Regras para Compartilhamento de Dados

CCGD
Comitê Central de Governança de Dados

Versão 1 - 04/05/2020

1 Sumário

2 Introdução

Este documento foi elaborado pelo Comitê Central de Governança de Dados, segundo os artigos 21 e 31 do Decreto nº 10.046, de 9 de outubro de 2019. As orientações presentes são válidas para o compartilhamento de dados entre os órgãos e as entidades da administração pública federal direta, autárquica e fundacional e os demais Poderes da União.

Este documento não se aplica ao compartilhamento de dados com os conselhos de fiscalização de profissões regulamentadas e com o setor privado.

Este documento poderá ser alterado para se adequar às regulamentações e orientações produzidas pela Autoridade Nacional de Proteção de Dados – ANPD, quando isso ocorrer.

A redução nos obstáculos para troca de dados entre as agências governamentais visa potencializar o uso da informação para orientar melhorias nos serviços prestados aos cidadãos. Entre os benefícios esperados, destacam-se:

A. **Redução nos custos e esforços para levantamento de informações necessárias à gestão governamental.** Atualmente, diversos agentes públicos e processos são empreendidos para levantar informações, gerando uma multiplicidade de iniciativas desarticuladas, ampliando redundâncias, sobreposições e ineficiências. Ao enxergar que informações outros órgãos já dispõem, será mais fácil repensar processos e reaproveitar informações já coletadas.
B. **Melhoria na qualidade dos dados e informações.** Ao reduzir as barreiras para recepção e entrega de informações de outros órgãos, a tendência é que estes optem pela obtenção das fontes de dados mais confiáveis, fidedignas, padronizadas e tempestivas. Naturalmente, as bases de dados mais qualificadas e certificadas tenderão a ser as mais requisitadas e prevalentes, fortalecendo as melhores práticas de coleta e processamento das informações e estimulando melhorias na forma como estes são gerados e mantidos.
C. **Maior transparência aos cidadãos, quanto a forma como seus dados são mantidos e compartilhados pelos órgãos públicos.** Atualmente, não há procedimentos e práticas comuns e transparentes sobre como os dados dos cidadãos podem ser compartilhados e mantidos pelas agências governamentais. Diversos são os níveis de maturidade organizacional e as formas como tratam esses dados. Com as diretrizes de compartilhamento, os órgãos passam a ter orientação comum, fundamentada em padrões de segurança e boas práticas de governança.
D. **Qualificação do processo decisório nos diversos níveis das agências governamentais, em prol da melhoria dos serviços públicos ao cidadão.** A obtenção e disponibilização de informações com mais facilidade, velocidade e confiança, constitui condição essencial para promoção de uma nova cultura de gestão, em que as decisões são tomadas com base em evidências. O uso de informações contextualizadas, integradas e tempestivas deve ampliar a capacidade de diagnóstico dos problemas públicos, oferecer novos insights para desenho de políticas, práticas e procedimentos, viabilizar ações de monitoramento, auditoria e avaliação de programas governamentais, estimular inciativas inovadoras, entre outros benefícios.

3 Objetivos

O objetivo deste trabalho é facilitar o compartilhamento de dados dentro do governo esclarecendo conceitos e procedimentos operacionais básicos para cumprimento do Decreto 10.046/2019. Nesta fase, três frentes estão sendo abordadas:

- Reduzir a ambiguidade das normas legais existentes
- Categorizar dados para facilitar o compartilhamento de dados
- Adequar os requisitos de segurança para o compartilhamento de dados

3.1 Reduzir a ambiguidade

As normas de restrição de acesso a dados presentes na legislação definem quais dados devem ter seu acesso controlado e como deve ser este controle. Algumas normas, por conterem conceitos jurídicos indeterminados, são abertas. Como exemplo temos o inciso X do art. 5ºda Carta Magna, ao prever que: "X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". Não é possível aferir de pronto o alcance dos termos "inviolável", "intimidade", "vida privada", "honra" e "imagem".

É objetivo deste trabalho buscar diminuir a incerteza na aplicação e na interpretação de normas relacionadas ao compartilhamento de dados dentro do governo, em especial em três aspectos:

Definição de informação a ser protegida	Embora exista a interpretação de que, em face do disposto inciso X do art. 5º da Constituição Federal, toda a informação pessoal deve ter seu acesso ~~a~~ restrito. Isso conflita com outras normas e princípios, como o da publicidade da informação do governo, e com práticas sociais que publicam, por exemplo, resultados de provas e concursos. É necessário fornecer orientações mais precisas a gestores de dados para que estes possam definir se os dados sob sua gestão são públicos ou não.
Detalhamento de regras de restrição de acesso	As previsões de restrição de acesso a serem aplicadas também a determinadas informações são pouco detalhadas nas normas legais. A legislação apenas estabelece comandos de que determinadas informações "são invioláveis" (inciso X do art. 5º da Constituição de 1988), que em relação a elas se deve "assegurar sigilo" (art. 50 da Lei nº 8.112/90), "guardar sigilo" (art. 116, VIII, da Lei nº 8.112/90 e § ~~2~~3º do art. 26 da Lei nº 10.180/01) e "assegurar a proteção da informação sigilosa e da informação pessoal" (art. 6º, III da Lei nº 12.527/11). Contudo, nenhuma dessas normas detalha o que é ser inviolável, assegurar ou guardar sigilo, ou assegurar a proteção.
Melhor clareza das regras de compartilhamento dentro do governo	As informações protegidas não podem ser de livre acesso ~~mostradas~~ para a sociedade e o seu tratamento dentro do governo é variado. Muitas são compartilhadas regularmente, outras não. Hoje não temos clareza sobre quais informações podem ser compartilhadas dentro do governo nem sobre como fazê-lo.

Além, de reduzir ambiguidades, outro objetivo é criar consensos e padrões.

Mesmo tratamento no acesso a informações	Fazer com que informações iguais tenham o mesmo tratamento em todos os órgãos.
Procedimentos de segurança semelhantes	Adotar procedimentos de segurança da informação semelhantes em todos os órgãos e entidades governamentais.

3.2 Categorizar compartilhamento

A categorização visa separar os compartilhamentos em três grandes grupos: amplo, restrito e específico. Na verdade. Isso já é uma prática em muitos órgãos, mesmo que com outros nomes.

Amplo são os dados que deveriam estar ~~na~~ em transparência ativa, ou que são cedidos sempre que solicitados pelo SIC – Serviço de Informações ao Cidadão. Trocá-los entre órgãos não é um problema, geralmente.

Os demais tipos são dados que possuem normas afirmando que são protegidos de ampla divulgação ou sigilosos, que não podem ser publicados. Mas isso não implica, ou proíbe, que sejam compartilhados dentro do governo. Os órgãos geralmente separam esses dados em dois grupos. O primeiro é o que habitualmente é cedido aos órgãos públicos, sem uma análise profunda de seu uso. Isso se deve, geralmente, ao baixo risco associado a essas informações. O segundo é um grupo de informações críticas, capazes de trazer problemas graves para seus titulares ou para o órgão. Até hoje esses dois grupos estavam sob as mesmas regras. A categorização pretende separá-los.

O gestor de dados irá decidir quais informações estão em cada grupo, usando as orientações desse documento e da aplicação das normas legais.

Os dados Restritos são aqueles que podem ser fornecidos a outro órgão sempre que solicitado, prescindindo de avaliação prévia. Esses terão um processo de acesso simples e padronizados por todos os órgãos. Esses procedimentos serão definidos pelo Comitê Central de Governança de Dados.

O grupo ao qual o acesso será analisado, podendo ser recusado eventualmente ou mesmo sempre, é o dos dados Específicos. Estes são de inteira responsabilidade do gestor de dados, tanto para os critérios de análise da permissão quanto para o processo de acesso.

3.3 Adequar os requisitos de segurança

É obrigatório aos órgãos e entidades, ao solicitar os dados restritos das bases, declarar que se comprometerão a cumprir os requisitos de segurança estipulados para o nível de compartilhamento restrito, conforme o Art. 12, § 1º do Decreto nº 10.046/2019.

Fornecedores das bases de dados, recebedores ou autoridades de auditoria competentes poderão auditar o cumprimento dos requisitos de segurança descritos neste documento.

4 Gestor de dados, Área de TI e Interlocutor

De acordo conforme o art. 2º, inciso XIII, do Decreto nº 10.046, de 2019, gestor de dados é o órgão ou a entidade responsável pela governança de determinado conjunto de dados. Este deve ser o menor órgão capaz de tomar decisões sobre o conjunto de dados, ou seja, deve-se evitar indicar o topo hierárquico do órgão ou entidade como gestor de todas as bases. Decisões, nesse contexto, não se trata de decisões envolvendo tecnologia, mas decisões gerais sobre a base, o sistema e os processos envolvidos.

Ademais, recomenda-se a indicação de um interlocutor por órgão superior (ministério, secretaria, autarquia, etc.), que deverá, observadas as especificidades do órgão ou entidade:

A. Manter interlocução e participar de eventos formativos promovidos pelo CCGD para obtenção de instruções e esclarecimentos necessários à aplicação do Decreto nº 10.046, de 2019;
B. Apoiar na disseminação interna das regras e orientações para compartilhamento de dados, especialmente, as contidas neste Documento;
C. Consolidar as categorizações de dados realizadas pelos gestores de dados em documento único, conforme modelo descrito no item 7.4 deste Documento, e remeter ao CCGD a cada nova revisão;
D. Consolidar as regras para compartilhamento de dados Restritos e Específicos, conforme definido pelos gestores de dados, e remeter ao CCGD a cada nova revisão~~;~~.

5 Categorias de compartilhamento de dados

A categorização da informação visa reduzir ambiguidades sobre os dados referidos nas normas legais.

A categorização, e suas implicações, somente se aplicam a informações que estão custodiadas pelo governo, sejam coletadas, sejam produzidas por este.

Estão definidas três categorias no Decreto 10.046 de 2019:

Categoria	Descrição	Regras de compartilhamento
Ampla	Dados não protegidos por norma, portanto públicos.	Dispensa autorização prévia pelo gestor de dados e será realizada pelos canais existentes para dados abertos e transparência ativa. (art. 11)
Restrita	Dados protegidos por norma e compartilhados dentro do governo sem necessitar permissão.	Regras estabelecidas pelo Comitê Central de Governança de Dados. (art. 12)
Específica	Dados protegidos por norma, cujo compartilhamento depende de decisão do gestor de dados.	Condicionado à permissão de acesso pelo gestor de dados e ao atendimento dos requisitos definidos por este como condição para o compartilhamento. (art. 14) Os dados recebidos por compartilhamento específico não serão retransmitidos ou compartilhados com outros órgãos ou entidades, exceto quando previsto expressamente na autorização concedida pelo gestor de dados ou se houver posterior permissão desse (art. 12, §2º).

6 Regras e requisitos de Compartilhamento

6.1 Regras gerais

1. Recomenda-se priorizar a categorização os dados seguindo a seguinte ordem:
   1.1. Primeiro os dados estruturados, depois os não estruturados.
   1.2. Primeiro as informações mais solicitadas, depois as demais informações.
2. Os dados que forem categorizados como Restritos ou Específicos devem ter uma justificativa para tal categorização.
3. Os órgãos que recebem dados deverão manter um histórico de que bases receberam e de quais órgãos.
4. Identificação de pessoa física
   4.1. Todas as identificações de pessoas físicas na categoria Ampla serão com nome e CPF mascarado no formato ***.999.999-** .
   4.2. Todas as identificações de pessoas físicas na categoria Restrita e Específica serão com nome e CPF completo e todos os demais identificadores disponíveis (PIS, Carteira de trabalho, PASEP, Identidade estadual, etc.).
5. Identificação de pessoa jurídica
   5.1. Todas as identificações de pessoas jurídicas, em qualquer categoria, serão com nome e CNPJ.
6. Dados recebidos não devem ser recategorizados. Vale a categorização recebida.
7. Caso a categorização de um conjunto de dados mude com o tempo, os dados já distribuídos e presentes em outros órgãos também mudarão.
8. No caso de dados combinados - isto é, aqueles constituídos pela junção de um ou mais conjunto de dados, quando não for viável sua separação, para efeito de categorização, deve-se classificar o conjunto na categoria mais privativa.
9. Os dados recebidos por compartilhamento restrito poderão ser retransmitidos ou compartilhados com outros órgãos ou entidades que comprovem a necessidade de acesso, exceto se proibido expressamente na autorização concedida pelo gestor de dados ou se houver posterior revogação da permissão desse, mediante fundamentação, nas duas hipóteses (art. 12. § 4º, do Decreto 10.046/2019).
10. Qualquer retransmissão e compartilhamento de dados continuam sujeitos aos termos do Decreto 10.046/2019, inclusive entre as entidades abrangidas: órgãos e as entidades da administração pública federal direta, autárquica e fundacional.
11. Prazos
    11.1. Em consonância com o art. 9 do Decreto 10.046, atendidos os critérios necessários ao compartilhamento, o acesso aos dados ocorrerá no prazo de trinta dias, contado da data da solicitação. Neste caso:
       11.1.1. Dados de categorização Ampla deverão ser entregues em 30 dias, ~~visto que não há critérios a serem tendidos~~ observada a legislação vigente.
       11.1.2. Dados de categorização Restrita deverão ser entregues em 30 dias após atenderem as regras desse documento.
       11.1.3. Dados de categorização Específica, caso seja concedida a permissão de acesso pelo gestor dos dados, ~~Restrita~~ deverão ser entregues em 30 dias após atenderem as regras definidas pelo gestor dos dados.
    11.2. No caso de solicitação a dados de Categorização Específica, o órgão gestor dos dados deverá se manifestar sobre a solicitação no prazo de 30 dias (art. 15, §2º).
12. Casos não previstos deverão ser encaminhados a CCGD.

6.2 Dados Restritos

São dados restritos aqueles que o órgão entende que podem ser acessados por todos os órgãos e entidades da Administração Pública Federal (APF), sem a necessidade de analisar pedidos e emitir permissões para cada caso. Não emitir permissão não deve ser confundido com não ter controle sobre acessos, como a rastreabilidade destes acessos.

Regras para Compartilhamento Restrito

1. **Ponto de contato.** O gestor de dados deve indicar o ponto de contato (órgão com telefone e e-mails institucionais) para informações sobre as bases. Este ponto de contato pode ser único para todo o órgão ou por base de dados. Este contato deve ser da área que irá fornecer o acesso, incluindo a área de TI ou da empresa pública onde os dados estão hospedados.

2. **Identificação do Solicitante.** O solicitante deve enviar um ofício indicando seu interesse nos dados e finalidade do acesso. Este ofício deve ser assinado por um dirigente do órgão, designado pela Alta Administração do órgão ou entidade, e é suficiente para a identificação do solicitante como representante de órgão ou entidade pública federal.

3. **Controle de acessos feitos.** O gestor de dados deverá manter um controle sobre todos os órgãos que acessam os seus dados. Esse controle deve prever plataformas de interoperabilidade e repasses de informação entre órgãos. Nessa fase, este controle deverá incluir, no mínimo todos os novos pedidos. Posteriormente, serão tratados os acessos anteriores.

4. **Formulários de acesso.** A chefia do solicitante deverá preencher um termo de responsabilidade com as seguintes informações:

    4.1. Órgão solicitante com nome, endereço, nome do titular e substituto e telefones e e-mails respectivos.

    4.2. Motivo da solicitação. Descrição do motivo da solicitação e do uso que será feito dos dados em conformidade com o art. 23 da Lei nº 13.709, de 2018. Essa descrição não será motivo para recusa de acesso, mas o órgão poderá ser advertido, pelo gestor de dados ou pelo CCGD, em caso de descrições vagas ou improcedentes.

    4.3. Compromisso da chefia de gerenciamento dos servidores do órgão solicitante que acessarão os dados.

    4.4. Os termos de compromisso serão enviados ao gestor de dados, ou quem este indicar.

Requisitos de segurança

1. DEFINIÇÕES

    1.1. ATIVO - qualquer coisa que tenha valor para a organização; Fonte: Portaria GSI/PR nº 93/2019 - Glossário de Segurança da Informação.

    1.2. ATIVOS DE INFORMAÇÃO - os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso; Fonte: Portaria GSI/PR nº 93/2019 - Glossário de Segurança da Informação.

1.3. EVENTO DE SEGURANÇA - qualquer ocorrência identificada em um sistema, serviço ou rede que indique uma possível falha da política de segurança, falha das salvaguardas ou mesmo uma situação até então desconhecida que possa se tornar relevante em termos de segurança; Fonte: Portaria GSI/PR nº 93/2019 - Glossário de Segurança da Informação.

1.4. 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. - Fonte: Portaria GSI/PR nº 93/2019 - Glossário de Segurança da Informação; BRASIL. Lei nº 13.509, de 14 de Agosto de 2018, art. 5º, inciso X.

2. CLÁUSULAS GERAIS

2.1. O tratamento de dados realizado por terceiro (empresa contratada) e pelos recebedores de dados deverão possuir os controles definidos neste documento.

2.2. O disposto no item 2.1 não exclui ou reduz a responsabilidade do órgão, o qual responderá de forma solidária pelos danos causados aos titulares dos dados em caso de negligência na fiscalização dos controles de segurança da informação.

2.3. Os órgãos e os recebedores de dados, no âmbito de suas competências e de acordo com a criticidade do dado tratado, poderão estabelecer outros controles de segurança da informação, regras e boas práticas e outros aspectos relacionados à segurança da informação, além dos definidos neste documento.

2.4. – As interfaces utilizadas na integração dos componentes de software devem dispor de controles que assegurem a confidencialidade, integridade e autenticidade das informações.

3. MECANISMOS GERAIS

3.1. Possuir Política de Segurança da Informação ou equivalente, vigente e atualizada, com processo de revisão periódica formalizado e institucionalizado, conforme norma complementar nº 03/IN01/DSIC/GSIPR do Gabinete de Segurança da Informação da Presidência da República.

3.2. Possuir Matriz de Responsabilidade que defina claramente as responsabilidades associadas ao tema segurança da informação para cada unidade organizacional interna e para fornecedores externos.

3.3. Firmar acordos de confidencialidade e não divulgação que reflitam a criticidade dos dados tratados com terceiros e outros órgãos que venha a retransmitir os dados compartilhados.

4. MONITORAMENTO DOS ATIVOS DE INFORMAÇÃO

4.1. Realizar análise/avaliação de riscos dos ativos de informação.

4.1.1. Realizar a gestão de vulnerabilidades dos ativos de informação com elaboração de plano de ação para corrigi-las ou mitigá-las, cronograma de cumprimento e evidência das correções aplicadas.

4.2. Utilizar recursos de segurança da informação e de tecnologia da informação em versões comprovadamente seguras e atualizadas.

5. SEGURANÇA DA INFRAESTRUTURA INTERNA

5.1. Segmentar a rede corporativa em domínios lógicos de forma a proteger as informações internas e acessos indevidos.

5.2. Utilizar mecanismos de detecção e prevenção de ataques cibernéticos (ex.: ataque de negação de serviço, DDOS, *malware*, *phishing*, etc.).

5.3. Implementar mecanismos de controle de segurança de rede e estações de trabalho.

5.4. Implementar mecanismos para que informações sobre o órgão (infraestrutura e pessoas) não sejam expostas de forma inadvertida ou sem os devidos cuidados de forma a evitar a coleta de informações que possam ser utilizadas em um ataque.

5.5. Segregar ambientes tecnológicos de desenvolvimento, teste, homologação e produção.

5.6. Implementar controles e procedimentos para assegurar a segurança física e do ambiente de acesso às bases, informações, sistemas e demais ativos que utilizem os dados compartilhados.

6. COMUNICAÇÃO

6.1. Utilizar criptografia na ~~de~~ transmissão de dados.

6.2. Aplicar mecanismo de filtragem da conexão de origem por conjunto de endereços de IP atribuídos aos órgãos fornecedores dos dados.

7. PADRÕES CRIPTOGRÁFICOS

7.1. Realizar o gerenciamento e distribuição de chaves criptográficas de forma segura (Norma Complementar 09/IN01/DSIC/GSI/PR de 2014).

8. CONTROLE DE ACESSO

8.1. Habilitar, de forma restrita, somente serviços e sistemas de acesso dos órgãos receptores dos dados, com vias a restringir o acesso apenas aos órgãos/usuários devidamente autorizados.

8.2. A política de controle de acesso deve

8.2.1. definir claramente as responsabilidades/papéis dos intervenientes desse processo e:

8.2.2. atender ao princípio do menor privilégio;

8.2.3. possuir perfis de acesso bem definidos e regras claras para habilitação, suspensão e revogação de direitos de acesso e que trate:

8.2.3.1. o controle de acesso aos registros de eventos (logs);

8.2.3.2. o controle de acesso às configurações dos sistemas (perfis administrativos);

8.2.3.3. o controle de acesso às cópias de segurança;

8.2.3.4. o controle de acesso às informações sensíveis e situações que requeiram a propriedade do não-repúdio e o acesso via certificado digital; e

8.2.3.5. os processos formais para a solicitação de acesso aos perfis dos sistemas, permitindo verificar, inclusive, os autorizadores que concederam as permissões ao usuário.

8.3. Realizar periodicamente a revisão dos direitos de acesso.

8.4. Política de senha forte.

8.5. Armazenar as senhas em ambiente controlado e seguro.

9. REGISTRO DE EVENTOS

9.1. Registrar eventos de transações, usuários e infraestrutura.

9.2. Implementar mecanismos de proteção dos logs contra perda, destruição, falsificação e acesso não autorizado.

9.3. Manutenção dos registros dos eventos de segurança.

10. GESTÃO DE INCIDENTES (PAUTA 2020)

10.1. Possuir infraestrutura protegida com firewall.

10.2. Registrar incidentes de segurança contendo as seguintes informações:

10.2.1. descrição dos incidentes ou eventos;

10.2.2. informações e sistemas envolvidos;

10.2.3. medidas técnicas e de segurança utilizadas para a proteção das informações;

10.2.4. procedimentos para a identificação, coleta, aquisição e preservação das informações, as quais podem servir como evidências;

10.2.5. riscos relacionados ao incidente; e

10.2.6. as medidas tomadas para mitigá-los e evitar reincidências.

10.3. Elaborar Plano de ~~Comunicação~~ Gerenciamento de Incidentes que estabeleça responsabilidades e procedimentos, de forma a assegurar respostas rápidas, efetivas e ordenadas e que estabeleçam a comunicação de ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares com o gestor da base afetada; com o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR-GOV) do Gabinete de Segurança Nacional da Presidência da República (GSI/PR); e com a Autoridade Nacional de Proteção de Dados, conforme art. 48 da Lei Geral de Proteção de Dados.

6.3 Dados Específicos

Os dados específicos somente são acessíveis em caso de permissão do gestor de dados. Critérios para aprovar ou recusar acesso, bem como detalhes do processo, são de total responsabilidade do gestor dos dados.

Regras gerais

1. **Ponto de contato**. O gestor de dados deve indicar um ponto de contato (órgão com telefone e e-mails institucional) para informações sobre as bases. Este ponto de contato pode ser único para todo o órgão ou por base de dados.

2. **Regras de acesso**, opcional. O gestor pode publicar antecipadamente regras esclarecendo em que casos, e para quais entidades, é concedido acesso a dados ou não. É recomendável para reduzir pedidos que não poderão ser atendidos.

3. **Controle de acessos feitos**. O gestor de dados deve manter histórico de todos os órgãos que acessam os dados. Nessa fase, este controle deve incluir, no mínimo, todos os novos acessos. Posteriormente serão tratados os acessos anteriores.

7 Categorização

A categorização dos dados é decidida pelo gestor de dado. Para isso ele deve seguir os seguintes passos:

- Rigor na aplicação das normas legais – qualquer categorização deve estar totalmente de acordo com as normas legais existentes.
- Conhecimento sobre a base – o gestor é aquele que tem o melhor conhecimento sobre as bases de dados e é o mais capaz para categorização, pois ele conhece as particularidades de sua base e as consequências de um possível vazamento.
- Maior dano potencial – nos casos onde as normas são ambíguas, deve se aplicar uma restrição proporcional ao dano que pode ser causado por um vazamento da informação. Quanto maior o dano, maior o nível de restrição. O dano pode ser moral, financeiro, legal ou de qualquer outra natureza.
- Inclusão em subcategoria – as subcategorias listadas no sibitem 7.4 deste documento são uma orientação para categorizar os dados. O gestor deve escolher uma subcategoria que descreva seus dados. No entanto, mesmo que suas informações estejam de acordo com uma subcategoria, caso o gestor conheça aspectos particulares de suas bases de dados, pode não usar essa subcategoria.

7.1 Tipos de informações

O gestor irá categorizar três tipos de informações

- Conjunto de informações – são grupos de informações identificadas por um título. Exemplos: endereços de órgão público, dados de um veículo, itens de compras governamentais, etc. O título deve ser suficiente para esclarecer que informações estão, ou não incluídas. Uma opção é explicitar as informações entre parênteses. Exemplos: cabeçalho de compras governamentais (nome e CNPJ do vendedor, data da venda, valor total, lista de itens, data de entrega, órgão comprador), dados de um veículo (fabricante, modelo e ano), etc. É possível também excluir informações. Exemplo: óbito (não inclui motivo do óbito).
- Canais de acesso – são os canais existentes para acessar as informações incluindo *WebServices, APIs, download*, etc.
- Atributos de tabelas – são os campos das tabelas nas bases de dados.

Essas informações serão fornecidas pelo gestor, mas consulte o calendário das versões.

7.2 Como categorizar

Categorizar significa enquadrar um conjunto de informações nas categorias Ampla, Restrita ou Específica, podendo se utilizar da lista de subcategorias contidas no subitem 7.4 deste documento.

Alguns exemplos

1. Exemplo 1: resultados de concursos públicos.
    a. Na categoria AMPLA existe uma subcategoria “A01 - Informação gerada, ou publicada, em evento público” na qual resultados de concursos de encaixa. Então o gestor irá colocar “resultados de concursos públicos” no campo “conjunto de informações” da subcategoria “A01 - Informação gerada, ou publicada, em evento público”. Isso implica que as informações contidas em “resultados de concursos públicos” estão na categoria AMPLA.
2. Exemplo 2: informações misturadas de servidor público.
    a. Embora muitas informações do servidor público sejam públicas, nem todas são. Neste caso o gestor deve separar um conjunto de informações públicas e categoriza-las como Ampla. Outros conjuntos, poderão ser categorizados como Restritos ou Específicos. Se a separação não viável, deve-se optar pela categoria mais limitante.
3. Exemplo 3: informações de atividades de segurança.
    a. Informações ligadas à segurança de pessoas em situações particulares podem acarretar risco para sua integridade física ou para a administração pública. Vão desde a lotação de fiscais em áreas fronteiriças a pessoas incluídas no programa de proteção à testemunha. Neste caso deve-se optar por E06 (Informações que coloquem pessoas em risco).

7.3 Subcategorias - estrutura

O gestor irá incluir suas informações dentro de uma subcategoria. Ao fazer essa inclusão, a informação já está categorizada.

	CATEGORIA	
Cod	**Subcategoria**	
	Definição	
	Conjunto de informações	
	Canais de acesso	
	Atributos de tabelas	

- Categoria – identifica a qual categoria pertence essa subcategoria: ampla, restrita ou específica.
- Código – código identificador da subcategoria.
- Subcategoria – contém as informações sobre a subcategoria.
    - Definição – definição da subcategoria.
        - Exemplo de descrição: “Informação sobre o governo incluindo funcionamento, gasto e serviço.”
        - Algumas definições têm esclarecimentos sobre a subcategoria e as informações contidas nela. Exemplo: alguns campos falam em informar o nome de uma pessoa, este campo deve esclarecer se o CPF será fornecido junto.
        - Exemplo de Informações incluídas: “Funcionamento inclui estrutura organizacional, recursos, pessoal (nome e dados funcionais), horários de funcionamento.”
    - Conjunto de informações, Canais de acesso e Atributos de tabelas
        - Campo a ser preenchido pelo gestor de dados em face do conjunto de informações que ele possui em suas bases.

7.4 Subcategorias

Essas são as subcategorias definidas pela CCGD.

	AMPLA	
Cod	Subcategoria	
A01	Definição	**Informação gerada, ou publicada, em evento público.** Exemplo: diploma universitário, informações publicadas no Diário Oficial ou outros documentos públicos oficiais.
	Conjunto de informações	
A02	Definição	**Informação sobre o governo incluindo funcionamento, gasto e serviço.** Exemplos: Funcionamento inclui estrutura organizacional, recursos, pessoal (nome e dados funcionais), horários de funcionamento. Gasto inclui compras governamentais e pagamentos a servidores. Serviço inclui lista de serviços, locais, regras de funcionamento.
	Conjunto de informações	
A03	Definição	**Informações declaradas públicas pelos órgãos competentes com transito em julgado.** Exemplo: informações declaradas públicas pela Comissão Mista de Reavaliação de Informações, pareceres jurídicos ou decisões judiciais.
	Conjunto de informações	
A04	Definição	**Situação de regularidade com a APF de Pessoas Jurídicas.** Exemplo: dívida ativa, certificados, certidões, alvarás, etc. Deverá incluir tipo de regularidade (qual alvará, permissão, etc.), situação (regular, irregular), validade (início e fim, se houver), nome e CNPJ.
	Conjunto de informações	
A05	Definição	**Informações estatísticas.** No caso de informações pessoais anonimizadas não basta retirar identificadores. É necessário garantir que o indivíduo não seja identificado.
	Conjunto de informações	
A06	Definição	**Beneficiários de programas sociais do governo.** Relação de beneficiários diretos de programa social do governo. Informações devem conter no mínimo o nome, CPF mascarado e valor.
	Conjunto de informações	

	RESTRITA	
Cod	Subcategoria	
R01	Definição	**Dados cadastrais** Inclui nome, identificadores (CPF, NIS, título eleitoral, etc), data de nascimento, situação civil, endereço, contatos (telefone, e-mail, etc.), filiação, nome social.
	Conjunto de informações	
R02	Definição	**Situação de regularidade com a APF de Pessoas FISICAS.** Exemplo: CPF, dívida ativa, certificados, certidões, alvarás, etc. Deverá incluir tipo de regularidade (qual alvará, permissão, etc.), situação (regular, irregular), validade (início e fim, se houver), nome e CPF.
	Conjunto de informações	
R03	Definição	**Beneficiários de programas sociais do governo.** Informações completas sobre beneficiários de programa social do governo.
	Conjunto de informações	

Obs: *1 Conforme Regras Gerais (item 6.1, item 9), na Categoria Ampla, a identificação de pessoas é com CPF mascarado. Já nas categorias Restrita e Específica, ela contém o CPF completo e demais identificações disponíveis.

ESPECÍFICA		
Cod	Subcategoria	
E01	Definição	**Informações com restrições legais sobre o compartilhamento intra governo.** Informações cujas restrições legais de controle de acesso façam restrições a compartilhamentos com outros órgãos do governo. Exemplo: CTN restringe acesso a servidores da Fazenda Pública.
	Conjunto de informações	
E03	Definição	**Segurança pública** Informações que comprometam a segurança pública.
	Conjunto de informações	
E04	Definição	**Segurança nacional** Informações que comprometam a segurança nacional.
	Conjunto de informações	
E05	Definição	**Informações internas de sistemas** Informações internas de sistemas que possam ter implicações sobre segurança, incluindo número IP, logs, etc.
	Conjunto de informações	
E06	Definição	**Informações que coloque pessoas em risco** Informações que coloque pessoas em situação de risco, incluindo quantidade de fiscais em postos de fiscalização, localização de bens confiscados, beneficiados do programa de proteção a testemunha, etc.
	Conjunto de informações	
E07	Definição	**Informações médicas** Informações relativas a saúde do cidadão identificado.
	Conjunto de informações	

8 Roteiro para publicação de regras de compartilhamento pelos órgãos

Os órgãos deverão publicar sua própria versão de Regras para Compartilhamento de Dados. Este documento poderá ser publicado por cada órgão separadamente, mas recomenda-se que os órgãos superiores publiquem um consolidado das regras de seus órgãos.

Estão previstas 3 versões do documento, cada versão com uma ampliação do conteúdo.

Versão	Obs
1ª versão	Seguindo o artigo 4 do Decreto 10.046/19.
2ª versão	90 dias após a data de publicação das diretrizes do órgão.
3ª versão	180 dias após a data de publicação das diretrizes do órgão.

Para mais informações sobre datas, contate sgd.dados@planejamento.gov.br.

Conteúdo previstos para as versões.

Conteúdo	1ª versão	2ª versão	3ª versão
Instruções e Contato para Compartilhamento Restrito	X	X	X
Instruções e Contato para Compartilhamento Específico	X	X	X
Categorização de conjuntos de informações	X	X	X
Categorização de maios acessos	--	X	X
Categorização de atributos tabelas	--	--	X

A descrição desses conteúdos está detalhada a seguir.

8.1 Instruções e Contato para Compartilhamento Restrito

Essa seção deve conter instruções para acessar dados categorizados como Restritos. Considerando que o compartilhamento Restrito dispensa permissão, as instruções se resumem ao preenchimento de termos de sigilo e confidencialidade.

Também deve constar dessa seção o contato para solicitar o acesso. O contato deve conter órgão, telefone e e-mail institucional. Este contato pode ser por base de dados ou por órgão.

8.2 Instruções e Contato para Compartilhamento Específico

Essa seção deve conter instruções para solicitar a permissão de acesso a dados categorizados como Específicos. As instruções podem já indicar as restrições de acesso existentes. Como restrições podemos citar o uso exclusivo de dados do censo para fins estatísticos (Lei 5.534/1968 e Lei 5.878/1973) e a vedação a divulgação fora da Fazenda Pública (Lei 5.172/66).

Também deve constar dessa seção o contato para solicitar o acesso. O contato deve conter órgão, telefone e e-mail institucional. Este contato pode ser por base de dados ou por órgão.

8.3 Categorização de conjuntos de informações

Nessa seção serão listados todos os serviços interoperáveis indicando a categorização de cada um. Instruções adicionais serão emitidas pela CCGD sobre essa seção.

8.4 Categorização de meios de acesso e atributos de tabelas

Instruções adicionais serão emitidas pela CCGD sobre essas seções.

9 Publicação

A publicação se dará por meio de portaria, instrução normativa ou documento equivalente.

O interlocutor deverá agrupar as publicações de seus órgãos e enviá-las para CCGD, pelo e-mail sgd.dados@planejamento.gov.br.

A SGD, que manterá, em página WEB, uma relação de todas as normas vigentes sobre categorização.

10 Referências

Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)

Decreto nº 10.046, de 9 de outubro de 2019 - Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001:2013. Tecnologia da Informação - Técnicas de Segurança – Código de Prática para controles de segurança da informação.

Instrução Normativa GSI Nº 1, de 13 de junho de 2008 - Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências

Normas Complementares à Instrução Normativa Nº 01 GSI/PR/2008 - N° 1 a 21

OWASP API Security Top 10 2019 - The Ten Most Critical API Security Risks

Versão 1

Sub versão 14.03 04/05/2020