - Proteção Física e do Ambiente;					
	7 - Gestão de Mudanças;					
	8 - Continuidade de Negócio;					
	9 - Tratamento e Resposta a Incidentes;					
	10 - Controles de Coleta e Preservação de Evidências;					
	11 - Controles Criptográficos;					
	12 - Cópia de Segurança;					
	13 - Controle de Acesso Lógico;					
	14 - Registro de Eventos e Rastreabilidade;					
	15 - Compartilhamento, Uso e Proteção da Informação;					
	16 - Desenvolvimento Seguro;					
	17 - Segurança em redes;					
Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	1 - Política de Segurança;	Reduzir	5	10	50	Sim
	2 - Gestão de Riscos;					
	3 - Segurança nas Operações;					
	4 - Organização da Segurança;					
	5 - Classificação da Informação;					
	6 - Proteção Física e do Ambiente;					
	7 - Gestão de Mudanças;					
	8 - Continuidade de Negócio;					
	9 - Tratamento e Resposta a Incidentes;					
	10 - Controles de Coleta e Preservação de Evidências;					
	11 - Controles Criptográficos;					

POLÍCIA FEDERAL

	12 - Cópia de Segurança; 13 - Controle de Acesso Lógico; 14 - Registro de Eventos e Rastreabilidade; 15 - Compartilhamento, Uso e Proteção da Informação; 16 - Desenvolvimento Seguro; 17 - Segurança em redes;					
Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	1 - Política de Segurança; 2 - Gestão de Riscos; 3 - Segurança nas Operações; 4 - Organização da Segurança; 5 - Classificação da Informação; 6 - Proteção Física e do Ambiente; 7 - Gestão de Mudanças; 8 - Continuidade de Negócio; 9 - Tratamento e Resposta a Incidentes; 10 - Controles de Coleta e Preservação de Evidências; 11 - Controles Criptográficos; 12 - Cópia de Segurança; 13 - Controle de Acesso Lógico; 14 - Registro de Eventos e Rastreabilidade; 15 - Compartilhamento, Uso e Proteção da Informação; 16 - Desenvolvimento Seguro; 17 - Segurança em redes;	Reduzir	5	10	50	Sim
Retenção prolongada de dados pessoais sem necessidade.	1 - Política de Segurança; 2 - Gestão de Riscos; 3 - Segurança nas Operações;	Reduzir	5	5	25	Sim

POLÍCIA FEDERAL

	4 - Organização da Segurança; 5 - Classificação da Informação; 6 - Proteção Física e do Ambiente; 7 - Gestão de Mudanças; 8 - Continuidade de Negócio; 9 - Tratamento e Resposta a Incidentes; 10 - Controles de Coleta e Preservação de Evidências; 11 - Controles Criptográficos; 12 - Cópia de Segurança; 13 - Controle de Acesso Lógico; 14 - Registro de Eventos e Rastreabilidade; 15 - Compartilhamento, Uso e Proteção da Informação; 16 - Desenvolvimento Seguro; 17 - Segurança em redes;					
Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	1 - Política de Segurança; 2 - Gestão de Riscos; 3 - Segurança nas Operações; 4 - Organização da Segurança; 5 - Classificação da Informação; 6 - Proteção Física e do Ambiente; 7 - Gestão de Mudanças; 8 - Continuidade de Negócio; 9 - Tratamento e Resposta a Incidentes; 10 - Controles de Coleta e Preservação de Evidências; 11 - Controles Criptográficos;	Reduzir	5	10	50	Sim

POLÍCIA FEDERAL

	12 - Cópia de Segurança; 13 - Controle de Acesso Lógico; 14 - Registro de Eventos e Rastreabilidade; 15 - Compartilhamento, Uso e Proteção da Informação; 16 - Desenvolvimento Seguro; 17 - Segurança em redes;					
Falha/erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com dado equivocado, ausência de validação dos dados de entrada, etc.).	1 - Política de Segurança; 2 - Gestão de Riscos; 3 - Segurança nas Operações; 4 - Organização da Segurança; 5 - Classificação da Informação; 6 - Proteção Física e do Ambiente; 7 - Gestão de Mudanças; 8 - Continuidade de Negócio; 9 - Tratamento e Resposta a Incidentes; 10 - Controles de Coleta e Preservação de Evidências; 11 - Controles Criptográficos; 12 - Cópia de Segurança; 13 - Controle de Acesso Lógico; 14 - Registro de Eventos e Rastreabilidade; 15 - Compartilhamento, Uso e Proteção da Informação; 16 - Desenvolvimento Seguro; 17 - Segurança em redes;	Aceitar	5	5	25	Sim
Reidentificação de dados pseudonimizados.	1 - Política de Segurança; 2 - Gestão de Riscos; 3 - Segurança nas Operações;	Aceitar	5	5	25	Sim

POLÍCIA FEDERAL

4 - Organização da Segurança;			
5 - Classificação da Informação;			
6 - Proteção Física e do Ambiente;			
7 - Gestão de Mudanças;			
8 - Continuidade de Negócio;			
9 - Tratamento e Resposta a Incidentes;			
10 - Controles de Coleta e Preservação de Evidências;			
11 - Controles Criptográficos;			
12 - Cópia de Segurança;			
13 - Controle de Acesso Lógico;			
14 - Registro de Eventos e Rastreabilidade;			
15 - Compartilhamento, Uso e Proteção da Informação;			
16 - Desenvolvimento Seguro;			
17 - Segurança em redes;			

Legenda: P – Probabilidade; I – Impacto. Aplicam-se as mesmas definições de Probabilidade e Impacto da seção 6.

¹ Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela. As seguintes opções podem ser selecionadas: Reduzir, Evitar, Compartilhar e Aceitar.

² Risco residual é o risco que ainda permanece mesmo após a aplicação de medidas para tratar o risco.

³ Medida aprovada pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.