

Guia de Elaboração de Inventário de Dados Pessoais

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

Versão 2.0

Brasília, março de 2023

GUIA DE ELABORAÇÃO DE INVENTÁRIO DE DADOS PESSOAIS

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

Esther Dweck

Ministra

SECRETARIA DE GOVERNO DIGITAL

Rogério Souza Mascarenhas

Secretário de Governo Digital

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Leonardo Rodrigo Ferreira

Diretor de Privacidade e Segurança da Informação

COORDENAÇÃO-GERAL DE PROTEÇÃO DE DADOS

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Proteção de Dados

Equipe Técnica de Elaboração

Denis Marcelo Oliveira

Julierme Rodrigues da Silva

Loriza Andrade Vaz de Melo

Luiz Henrique do Espírito Santo Andrade

Tássio Correia da Silva

Wellington Francisco Pinheiro de Araújo

Equipe Técnica de Revisão - Versão 2.0

Bruno Pierre Rodrigues de Sousa

Francisco Magno Felix Nobre

Ivaldo Jeferson De Santana Castro

Julierme Rodrigues da Silva

Leonard Keyzo Yamaoka Batista

Rafael Da Silva Ribeiro

Raphael César Estevão

Rogério Vinícius Matos Rocha

Histórico de Versões

Data	Versão	Descrição	Autor
23/09/2020	1.0	Primeira versão do Guia de Elaboração de Inventário de Dados Pessoais.	Equipe Técnica de Elaboração
26/04/2021	1.1	Atualização do link com a tabela de temporalidade das atividades meio do Poder Executivo (Portaria 47/2020 do CONARQ).	Equipe Técnica de Elaboração
31/03/2023	2.0	Atualização para alinhamento com o Guia do Framework de Privacidade e Segurança da Informação, conforme destacado no Anexo II.	Equipe Técnica de Revisão

SUMÁRIO

AVISO PRELIMINAR E AGRADECIMENTOS	6
INTRODUÇÃO	8
1 O INVENTÁRIO DE DADOS PESSOAIS	10
1.1 O que é	10
1.2 Estruturação	10
1.3 Inventário de Dados Pessoais, RIPD e Conformidade	11
2 COMO ELABORAR O INVENTÁRIO DE DADOS PESSOAIS	13
2.1 Identificação do serviço/processo	14
2.2 Identificação dos agentes de tratamento e encarregado	15
2.3 Atuação do operador no ciclo de vida do tratamento do dado pessoal	16
2.4 Fluxo de tratamento dos dados pessoais	17
2.5 Escopo e Natureza dos dados pessoais	18
2.6 Finalidade do Tratamento dos dados pessoais	18
2.7 Categorias de dados pessoais	19
2.8 Categorias de dados pessoais sensíveis	22
2.9 Frequência e totalização das categorias de dados pessoais tratados	23
2.10 Categorias de titulares de dados pessoais	24
2.11 Compartilhamento de dados pessoais	26
2.12 Controles de Privacidade e Segurança da Informação	27
2.13 Transferência internacional de dados pessoais	29
2.14 Contrato(s)	31
2.15 Manter Atualização	32
3 LISTAGEM GERAL DO INVENTÁRIO DOS SERVIÇOS / PROCESSOS DE NÉGOCIO QUE TRATAM DADOS PESSOAIS	34
3.1 Identificação do Controlador e Encarregado	34
3.2 Listagem geral dos serviços e processos de negócio	35
REFERÊNCIAS BIBLIOGRÁFICAS	37
ANEXO I	39
ANEXO II	44

AVISO PRELIMINAR E AGRADECIMENTOS

O presente Guia, especialmente recomendado e dirigido aos órgãos e às entidades da Administração Pública Federal - APF, visa a auxiliar na Elaboração de um Inventário de Dados Pessoais, em atendimento ao previsto no art. 37 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), que determina que a Administração Pública, ao prestar diversos serviços que tratam dados pessoais à sociedade, deve manter registro das operações de tratamento realizadas sobre os dados que estão sob sua custódia. Adicionalmente, a Elaboração de um Inventário de Dados Pessoais visa a atender, além da LGPD, a outros normativos vigentes sobre o tema de privacidade e segurança da informação.

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

Nesse cenário, a Secretaria de Governo Digital enfatiza que:

- a) não representa, tampouco se manifesta em nome do CIS, da ISO e do NIST e vice-versa;
- b) não se manifesta em nome de autoridades de privacidade e segurança da informação;
- c) não é coautora das publicações internacionais abordadas;
- d) não assume nenhuma responsabilidade administrativa, técnica ou jurídica por usos ou interpretações inadequadas, fragmentados ou parciais do presente guia;
- e

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

- e) caso o leitor deseje se certificar de que atende integralmente os requisitos das publicações das instituições mencionadas, deverá consultar diretamente as fontes oficiais de informação ofertadas por elas, que foram listadas na seção “Referências Bibliográficas” deste documento.

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

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

INTRODUÇÃO

Este Guia tem por finalidade apresentar orientações com o intuito de auxiliar os órgãos e entidades da Administração Pública Federal, direta, autárquica e fundacional a realizar o levantamento e registro dos dados pessoais tratados no âmbito institucional.

O Controle 19 do Guia do Framework de Privacidade e Segurança da Informação (p. 60) estabelece que:



Controle 19: Inventário e Mapeamento – *As operações de tratamento de dados pessoais por sistemas, produtos, processos ou serviços devem ser identificadas e inventariadas.*

O presente Guia serve como um modelo prático a ser utilizado para auxiliar na adoção do Controle 19 do Guia do Framework de Privacidade e Segurança da Informação¹ v1 e respectivas evoluções desta versão (1.1, 1.2 etc.) elaborado e publicado pela SGD. As medidas do Controle 19 que estão contempladas por este Guia são: 19.1, 19.2, 19.3, 19.4, 19.5, 19.6, 19.7, 19.8, 19.9, 19.10, 19.11, 19.12, 19.13 e 19.14.

Um modo de manter os registros das operações de tratamento de dados pessoais é manter um inventário ou uma lista das atividades de tratamento que a organização realiza. O Inventário de Dados Pessoais representa o documento primordial para documentar o tratamento de dados pessoais realizados pela instituição em alinhamento ao previsto pelo art. 37 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD):

“Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.”

O inventário consiste em uma excelente forma de fazer um balanço do que o órgão e entidade faz com os dados pessoais, identificando quais dados pessoais são tratados, onde estão e que operações são realizadas com eles.

¹ < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf >. Acesso em 03/02/2023.

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

As orientações relativas à elaboração do Inventário de Dados Pessoais foram estruturadas em três capítulos:

- O Capítulo 1 destaca sua composição;
- O Capítulo 2 trata sobre como elaborá-lo; e
- O Capítulo 3 aborda a elaboração de uma listagem geral dos serviços/processos de negócios que tratam dados pessoais.

1 O INVENTÁRIO DE DADOS PESSOAIS

1.1 O que é

O **Inventário de Dados Pessoais - IDP** consiste no registro das operações de tratamento dos dados pessoais realizados pela instituição (LGPD. Art. 37).

De uma forma geral, esse registro mantido pelo **IDP** envolve descrever informações em relação ao tratamento de dados pessoais realizado pelo órgão ou entidade como:

- atores envolvidos (agentes de tratamento e o encarregado);
- finalidade (o que a instituição faz com o dado pessoal);
- hipótese (arts. 7º e 11 da LGPD);
- previsão legal;
- dados pessoais tratados pela instituição;
- categoria dos titulares dos dados pessoais;
- tempo de retenção dos dados pessoais;
- instituições com as quais os dados pessoais são compartilhados;
- transferência internacional de dados (art. 33 LGPD); e
- medidas de segurança atualmente adotadas.

O **IDP** representa um documento importante de governança de dados pessoais e de subsídio para avaliação de impacto à proteção de dados pessoais com vistas a verificar a conformidade da instituição no que se refere ao preconizado pela LGPD.

1.2 Estruturação

A estrutura do **IDP** apresentado neste documento é inspirado nos modelos propostos pelas autoridades de proteção de dados da França², Bélgica³ e Inglaterra⁴.

² < <https://www.cnil.fr/sites/default/files/atoms/files/record-processing-activities.ods>>. Acesso em 06/07/2020.

³ < <https://www.autoriteprotectiondonnees.be/publications/modele-de-registe-des-activites-de-traitement.xls> >. Acesso em 06/07/2020.

⁴ < <https://ico.org.uk/media/for-organisations/documents/2172937/gdpr-documentation-controller-template.xlsx> >. Acesso em 06/07/2020.

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

O **inventário** foi estruturado em formato de planilha eletrônica, disponível no link < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/template_inventario_dados_pessoais.xlsx >.

A planilha eletrônica que representa o template do **IDP** é composta por 4 divisões denominadas:

- “1-Orientações” – orientações gerais sobre preenchimento do template;
- “2-Lista Inventário” – lista geral dos serviços/processos de negócio institucionais que realizam o tratamento de dados pessoais;
- “3-Template” – modelo de inventário de dados pessoais a ser elaborada para cada serviço/processo de negócio da instituição; e
- “4-Listas” – apresenta uma sugestão de informações para preenchimento do inventário de dados com valores padronizados. A lista não é exaustiva e por isso pode ser ajustada de acordo com a realidade de cada instituição.

O próximo capítulo descreve o processo de elaboração do **IDP** com base divisão denominada “3-Template” constante da planilha eletrônica mencionada no início desta seção.

1.3 Inventário de Dados Pessoais, RIPD e Conformidade

O **IDP** consiste no registro das operações de tratamento dos dados pessoais realizados pela instituição. Ele proporciona uma espécie de “fotografia” do atual cenário do tratamento de dados pessoais do serviço/processo de negócio.

As informações contidas no **IDP** fornecem subsídios para a elaboração do RIPD, o qual é um instrumento fundamental para avaliação da conformidade do tratamento de dados pessoais em relação à LGPD, bem como de análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

Ao finalizar a elaboração do **IDP**, caso a instituição identifique, por exemplo, a necessidade de minimização dos dados pessoais tratados ou incompatibilidades de adequação à finalidade do tratamento de dados, **não há objeções, caso opte por sanar imediatamente no serviço/processo de negócio essas não conformidades antes da**

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

elaboração do RIPD. Todavia, **após realizar tal ação é indicado que seja gerado nova versão do IDP**, refletindo o novo cenário de tratamento de dados pessoais.

2 COMO ELABORAR O INVENTÁRIO DE DADOS PESSOAIS

De acordo com o art. 37 da LGPD, o “controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem (...)”. O inventário de dados pessoais vem atender precisamente essa determinação da Lei 13.709/2018 no que se refere à manutenção de registro do levantamento do tratamento de dados pessoais realizados pela instituição.

O formulário de **IDP** apresentado neste documento constitui uma **sugestão para auxiliar os órgãos e entidades, que exercem papel de controlador de dados pessoais**, na elaboração de inventário de dados pessoais. Dessa forma, e caso seja considerado pertinente pela instituição, o modelo de **IDP** pode ser adaptado para se adequar a cada contexto particular. A figura a seguir destaca as fases de elaboração do inventário.

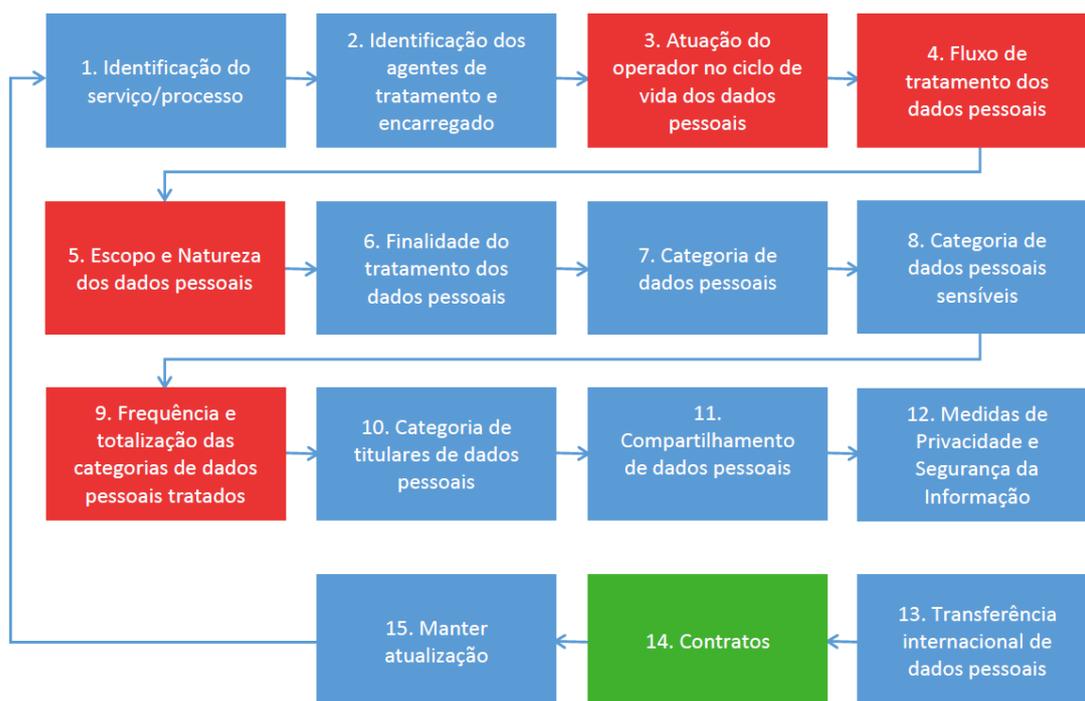


Figura 1 Fases de elaboração do Inventário de Dados Pessoais

As fases acima destacadas **em azul** representam os elementos mínimos para o **IDP**, as destacadas **em laranja** representam levantamento complementar no inventário de informações que auxiliarão a elaboração do Relatório de Impacto de Proteção de Dados

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

Pessoais - RIPD⁵ (CCGD, 2020) e a destacada em **verde** corresponde à identificação inicial de contratações a serem avaliadas na análise de adequação contratual. Importante ressaltar que todas as informações do **IDP** subsidiarão o RIPD.

Usar o modelo proposto por este Guia não é obrigatório. A instituição pode documentar as atividades de tratamento de dados pessoais da sua organização de muitas maneiras diferentes, desde modelos básicos até pacotes de software especializados. A forma como o órgão mantém sua documentação dependerá de fatores como o tamanho da instituição, o volume de dados pessoais tratados e a complexidade das operações de tratamento.

Além da proteção de dados, os órgãos e entidades muitas vezes estão sujeitos a vários outros regulamentos que têm suas próprias obrigações de documentação, especialmente em setores como seguros e finanças. Se a organização está sujeita a tais requisitos regulamentares, então é provável que já exista uma estrutura de governança de dados estabelecida em vigor que suporta seus procedimentos de documentação existentes; pode até se sobrepor aos requisitos de manutenção de registros da LGPD. Nesse caso, a LGPD não proíbe de combinar e incorporar a documentação de suas atividades de tratamento de dados pessoais com as práticas existentes de inventário de dados. Mas deve-se ter cuidado para garantir que pode cumprir os requisitos do art. 37 da LGPD, se necessário, ajustando sua estrutura de governança de dados para inventariar os dados pessoais.

As próximas seções descrevem o processo de elaboração do **IDP**, **cujo modelo tratado por este Capítulo deve ser elaborado para cada serviço/processo de negócio da instituição.**

2.1 Identificação do serviço/processo

O modelo de **IDP** proposto neste Guia adota a estratégia de inventariar os dados pessoais por serviço e/ou processo de negócio realizado pelo órgão ou entidade (Figura 2).

⁵ Informações sobre o RIPD podem ser obtidas na seção 2.5 do Guia de Boas Práticas LGPD, disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

1 - Identificação dos serviços / processo de negócio de tratamento de dados pessoais	
1.1 - Nome do serviço / Processo de negócio	
1.2 - Nº Referência / ID	
1.3 - Data de Criação do Inventário	
1.4 - Data Atualização do Inventário	

Figura 2 Seção 1 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

A opção de inventariar por serviço possibilita que a instituição realize o levantamento dos dados pessoais tratados pelos serviços divulgado no portal gov.br (<https://www.gov.br/pt-br/servicos>).

Cumpra destacar que os dados pessoais de todos os serviços devem ser inventariados, mesmo os serviços que, porventura, não são digitais.

O **IDP** também possibilita o inventário de dados pessoais por processo de negócio. Essa opção visa contemplar processos ou rotinas internas como, por exemplo, processo interno de gestão de pessoas (servidores, empregados públicos, etc.) da instituição.

Com a finalidade facilitar a identificação do serviço ou processo inventariado, o item 1.2 da Figura 2 deve ser preenchido com um número de referência ou um ID para identificação da atividade de tratamento de dados pessoais relacionada ao serviço/ processo de negócio. **Exemplos de números de referência:** 0001, 0002, etc. **Exemplo de ID adotando Sigla do Serviço informado no campo "Nome do serviço/ Processo de Negócio:** AVA, CRRA e etc. Essa etapa é finalizada com o preenchimento das datas de criação e de última atualização do inventário de dados pessoais do serviço/processo de negócio.

2.2 Identificação dos agentes de tratamento e encarregado

Esta fase envolve identificar os agentes de tratamento (controlador e operador) e o encarregado no **IDP** (art. 5º da LGPD), destacando nome, endereço, CEP, telefone e e-mail (Figura 3).

2 - Agentes de Tratamento e Encarregado	Nome	Endereço	CEP	Telefone	E-mail
2.1 - Controlador					

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

2.2 - Encarregado					
2.3 - Operador					

Figura 3 Seção 2 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

Explicações sobre controlador, operador e encarregado podem ser conferidas na seção 1.1 do Guia de Boas Práticas LGPD (CCGD, 2020).

2.3 Atuação do operador no ciclo de vida do tratamento do dado pessoal

O ciclo de vida do tratamento do dado pessoal envolve as fases de: coleta, retenção, processamento, compartilhamento e eliminação.

Constatar em que fase do ciclo de vida do tratamento do dado pessoal o operador atua (Figura 4) é essencial para compreensão de quais operações de tratamento são realizadas por ele e quais ativos organizacionais estão envolvidos nesse tratamento.

3 - Fases do Ciclo de Vida do Tratamento Dados Pessoais	Coleta	Retenção	Processamento	Compartilhamento	Eliminação
3.1 - Em qual fase do ciclo de vida o Operador atua					

Figura 4 Seção 3 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

Uma vez identificados os ativos, é necessário analisá-los para verificar quais medidas técnicas de segurança estão efetivamente implementadas nesses ativos, com vistas a prover a adequada proteção aos dados pessoais de que trata a LGPD. As medidas de segurança resultantes dessa análise serão descritas na fase "Medidas de Segurança" descrita na seção 2.12 deste Guia.

Orientações sobre ciclo de vida de tratamento de dados pessoais e seu relacionamento com os ativos organizacionais podem ser observadas no Capítulo 3 do Guia de Boas Práticas LGPD (CCGD, 2020).

Esta fase do **IDP** subsidiará um dos elementos que compõem a descrição da natureza do tratamento no RIPD (CCGD, 2020), no que tange ao papel do operador em relação ao tratamento do dado pessoal.

2.4 Fluxo de tratamento dos dados pessoais

Descrever como (de que forma) os dados pessoais são coletados, retidos/armazenados, processados/usados e eliminados (Figura 5).

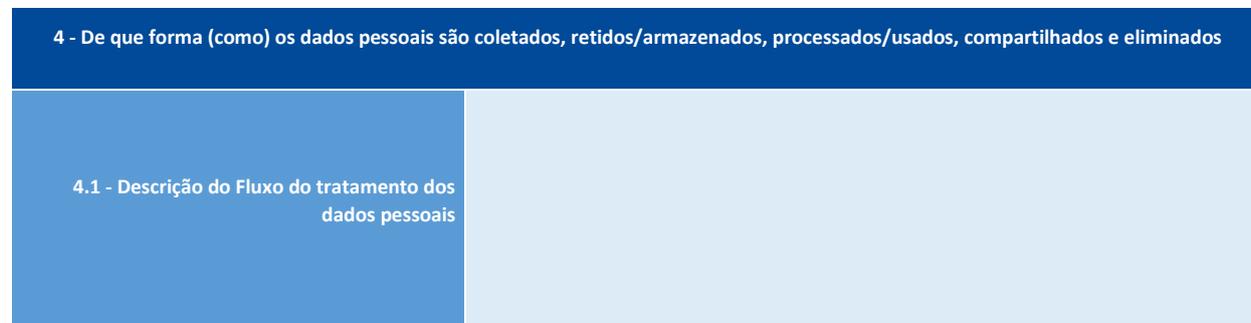


Figura 5 Seção 4 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

Nessa fase, pode até ser elaborado um desenho com um fluxo de dados.

Abaixo, consta exemplificação de descrição do fluxo de tratamento de dados pessoais do programa fictício de localização de desaparecidos do Departamento de Segurança Pública - DSP.

Exemplo de descrição de fluxo de dados:

1. Os dados pessoais são coletados mediante preenchimento formulário eletrônico do Sistema Nacional pelo titular dos dados pessoais.
2. Os dados são transferidos armazenados nas instalações físicas da Empresa de Processamento e Tecnologia Fictum (operador).
3. A empresa Fictum realiza processamento sobre os dados pessoais e disponibiliza para uso do Departamento de Segurança Pública – DSP (controlador). O DSP disponibiliza os dados pessoais para utilização e consumo do comunicante.
4. O DSP transfere dados de comunicantes e pessoas desaparecidas para a Secretaria de Desenvolvimento Humano desenvolver as ações de apoio psicológico para as famílias dos desaparecidos.
5. Os dados pessoais podem ser eliminados a pedido do titular. Nesse caso, o DSP encaminha essa solicitação para a empresa Fictum executar a eliminação dos dados pessoais da base de dados do Sistema Nacional de Desaparecidos.

2.5 Escopo e Natureza dos dados pessoais

Esta fase contempla identificar dois elementos relevantes do escopo e natureza dos dados pessoais tratados a serem futuramente descritos no RIPD (CCGD, 2020). Esses elementos são, respectivamente, a abrangência e a fonte de dados pessoais (Figura 6).

5 - Escopo e Natureza dos Dados Pessoais	
5.1 - Abrangência da área geográfica do tratamento	
5.2 - Fonte de dados utilizada para obtenção dos dados pessoais	

Figura 6 Seção 5 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

A abrangência representa o alcance geográfico do tratamento de dados realizado: nacional, estadual, distrital, municipal ou regional.

A fonte de obtenção de dados pessoais, pode ser por exemplo: titular dos dados pessoais, XML, API, etc. A forma de obtenção dos dados pessoais tem influência direta nos mecanismos que devem ser implementadas para assegurar os princípios da qualidade dos dados (LGPD, art. 6º, V) e segurança (LGPD, art. 6º, VII).

Exemplo 1: Se os dados pessoais são obtidos por meio de preenchimento de formulário eletrônico, então a fonte de dados é o titular dos dados pessoais.

Exemplo 2: Fonte de dados que não seja o titular de dados, é importante detalhar a fonte, como por exemplo, API CONSULTA CPF.

2.6 Finalidade do Tratamento dos dados pessoais

Esta fase aborda a identificação de três aspectos fundamentais para respaldar o tratamento dos dados pessoais: a hipótese (arts. 7º e 11) da LGPD, a especificação da finalidade e a previsão legal (Figura 7).

6 - Finalidade do Tratamento de Dados Pessoais	
6.1 - Hipótese de Tratamento	
6.2 - Finalidade	
6.3 - Previsão legal	

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

6.4 - Resultados pretendidos para o titular de dados	
6.5 - Benefícios esperados para o órgão, entidade ou para a sociedade como um todo	

Figura 7 Seção 6 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

Orientações sobre base legal (Figura 7, item 6.3) e hipóteses de tratamento (Figura 7, item 6.1) podem ser conferidas, respectivamente, nas seções 1.1 e 2.1 do Guia de Boas Práticas LGPD (CCGD, 2020).

A previsão legal representa informar no item 6.3 da Figura 7 qual Lei, Decreto, normativo ou regulamento que respalda a finalidade do tratamento de dados pessoais realizado.

Exemplo fictício de previsão legal considerando o Programa de Localização de Desaparecidos:

- Decreto nº 8.956, de 25 de janeiro de 2018, institui o Programa de Localização de Desaparecidos.

Nesse momento, cabe ressaltar que os órgãos e entidades da administração pública tem a prerrogativa de tratar os dados pessoais para o exercício de suas competências legais ou execução de políticas públicas sem a necessidade de obter consentimento do titular dos dados pessoais (CCGD, 2020).

A finalidade (Figura 7, item 6.2) é a razão ou motivo pela qual se deseja tratar os dados pessoais. É fundamental estabelecer claramente a finalidade, pois é ela que apresenta a justificativa do tratamento de dados pessoais e fornece os elementos para informar o titular dos dados pessoais (CCGD, 2020).

A conclusão dessa fase compreende descrever em relação à finalidade do tratamento:

- os resultados pretendidos para o titular dos dados pessoais; e
- benefícios esperados para o órgão, entidade ou para a sociedade como um todo.

2.7 Categorias de dados pessoais

Identificar quais são os dados pessoais tratados pelo órgão ou entidade que representa o objetivo central do **IDP**. Inventariar os dados pessoais utilizados pela instituição

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

possibilitará avaliar se todos os dados pessoais usados são realmente necessários e adequados para realização de suas finalidades (LGPD, art. 6º, III).

A fim de facilitar a identificação dos dados pessoais tratados, o modelo de **IDP** **elencia uma lista exemplificativa e não exaustiva de 15 categorias de dados pessoais com suas respectivas subcategorias**, para as quais devem ser especificamente descritos os dados pessoais tratados.

A Figura 8 destaca o primeiro tipo de categoria de dados pessoais, "7.1 Dados de Identificação Pessoal", e as colunas a serem preenchidas explicadas a seguir.

7 - Categoria de Dados Pessoais				
7.1 -Dados de Identificação Pessoal	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.1.1 - Informações de identificação pessoal				
7.1.2 - Informações de identificação atribuídas por instituições governamentais				
7.1.3 - Dados de identificação eletrônica				
7.1.4 - Dados de localização eletrônica				

Figura 8 Seção 7 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

Descrição: descrever de forma específica os dados pessoais tratados (ex.: CPF, nome, etc.) de acordo com as subcategorias listadas no Anexo deste Guia.

Tempo Retenção dos dados: informação sobre quanto tempo o dado pessoal será armazenado. Para definição do tempo de retenção é indicado verificar:

- se existe alguma definição legal de tempo de retenção/guarda/arquivamento de documentos e/ou dos dados tratados pelo órgão e/ou entidade; e
- tabela de temporalidade do CONARQ⁶.

⁶ Disponível em: < https://www.gov.br/arquivonacional/pt-br/servicos/gestao-de-documentos/orientacao-tecnica-1/codigo-de-classificacao-e-tabela-de-temporalidade-e-destinacao-de-documentos-de-arquivo/copy_of_cod_classif_-e_tab_temp_2019_m_book_digital_25jun2020.pdf >

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

Fonte de Retenção: em que local o dado pessoal está armazenado/retido. Nesse campo deve ser informado a principal fonte de retenção/armazenamento dos dados para cada categoria de dados pessoais efetivamente tratada pela instituição.

Nome Base de Dados: essa coluna deverá ser preenchida, se a principal fonte de retenção / armazenamento dos dados pessoais for base de dados. Informar o mesmo nome da base de dados registrada no Sistema de Catálogo de Dados⁷ mantido pela Secretaria de Governo Digital - SGD. O nome e a descrição da base de dados devem ser atualizados na guia "4-Listas" apresentada na seção 1.2 deste documento. **Necessário destacar que não há obrigatoriedade de se informar o nome da base de dados, caso a instituição não tenha iniciado o citado Catálogo de Dados.**

Se órgão não for iniciar o cadastro do Catálogo de Base de Dados – CBD antes ou concomitante ao **IDP**, então a instituição pode optar por definir o nome e a descrição da base de dados, conforme orientado na guia “4-Listas” mencionada acima. Posteriormente, ao iniciar o CBD, o órgão ou entidade pode aproveitar os nomes e descrições das bases de dados definidos no inventário e informá-los no sistema do CBD.

Compreendido o que significa cada coluna exibida pelo Figura 8, é recomendável que seja realizada a leitura do Anexo deste documento, no qual consta uma tabela com **rol não exaustivo** de categorias, subcategorias e o que deve ser descrito na coluna “Descrição” constante da Figura 8 referentes aos dados pessoais tratados pela instituição. Dessa forma, ao elaborar o **IDP**, **a instituição tem total liberdade para adaptar, remover, incluir categorias, subcategorias e descrição dos dados tratados de acordo com sua realidade institucional.**

Diante do listado no Anexo deste Guia, para cada categoria e subcategoria dos dados pessoais tratados pelo órgão ou entidade, deve-se preencher os dados pessoais efetivamente usados. A título de exemplificação, se a instituição trata apenas dados pessoais de CPF e nome, então a coluna “Descrição” da Figura 8 serão preenchidos da seguinte forma:

⁷ Para saber mais sobre a iniciativa de Catálogo de Base de Dados da SGD, acesse o link: < <https://www.gov.br/governodigital/pt-br/governanca-de-dados/catalogo-de-bases-de-dados> >

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

- na subcategoria “7.1.1 - Informações de identificação pessoal” constaria o dado pessoal “Nome”; e
- na subcategoria “7.1.2 - Informações de identificação atribuídas por instituições governamentais” constaria o dado pessoal “CPF”.

2.8 Categorias de dados pessoais sensíveis

O preenchimento das colunas relativas aos dados pessoais sensíveis da Figura 9 segue a mesma forma explicada na seção 2.7 do Guia.

8 - Categorias de Dados Pessoais Sensíveis	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
8.1 - Dados que revelam origem racial ou étnica				
8.2 - Dados que revelam convicção religiosa				
8.3 - Dados que revelam opinião política				
8.4 - Dados que revelam filiação a sindicato				
8.5 - Dados que revelam filiação a organização de caráter religioso				
8.6 - Dados que revelam filiação ou crença filosófica				
8.7 - Dados que revelam filiação ou preferências política				
8.8 - Dados referentes à saúde ou à vida sexual				
8.9 - Dados genéticos				
8.10 - Dados biométricos				

Figura 9 Seção 8 da guia “3-Templates” da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

Realizar o inventário de dados pessoais sensíveis é extremamente importante, visto que o uso indevido desses dados pode resultar em algum tipo de discriminação em relação ao titular dos dados pessoais sensíveis. A seção 2.1.3 do Guia de Boas Práticas LGPD (CCGD, 2020) trata das especificidades para o tratamento de dados pessoais sensíveis.

As categorias listadas na Figura 9 representam a lista de dados sensíveis do inciso II do art. 5º da LGPD.

Art. 5º Para os fins desta Lei, considera-se:

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

2.9 Frequência e totalização das categorias de dados pessoais tratados

Nesta fase são identificadas a frequência de tratamento dos dados pessoais e a quantidade de dados pessoais e dados pessoais sensíveis tratados pelo serviço / processo de negócio (Figura 10).

A frequência e totalização das categorias de dados pessoais tratados fornecerão subsídio para o escopo do tratamento de dados pessoais a serem descritos no RIPD (CCGD, 2020).

9 - Frequência e totalização das categorias de dados pessoais tratados	
9.1 - Frequência de tratamento dos dados pessoais	
9.2 - Quantidade de dados pessoais e dados pessoais sensíveis tratados	

Figura 10 Seção 9 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

A frequência de tratamento de dados pessoais representa a disponibilidade e horário de funcionamento do sistema automatizado ou processo manual que trata os dados pessoais.

Exemplo fictício de descrição da frequência de tratamento de dados pessoais do Sistema Nacional de Desaparecidos - SND:

O SND está disponível no regime 24x7 (24 horas por dia nos 7 dias da semana) para comunicação (coleta) dos dados dos desaparecimentos e as demais fases e operações de tratamento são realizadas no horário comercial em dias úteis.

Informação sobre o horário em que os dados pessoais são tratados contribui para identificar acessos ou processamentos indevidos dos dados pessoais. Considerando o exemplo acima, se operações específicas de tratamento de dados pessoais somente ocorre em horário comercial e dias úteis, uma ação no sistema fora

desses parâmetros pode indicar que alguma operação suspeita sobre os dados foi realizada.

Totalizar a quantidade de dados pessoais e dados pessoais sensíveis tratados propicia uma visão quantitativa do número de dados pessoais tratados. Essa totalização é muito relevante, pois quantos mais dados pessoais são tratados maior será o potencial impacto aos titulares dos dados pessoais em caso, por exemplo, de vazamentos.

Exemplo de totalização de dados pessoais:

A instituição realiza tratamento de dados pessoais como: idade, sexo, data de nascimento, local de nascimento, estado civil e nacionalidade.

Trata dados pessoais sensíveis de saúde como: CID10 e data do exame médico.

Nesse exemplo a informação a ser preenchida no item 9.2 exibido na Figura 10 é:

São tratados 6 dados pessoais e 2 dados pessoais sensíveis, totalizando 8 dados pessoais tratados pelo serviço.

2.10 Categorias de titulares de dados pessoais

Além de elencar os dados pessoais tratados, é necessário identificar em relação a esses dados (Figura 11): quais são as categorias (tipos) de titulares a quem pertencem os dados pessoais; e se são tratados dados pessoais de crianças/adolescentes, bem como de outro grupo vulnerável.

10 - Categorias dos titulares de dados pessoais	Tipo de Categoria	Descrição
10.1 - Categoria 1		
10.2 - Categoria 2		
10.3 - Trata dados de crianças e adolescentes		
10.4 - Além de crianças e adolescente trata dados de outro grupo vulnerável		

Figura 11 Seção10 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

Na planilha eletrônica que automatiza o **IDP**, podem ser inseridas quantas categorias de titulares que forem necessárias para o fiel registro dos tipos de titulares de dados pessoais que estão envolvidos pelo tratamento de dados realizado pelo serviço / processo de negócio. **Os tipos de categorias já estão previamente definidos na guia “4-Listas” citada na seção 1.2, mas podem ser alterados e ajustados de acordo com o contexto da instituição.**

A coluna “Descrição” constante da Figura 11, deve ser preenchida se for necessário descrever informações complementares, detalhando a categoria do titular dos dados pessoais.

Exemplo 1: Categoria de titular = Pessoas. Nesse caso, a coluna "Descrição" poderia ser preenchida com "Pessoas com deficiência", "Pessoas de baixa renda", etc.

Exemplo 2: Categoria de titular = Dependentes. Nesse caso, a coluna "Descrição" poderia ser preenchida com "Dependentes para fins de IRRF", "Dependentes de para fins de Plano de Saúde", etc.

No item 10.3 mostrado pela Figura 11, o **IDP** propicia constatar se são tratados dados de crianças e adolescentes. Tal constatação é fundamental no sentido de o órgão ou entidade analisar se são atendidas as determinações do art. 14 da LGPD, tal como o prévio consentimento de pais e responsáveis para o tratamento de dados pessoais de crianças. Considerações sobre esse tema podem ser conferidas na seção 2.1.4 do Guia de Boas Práticas LGPD (CCGD, 2020).

O item 10.4 destacado pela Figura 11, permite identificar se é tratado dado pessoal de algum outro grupo vulnerável como, por exemplo: idosos, população em condição de rua, pessoas com deficiência física ou sofrimento mental etc.

A identificação do tratamento de dados pessoais propiciada pelos itens 10.3 e 10.4 da Figura 11 fornecerão elementos para descrição do contexto de tratamento no RIPD (CCGD, 2020) subsidiando a composição do cenário de riscos para avaliar quais controles e

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

medidas de segurança devem ser adotados para proteção dos dados de crianças, adolescentes e outros grupos vulneráveis em alinhamento à legislação vigente que os protegem.

2.11 Compartilhamento de dados pessoais

Informar com quais instituições os dados pessoais são compartilhados e para qual finalidade (Figura 12). **Devem ser inseridas quantas linhas forem necessárias para registrar todas as instituições que têm acesso aos dados pessoais via compartilhamento. Caso sejam compartilhados dados pessoais com menos de 4 instituições, indica-se a exclusão das linhas excedentes.**

11 - Compartilhamento de Dados Pessoais	Dados pessoais compartilhados	Finalidade do compartilhamento
11.1 - Nome da Instituição 1		
11.2 - Nome da Instituição 2		
11.3 - Nome da Instituição 3		
11.4 - Nome da Instituição 4		

Figura 12 Seção 11 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

O início dessa fase é marcado pela indicação do nome da instituição que recebe os dados pessoais compartilhados, deve-se substituir o subitem da seção 11 da Figura 12 pelo nome da instituição.

Exemplos de registro das instituições que recebem dados pessoais por compartilhamento:

Exemplo 1: Compartilhamento com o Ministério da Gestão e da Inovação em Serviços Públicos. Nesse caso, substitua "11.1 - Nome da Instituição 1" por "11.1 - Ministério da Gestão e da Inovação em Serviços Públicos".

Exemplo 2: Compartilhamento com o Banco Central. Nesse caso, substitua "11.2 - Nome da Instituição 2" por "11. 2 - Banco Central".

Exemplo 3: Compartilhamento com a CGU. Nesse caso, substitua "11.3 - Nome da Instituição 3" por "11.3 - CGU".

Exemplo 4: Compartilhamento com o INSS. Nesse caso, substitua "11.4 - Nome da Instituição 4" por "11. 4 - INSS".

Para cada instituição deve-se informar quais são os dados compartilhados e a finalidade do compartilhamento.

Desse modo, a coluna **“Dados pessoais compartilhados”** referenciada pela Figura 12, é preenchida com os dados pessoais e dados pessoais sensíveis compartilhados com as instituições destinatárias dos dados. No preenchimento dessa coluna utilize, no que couber, as informações descritas nas seções "7 - Categorias de Dados Pessoais" e "8 - Categorias de Dados Pessoais Sensíveis" explicitadas nas seções 2.7 e 2.8 deste Guia. **Se não compartilhar dados com outras instituições, preencha a coluna “Dados pessoais compartilhados” do item "11.1 - Nome da Instituição 1" destacado na Figura 12 com “Não se Aplica”.**

Esta fase é finalizada com o preenchimento finalidade do compartilhamento. Nesse caso, **é fundamental atentar que a finalidade do compartilhamento deve ser compatível com a finalidade que embasou o tratamento dos dados pessoais discutida na seção 2.6 deste Guia.**

Se existir incompatibilidade, então esse é um ponto de atenção a ser tratado pela instituição no sentido de existir uma adequação da finalidade do compartilhamento ou até mesmo sua interrupção. Essa situação é um dos pontos de atenção a ser considerado na seção 2.16 deste documento.

2.12 Controles de Privacidade e Segurança da Informação

Esta fase envolve identificar os atuais controles de segurança, técnicos administrativos adotados e a descrição das medidas implementadas (Figura 13) que visam assegurar a integridade dos dados pessoais, minimizando os riscos como, por exemplo, de

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

perda ou vazamento de dados. **Devem ser inseridas quantas linhas forem necessárias para registrar todos os controles de privacidade e segurança da informação aplicados para proteção de dados pessoais, bem como a descrição das medidas adotadas. Caso sejam implementadas menos de 3 controles, indica-se a exclusão das linhas excedentes.**

Os controles de segurança implementados dependem da sensibilidade dos dados pessoais que são tratados e dos riscos para os titulares de dados no caso de um incidente.

12 – Controles de Privacidade e Segurança da Informação	Tipo de Controle de Privacidade e Segurança da Informação	Descrição da(s) Medida(s)
12.1 - Controle de Privacidade e Segurança da Informação 1		
12.2 - Controle de Privacidade e Segurança da Informação 2		
12.3 - Controle de Privacidade e Segurança da Informação 3		

Figura 13 Seção 12 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

Na planilha eletrônica que automatiza o **IDP**, podem ser inseridos quantos controles de privacidade e segurança da informação forem necessários para o fiel registro dos tipos de titulares de dados pessoais que estão envolvidos pelo tratamento de dados realizado pelo serviço / processo de negócio. **Os tipos de controles de privacidade segurança da informação da coluna "Tipos de controles de privacidade e segurança da informação" já estão previamente definidos na guia "4-Listas" citada na seção 1.2 e foram selecionados do Guia do Framework de Privacidade e Segurança da Informação, mas podem ser alterados e ajustados de acordo com o contexto da instituição.**

A coluna "Descrição das Medidas" exibida na Figura 13 deve ser preenchida com os identificadores ou a descrição da(s) medida(s) específica(s) adotada(s) para o controle de privacidade e segurança da informação.

[Exemplos de controles de privacidade e segurança da informação e descrição de medidas:](#)

[Exemplo 1:](#)

Tipo de controle de privacidade e segurança da informação = Proteção de dados.

Descrição da(s) Medida(s) = Descarte seguro de dados; Uso de criptografia em mídia removível, dados sensíveis em trânsito e em repouso; e Adoção de solução de prevenção contra perda de dados.

Exemplo 2:

Tipo de controle de privacidade e segurança da informação = Abertura, Transparência e Notificação.

Descrição da(s) Medida(s) = Disponibilização de política de privacidade em local de fácil acesso, antes ou no momento do tratamento de dados pessoais, sem a necessidade de o titular ter que solicitá-lo especificamente.

2.13 Transferência internacional de dados pessoais

Esta fase do **IDP** envolve destacar as organizações internacionais que recebem dados pessoais por meio de qualquer tipo de transferência ou compartilhamento (Figura 14). **Devem ser inseridas quantas linhas forem necessárias para registrar todas as organizações que têm acesso ao dado pessoal por transferência internacional. Caso exista transferência internacional de dados pessoais com menos de 3 organizações, indica-se a exclusão das linhas excedentes.**

13 - Transferência Internacional de Dados Pessoais	País	Dados pessoais transferidos	Tipo de garantia para transferência
13.1 - Organização 1			
13.2 - Organização 2			
13.3 - Organização 3			

Figura 14 Seção 13 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

O início dessa fase é marcado pelo registro do nome da organização e país que recebe o dado pessoal por transferência internacional. Deve-se substituir o subitem da seção 13 da Figura 14 pelo nome da organização.

Exemplos de registros das organizações e países que recebem dados pessoais por transferência internacional:

Exemplo 1: Transferência Internacional para a Universidade de Coimbra. Nesse caso, substitua "**13.1 - Nome da Organização 1**" por "**13.1 - Universidade de Coimbra**". Nesse caso, preencher a coluna "**País**" com "**Portugal**".

Exemplo 2: Transferência Internacional para o U.S. Department of Agriculture (USDA). Nesse caso, substitua "**13.2 - Nome da Organização 2**" por "**13.2 - U.S. Department of Agriculture (USDA)**". Nesse caso, preencher a coluna "País" com "**Estados Unidos**".

Exemplo 3: Transferência Internacional para o Department of Justice - Government of Western Australia. Nesse caso, substitua "**13.3 - Nome da Organização 3**" por "**13.3 - Department of Justice - Government of Western Australia**". Nesse caso, preencher a coluna "País" com "**Austrália**".

Caso o órgão ou entidade não realize transferência internacional de dados pessoais, preencha a coluna "País" do item "13.1 - Nome da Organização 1" destacada na Figura 14 com "Não se Aplica".

Para cada organização que recebe dados por transferência internacional deve-se informar quais são os dados pessoais transferidos e o tipo de garantia para transferência. Desse modo, a coluna "**Dados pessoais transferidos**" referenciada pela Figura 14, é preenchida com os dados pessoais e dados pessoais sensíveis compartilhados com as instituições destinatárias dos dados. No preenchimento dessa coluna utilize, no que couber, as informações descritas nas seções "**7 - Categorias de Dados Pessoais**" e "**8 - Categorias de Dados Pessoais Sensíveis**" explicitadas nas seções 2.7 e 2.8 deste Guia.

A coluna "**Tipo de garantia para transferência**" deve ser preenchida para cada organização que recebe dados pessoais por transferência internacional. **Os tipos de garantia da coluna "Tipo de garantia para transferência" já estão previamente definidos na divisão "4-Listas" citada na seção 1.2, mas podem ser alterados e ajustados de acordo com o contexto da instituição.** A transferência internacional de

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

dados pessoais somente é permitida para os casos elencados no art. 33 da LGPD, os quais já estão contemplados pelo modelo de **IDP** apresentado neste Guia.

Antes de realizar transferência internacional, é recomendado verificar se o país estrangeiro para o qual o órgão ou entidade está transferindo os dados pessoais detém legislação de proteção de dados e se é reconhecida como adequada pela Autoridade Nacional de Proteção de Dados - ANPD. Caso a legislação do país estrangeiro não seja considerada como adequada pela ANPD, o órgão ou entidade precisará indicar ao país estrangeiro uma das estruturas legais descritas no art. 33 a fim de garantir a proteção dos dados pessoais dos cidadãos brasileiros no exterior.

2.14 Contrato(s)

Nesse momento, identificam-se as contratações de serviços ou soluções de TI que realizam algum tipo de operação de tratamento com os dados pessoais do serviço/processo de negócio (Figura 15). **Devem ser inseridas quantas linhas forem necessárias para destacar todos os contratos que tratam os dados pessoais elencados para o serviço/processo de negócio. Se existir apenas um contrato, então deve-se excluir a linha identificada por "14.2 - Contrato nº 2".**

14 - Contrato(s) de serviços e/ou soluções de TI que trata(m) dados pessoais do serviço/processo de negócio	Nº Processo Contratação	Objeto	E-mail do Gestor do Contrato
14.1 - Contrato nº 1			
14.2 - Contrato nº 2			

Figura 15 Seção 14 da guia "3-Templates" da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

Inicialmente, é necessário informar o número de identificação do contrato de serviço ou solução de TI que realiza algum tipo de operação de tratamento com os dados pessoais elencados no inventário, assim, deve-se substituir o subitem da seção 14 da Figura 15 pelo número do contrato.

[Exemplos de registros de identificação de contratos de serviços e/ou solução de TI que realizam alguma operação de tratamento sobre os dados pessoais elencados no IDP.](#)

Exemplo 1: Contrato identificado pelo nº 15/2020. Nesse caso, substitua "Contrato nº 1" por "Contrato nº 15/2020".

Exemplo 2: Contrato identificado pelo nº 30/2020. Nesse caso, substitua "Contrato nº 2" por "Contrato nº 30/2020".

Caso não exista contrato de serviço ou solução de TI que realize operação de tratamento com os dados pessoais elencados no inventário, preencha a coluna “Nº Processo de Contratação” do item “14.1 – Contrato nº 1” destacada na Figura 15 com “Não há contrato de serviço ou solução de TI que realize operação de tratamento com os dados pessoais elencados neste inventário”.

Após identificar os contratos, é necessário informar o objeto contrato e o e-mail de contato do gestor do contrato.

Dessa forma, a coluna **“Objeto do Contrato”** referenciada pela Figura 15, é preenchida com a especificação do objeto descrita no contrato.

A coluna **“E-mail do Gestor do Contrato”** deve ser preenchida com o e-mail institucional do gestor responsável pelo contrato.

A identificação dos gestores de contratos viabiliza a discussão dos possíveis ajustes contratuais no momento de a instituição realizar a atividade de análise da adequação dos contratos em relação ao preconizado pela LGPD.

A atividade de adequação contratual é abordada no “Guia de Boas Práticas para Especificação de Requisitos de Segurança da Informação em Contratações de Tecnologia da Informação” disponibilizado pela Secretaria de Governo Digital.

2.15 Manter Atualização

O **IDP** não termina com a conclusão de sua elaboração. É extremamente necessário que as informações documentadas no **inventário** sempre reflitam a situação atual do tratamento de dados pessoais do serviço/processo de negócio. Ele é um documento “vivo” que é atualizado quando necessário.

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

Portanto, indica-se que o **IDP** deva ser revisto e atualizado, no mínimo, anualmente, ou sempre que existir qualquer mudança que afete o tratamento dos dados pessoais do serviço/processo de negócio registrado no inventário.

3 LISTAGEM GERAL DO INVENTÁRIO DOS SERVIÇOS / PROCESSOS DE NÉGOCIO QUE TRATAM DADOS PESSOAIS

Ter uma visão geral de todos os inventários de dados pessoais elaborados para cada serviço/processo de negócio é de suma importância para a instituição. Isso facilita o acompanhamento do andamento das ações de inventário e propicia rápida localização da identificação de um inventário de um serviço/processo inventariado.

Nesse contexto, as próximas seções abordarão o modelo de listagem geral sintética apresentado pela guia “2-Lista Inventário” constante da planilha eletrônica disponível em <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/template_inventario_dados_pessoais.xlsx>. Tal listagem visa elencar os **IDPs** elaborados pelo órgão/entidade.

3.1 Identificação do Controlador e Encarregado

Nesta parte inicial da listagem são identificados o controlador e o encarregado (incisos VI e VII do art. 5º da LGPD), destacando nome, e-mail, endereço, CEP, cidade e telefone (Figura 16).

Controlador	Nome:	E-mail:	Endereço:
	CEP:	Cidade:	Telefone:
Encarregado	Nome:	E-mail:	Endereço:
	CEP:	Cidade:	Telefone:

Figura 16 Parte inicial da guia “2-Lista Inventário” da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

Diferentemente da seção 2.2 deste Guia, na listagem geral não consta a identificação do operador porque pode ocorrer de existir mais de um operador atuando em cada serviço/processo de negócio que trata dados pessoais. Contudo, se a instituição considerar importante constar a informação do operador na listagem geral, então realize esse ou

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

qualquer outro ajuste no modelo da listagem, de acordo com o mais indicado para sua realidade institucional.

3.2 Listagem geral dos serviços e processos de negócio

Nesta parte final da listagem geral são preenchidas as seguintes colunas para cada serviço/processo de negócio inventariado (Figura 16):

- “Nome do serviço/processo de negócio”;
- “Nº Ref / ID”;
- “Data de Criação do Inventário”;
- “Data de Atualização do Inventário”;
- “Finalidade do tratamento dos dados pessoais”; e
- “Trata Dados Pessoais Sensíveis?”

Nome do serviço/processo de negócio	Nº Ref / ID	Data de Criação do Inventário	Data de Atualização do Inventário	Finalidade do tratamento dos dados pessoais	Trata Dados Pessoais Sensíveis?

Figura 17 Parte final do guia “2-Lista Inventário” da planilha eletrônica do Inventário de Dados Pessoais (seção 1.2 deste Guia)

As informações a serem preenchidas nas colunas destacadas pela Figura 16 constam das seções discutidas no capítulo 2 deste Guia. Assim, com a finalidade de destacar a correspondência entre as colunas exibidas pela Figura 16 com o modelo de **IDP** apresentado no Capítulo 2, é apresentada a tabela a seguir.

Coluna da guia “2-Lista Inventario” (Figura 16)	Seção do Capítulo 2 do Guia - item da figura
Nome do serviço/processo de negócio	Seção 2.1 – item 1.1 da Figura 2
Nº Ref / ID	Seção 2.1 – item 1.2 da Figura 2
Data de Criação do Inventário	Seção 2.1 – item 1.3 da Figura 2
Data de Atualização do Inventário	Seção 2.1 – item 1.4 da Figura 2
Finalidade do tratamento dos dados pessoais	Seção 2.6 – item 6.2 da Figura 7

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

Coluna da guia "2-Lista Inventario" (Figura 16)	Seção do Capítulo 2 do Guia - item da figura
Trata Dados Pessoais Sensíveis?	Seção 2.8 – Item 8.1 até 8.10 da Figura 9 Preencher com Sim: se existir pelo menos uma informação de dado sensível estiver preenchida em qualquer das subcategorias do item 8. Preencher com Não se nenhuma informação de dado sensível estiver preenchida nas subcategorias do item 8.

Tabela 1 Correspondência da Listagem Geral com o IDP

REFERÊNCIAS BIBLIOGRÁFICAS

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: 04 set. 2020.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS - CNIL. **Record of processing activities**. Disponível em: < <https://www.cnil.fr/sites/default/files/atoms/files/record-processing-activities.ods> >. Acesso em: 04 set. 2020.

COMITÊ CENTRAL DE GOVERNANÇA DE DADOS - CCGD. **Guia de Boas Práticas LGPD**. Abril 2020. Disponível em: < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/quias/quia_lgpd.pdf >. Acesso em: 04 set. 2020.

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE GOVERNO DIGITAL – DPSI/SGD. **Guia do Framework de Privacidade e Segurança da Informação**. Novembro 2022. Disponível em: < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf >. Acesso em: 06 fev. 2023.

CONSELHO NACIONAL DE ARQUIVOS - CONARQ. **Classificação, Temporalidade e Destinação de documentos de Arquivo Relativo às Atividades-Meio da Administração Pública**. Disponível em: < https://www.gov.br/arquivonacional/pt-br/servicos/gestao-de-documentos/orientacao-tecnica-1/codigo-de-classificacao-e-tabela-de-temporalidade-e-destinacao-de-documentos-de-arquivo/copy_of_cod_classif_-e_tab_temp_2019_m_book_digital_25jun2020.pdf >. Acesso em: 26 abr. 2021.

Information Commissioner's Office - ICO. **Documentation template for controllers**. Disponível em: < <https://ico.org.uk/media/for-organisations/documents/2172937/gdpr-documentation-controller-template.xlsx> >. Acesso em: 04 set. 2020.

AUTORITÉ DE PROTECTION DES DONNÉES GEGEVENSBSCHERMINGS AUTORITEIT. **Modele de Registe des Activites de Traitement**. Disponível em: <

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

<https://www.autoriteprotectiondonnees.be/publications/modele-de-registe-des-activites-de-traitement.xls> >. Acesso em: 04 set. 2020.

ANEXO I

Categorias de Dados Pessoais

As categorias, subcategorias e descrições dos dados pessoais apresentadas na tabela abaixo foram inspiradas no modelo de registro (inventário) proposto pela autoridade de proteção de dados da Bélgica⁸.

SUBCATEGORIA	DESCRIÇÃO (Descrever se são tratados dados pessoais sobre:)
CATEGORIA: 7.1 - Dados de Identificação Pessoal	
7.1.1 - Informações de identificação pessoal	Nome, endereço residência, histórico de endereços anteriores, número de telefone fixo residencial, número celular pessoal, e-mail pessoal, etc.
7.1.2 - Informações de identificação atribuídas por instituições governamentais	CPF, RG, número do passaporte, número da carteira de motorista, número da placa, número de registro em conselho profissional, etc.
7.1.3 - Dados de identificação eletrônica	Endereços IP, cookies, momentos de conexão etc.
7.1.4 - Dados de localização eletrônica	Dados de comunicação de torres de celulares (ex: GSM), dados de GPS etc.
CATEGORIA: 7.2 - Dados Financeiros	
7.2.1 - Dados de identificação financeira	Números de identificação, números de contas bancárias, números de cartões de crédito ou débito, códigos secretos.
7.2.2 - Recursos financeiros	Renda, posses, investimentos, renda total, renda profissional, poupança, datas de início e término dos investimentos, receita de investimento, dívidas sobre ativos.
7.2.3 - Dívidas e despesas	Total de despesas, aluguel, empréstimos, hipotecas e outras formas de crédito.
7.2.4 - Situação financeira (Solvência)	Avaliação do rendimento e avaliação de capacidade de pagamento.
7.2.5 - Empréstimos, hipotecas, linhas de crédito	Natureza do empréstimo, valor emprestado, saldo remanescente, data de início, período do empréstimo, taxa de juros, visão geral do pagamento, detalhes sobre as garantias.
7.2.6 - Assistência financeira	Benefícios, assistência, bonificações, subsídios, etc.

⁸ < <https://www.autoriteprotectiondonnees.be/publications/modele-de-registe-des-activites-de-traitement.xls> >. Acesso em 06/07/2020.

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

SUBCATEGORIA	DESCRIÇÃO (Descrever se são tratados dados pessoais sobre:)
7.2.7 - Detalhes da apólice de seguro	Natureza da apólice de seguro, detalhes sobre os riscos cobertos, valores segurados, período segurado, data de rescisão, pagamentos feitos, recebidos ou perdidos, situação do contrato, etc.
7.2.8 - Detalhes do plano de pensão	Data efetiva do plano de pensão, natureza do plano, data de término do plano, pagamentos recebidos e efetuados, opções, beneficiários, etc.
7.2.9 - Transações financeiras	Valores pagos e a pagar pelo titular dos dados, linhas de crédito concedidas, avais, forma de pagamento, visão geral do pagamento, depósitos e outras garantias, etc.
7.2.10 - Compensação	Detalhes sobre compensações reivindicadas, valores pagos ou outros tipos de compensação, etc.
7.2.11 - Atividades profissionais	Atividades profissionais executadas pelo titular dos dados: natureza da atividade, natureza dos bens ou serviços utilizados ou entregues pela pessoa no registro, relações comerciais, etc.
7.2.12 - Acordos e ajustes	Detalhes sobre acordos ou ajustes comerciais; acordos sobre representação ou acordos legais, etc.
7.2.13 - Autorizações ou consentimentos	Autorizações ou consentimentos realizados pelo titular de dados, etc.
CATEGORIA: 7.3 - Características Pessoais	
7.3.1 - Detalhes pessoais	Idade, sexo, data de nascimento, local de nascimento, estado civil, nacionalidade.
7.3.2 - Detalhes militares	Situação militar, patente militar, distinções militares, etc.
7.3.3 - Situação de Imigração	Detalhes sobre o visto, autorização de trabalho, limitações de residência ou movimentação, condições especiais relacionadas à autorização de residência, etc.
7.3.4 - Descrição Física (informações físicas de uma pessoa com possibilidade de serem visivelmente identificadas.)	Altura, peso, cor do cabelo, cor dos olhos, características distintivas, etc.
CATEGORIA: 7.4 - Hábitos Pessoais	
7.4.1 - Hábitos	Uso de tabaco, uso de álcool, hábito alimentar, dieta alimentar etc.

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

SUBCATEGORIA	DESCRIÇÃO (Descrever se são tratados dados pessoais sobre:)
7.4.2 - Estilo de vida	Informações sobre o uso de bens ou serviços, comportamento dos titulares dos dados, etc.
7.4.3 - Viagens e deslocamentos	Antigas residências e deslocamentos, visto de viagem, autorizações de trabalho, etc.
7.4.4 - Contatos sociais	Amigos, parceiros de negócios, relacionamentos com pessoas que não sejam familiares próximos; etc.
7.4.5 - Posses	Terra, propriedade ou outros bens.
7.4.6 - Denúncias, incidentes ou acidentes	Informações sobre um acidente, incidente ou denúncia na qual o titular dos dados está envolvido, a natureza dos danos ou ferimentos, pessoas envolvidas, testemunhas, etc.
7.4.7 - Distinções	Distinções civis, administrativas ou militares.
7.4.8 - Uso de mídia	Definição do comportamento de uso de mídias e meios de comunicação.
CATEGORIA: 7.5 - Características Psicológicas	
7.5.1 - Descrição Psicológica	Personalidade ou caráter.
CATEGORIA: 7.6 - Composição Familiar	
7.6.1 - Casamento ou forma atual de coabitação	Nome do cônjuge ou companheiro(a), nome de solteira do cônjuge ou companheira, data do casamento, data do contrato de coabitação, número de filhos, etc.
7.6.2 - Histórico conjugal	Casamentos ou parcerias anteriores, divórcios, separações, nomes de parceiros anteriores.
7.6.3 - Familiares ou membros da família	Detalhes de outros familiares ou membros da família do titular de dados.
CATEGORIA: 7.7 - Interesses de lazer	
7.7.1 - Atividades e interesses de lazer	Hobbies, esportes, outros interesses.
CATEGORIA: 7.8 - Associações	
7.8.1 Associações (exceto profissionais, políticas, em sindicatos ou qualquer outra associação que se enquadre em dados pessoais sensíveis)	Participação em organizações de caridade ou benevolentes, clubes, parcerias, organizações, grupos, etc.
CATEGORIA: 7.9 - Processo Judicial/Administrativo/Criminal	

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

SUBCATEGORIA	DESCRIÇÃO (Descrever se são tratados dados pessoais sobre:)
7.9.1 - Suspeitas	Suspeitas de violações, conexões conspiratórias com criminosos conhecidos. Inquéritos ou ações judiciais (civis ou criminais) empreendidas por ou contra o titular dos dados, etc.
7.9.2 - Condenações e sentenças	Condenações e sentenças, etc.
7.9.3 - Ações judiciais	Tutela, guarda temporária ou definitiva, interdição, adoção, etc.
7.9.4 - Penalidades Administrativas	Multas, processo disciplinar, advertências, bem como qualquer outro tipo de penalidade ou sanção administrativa prevista em leis, normas e regulamentos.
CATEGORIA: 7.10 - Hábitos de Consumo	
7.10.1 - Dados de bens e serviços	Bens e serviços vendidos, alugados ou emprestados ao titular dos dados.
CATEGORIA: 7.11 - Dados Residenciais	
7.11.1 - Residência	Natureza da residência, propriedade própria ou alugada, duração da residência nesse endereço, aluguel, custos, classificação da residência, detalhes sobre a avaliação, nomes das pessoas que possuem as chaves.
CATEGORIA: 7.12 - Educação e Treinamento	
7.12.1 - Dados acadêmicos/escolares	Diplomas, certificados obtidos, resultados de exames, avaliação do progresso dos estudos, histórico escolar, grau de formação, etc.
7.12.2 Registros financeiros do curso/treinamento	Taxas de inscrição e custos pagos, financiamento, formas de pagamento, registros de pagamento, etc.
7.12.3 - Qualificação e experiência profissional	Certificações profissionais, interesses profissionais, interesses acadêmicos, interesses de pesquisas, experiência de ensino, etc.
CATEGORIA: 7.13 - Educação e Treinamento	
7.13.1 - Emprego atual	Empregador, descrição do cargo e função, antiguidade, data de recrutamento, local de trabalho, especialização ou tipo de empresa, modos e condições de trabalho, cargos anteriores e experiência anterior de trabalho no mesmo empregador, etc.

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

SUBCATEGORIA	DESCRIÇÃO (Descrever se são tratados dados pessoais sobre:)
7.13.2 - Recrutamento	Data de recrutamento, método de recrutamento, fonte de recrutamento, referências, detalhes relacionados com o período de estágio, etc.
7.13.3 - Rescisão de trabalho	Data de rescisão, motivo, período de notificação, condições de rescisão, etc.
7.13.4 - Carreira	Emprego anterior e empregadores, períodos sem emprego, serviço militar, etc.
7.13.5 - Absentismo e disciplina	Registos de absentismo, motivos de ausência, medidas disciplinares, etc.
7.13.6 - Avaliação de Desempenho	Avaliação de desempenho ou qualquer outro tipo de análise de qualificação ou habilidades profissionais, etc.
CATEGORIA: 7.14 -Registros/gravações de vídeo, imagem e voz	
7.14.1 - Vídeo e imagem	Arquivos de vídeos, fotos digitais, fitas de vídeo, etc.
7.14.2 - Imagem de Vigilância	Imagens e/ou vídeos de câmeras de segurança/vigilância (ex: CFTV), etc.
7.14.3 - Voz	Fitas e arquivos digitais de voz, bem como outros registros de gravações de voz, etc.
CATEGORIA: 7.15 -Outros (Especificar)	
7.15.1 - Outros (Especificar)	Obs.: Conforme explicado na seção 2.7, a lista não é exaustiva. Assim, pode incluir quantas outras categorias e subcategorias que forem necessárias.

ANEXO II

Mudanças da Versão 2.0

Este anexo tem a finalidade de fornecer os destaques das mudanças inseridas nesta versão do Guia de Elaboração Inventário de Dados Pessoais.

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

Foram realizadas inclusões de: seção sobre aviso preliminar e agradecimentos; e referência de que controle e medidas do Framework de Privacidade e Segurança da Informação são atendidos pelo Guia de Elaboração do IDP.

Cumpré destacar os 32 Controles de Privacidade e Segurança da Informação trazidos pelo Guia do Framework que foram inseridos na ferramenta em formato de planilha eletrônica, disponível no link < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/template_inventario_dados_pessoais.xlsx>.

A listagem geral dos controles é apresentada na guia “4-Listas” da ferramenta constante da planilha eletrônica disponível em < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/template_inventario_dados_pessoais.xlsx>.

Os 32 novos Controles de Privacidade e Segurança da Informação substituem as antigas 23 Medidas de Segurança trazidas na versão anterior que eram baseadas no Guia de Avaliação de Riscos de Segurança e Privacidade v1 (p. 10 e 11) publicado pela SGD em novembro de 2020.

A Tabela a seguir apresenta os 32 novos controles e as 23 antigas medidas.

Controles de Privacidade e Segurança da Informação (Guia do Framework de Privacidade e Segurança da Informação)	Medidas de Segurança (Guia de Avaliação de Riscos de Segurança e Privacidade)
ESTRUTURAÇÃO BÁSICA DE GESTÃO EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO	
Controle 0: Estruturação básica de gestão em privacidade e segurança da informação	
CIBERSEGURANÇA / SEGURANÇA	
Controle 1: Inventário e Controle de Ativos Institucionais	Continuidade de Negócio
Controle 2: Inventário e Controle de Ativos de Software	Controles Criptográficos
Controle 3: Proteção de Dados	Controles de Acesso Lógico
Controle 4: Configuração Segura de Ativos Institucionais e Software	Controles de Segurança em Redes, Proteção Física e do Ambiente

GUIA DE ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS

Controles de Privacidade e Segurança da Informação (Guia do Framework de Privacidade e Segurança da Informação)	Medidas de Segurança (Guia de Avaliação de Riscos de Segurança e Privacidade)
Controle 5: Gestão de Contas	Cópia de Segurança
Controle 6: Gestão do Controle de Acesso	Desenvolvimento Seguro
Controle 7: Gestão Contínua de Vulnerabilidades	Gestão de Capacidade e Redundância
Controle 8: Gestão de Registros de Auditoria	Gestão de Mudanças
Controle 9: Proteções de E-mail e Navegador Web	Gestão de Riscos
Controle 10: Defesas Contra <i>Malware</i>	Registro de Eventos, Rastreabilidade e Salvaguarda de Logs
Controle 11: Recuperação de Dados	Segurança Web
Controle 12: Gestão da Infraestrutura de Rede	Resposta a Incidente
Controle 13: Monitoramento e Defesa da Rede	
Controle 14: Conscientização e Treinamento de Competências sobre Segurança	
Controle 15: Gestão de Provedor de Serviços	
Controle 16: Segurança de Aplicações	
Controle 17: Gestão de Resposta a Incidentes	
Controle 18: Testes de Invasão	
PRIVACIDADE	
Controle 19: Inventário e Mapeamento	Abertura, Transparência e Notificação
Controle 20: Finalidade e Hipóteses Legais	<i>Compliance</i> com a Privacidade
Controle 21: Governança	Consentimento e Escolha
Controle 22: Políticas, Processos e Procedimentos	Controle de Acesso e Privacidade
Controle 23: Conscientização e Treinamento	Legitimidade e Especificação de Propósito
Controle 24: Minimização de Dados	Limitação de Coleta
Controle 25: Gestão do Tratamento	Minimização de Dados
Controle 26: Acesso e Qualidade	Participação Individual e Acesso
Controle 27: Compartilhamento, Transferência e Divulgação	Precisão e qualidade
Controle 28: Supervisão em Terceiros	Responsabilização
Controle 29: Abertura, Transparência e Notificação	Uso, Retenção e Limitação de Divulgação
Controle 30: Avaliação de Impacto, Monitoramento e Auditoria	
Controle 31: Segurança Aplicada à Privacidade	

