Instituto Brasileiro de Geografia e Estatística

Auditoria Interna (AUD)

RELATÓRIO DE AVALIAÇÃO

Gestão da Privacidade de Dados em atendimento à Lei Geral de Proteção de Dados (LGPD)

05 de dezembro de 2023

Ministério do Planejamento e Orçamento (MPO)
Fundação Instituto Brasileiro de Geografia e Estatística (IBGE)
Auditoria Interna (AUD)

RELATÓRIO DE AVALIAÇÃO

Objeto: **Gestão da Privacidade de Dados no atendimento à Lei Geral de Proteção de Dados (LGPD)**

Unidade Gestora: **Centro de Documentação e Disseminação de Informações (CDDI) – José Daniel Castro da Silva**

Relatório de Avaliação: 03/2023

Missão

Aumentar e proteger o valor organizacional do IBGE, fornecendo avaliação, assessoria e conhecimentos objetivos e baseados em riscos.

Avaliação

O trabalho de avaliação, como parte da atividade de auditoria interna, consiste na obtenção e na análise de evidências com o objetivo de fornecer opiniões ou conclusões independentes sobre um objeto de auditoria. Objetiva também avaliar a eficácia dos processos de governança, de gerenciamento de riscos e de controles internos relativos ao objeto, e contribuir para o seu aprimoramento.

QUAL FOI O TRABALHO REALIZADO PELA AUD?

A Lei n° 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), estabelece o marco legal para a proteção de informações pessoais, criando um cenário de segurança jurídica, que visa garantir transparência e proteção aos dados pessoais da pessoa natural.

O trabalho de auditoria teve como objetivo avaliar a governança, o gerenciamento de riscos e os controles internos instituídos pelo IBGE para adequação do processo de gestão da privacidade de dados à Lei Geral de Proteção de Dados Pessoais (LGPD), em todos os aspectos relevantes, de acordo com os critérios aplicáveis, em conformidade com as normas e padrões nacionais e internacionais de auditoria no setor público.

Tal tema foi definido como objeto de avaliação no PAINT 2022, mas em que pese o esforço da Auditoria Interna não foi possível a conclusão, tendo a sua continuidade prevista no PAINT 2023.

POR QUE A AUD REALIZOU ESSE TRABALHO?

O processo de Gestão da Privacidade de Dados em atendimento à LGPD foi selecionado a partir da avaliação da Auditoria Interna sobre alguns temas para objetos auditáveis que poderiam ser considerados e priorizados para seleção de trabalhos de auditoria com base em riscos. A Auditoria Interna do IBGE (AUD) encaminhou uma lista de objetos, por meio de formulário eletrônico, aos membros dos Conselhos Diretor e Curador para que pudessem orientar e opinar sobre trabalhos baseados em riscos no PAINT 2022, indicando a priorização sob a ótica da avaliação de riscos estratégico, operacional e de integridade, na qual um dos temas mais pontuados foi a convergência da gestão de privacidade de dados no IBGE à LGPD.

QUAIS AS CONCLUSÕES ALCANÇADAS PELA AUD? QUAIS AS RECOMENDAÇÕES QUE DEVERÃO SER ADOTADAS?

Apesar do esforço, dedicação e comprometimento dos gestores relacionados ao tema, observou-se:

1. Requisitos de privacidade avançaram no IBGE mas não foram totalmente capturados e consolidados de forma a influenciar a gestão dos dados pessoais e o seu ciclo de vida;
2. Inexistência da gestão de dados pessoais na Arquitetura de Processos do IBGE e de processos formalmente constituídos contemplando todas as atividades de trabalho relacionadas à proteção de dados pessoais de forma a subsidiar o Programa de Governança em Privacidade e a necessária análise de riscos;
3. Serviços de consultoria contratados para o diagnóstico, o planejamento, a avaliação da conformidade e o gerenciamento de riscos no âmbito da gestão de proteção de dados pessoais em consonância com a LGPD ainda não se iniciou; e
4. A função de Encarregado de Dados no IBGE poderia possuir dedicação exclusiva e estar desvinculada de qualquer Unidade Operacional.

LISTA DE SIGLAS E ABREVIATURAS

ANPD	Autoridade Nacional de Proteção de Dados Pessoais
AUD	Auditoria Interna do IBGE
CC	Conselho Curador
CD	Conselho Diretor
CDDI	Centro de Documentação e Disseminação de Informações
CTA	Coordenação de Treinamento e Aperfeiçoamento
DE	Diretoria-Executiva
DSIC/GSIPR	Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República.
DPSI/SGD	Departamento de Privacidade e Segurança da Informação da Secretaria de Governo Digital
DTI	Diretoria de Tecnologia da Informação
ENCE	Escola Nacional de Ciências Estatísticas/IBGE
ETIR	Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos
GPG	Gerência de Planejamento e Gestão
GT	Grupo de Trabalho
IBGE	Fundação Instituto Brasileiro de Geografia e Estatística
IN	Instrução Normativa
LGPD	Lei Geral de Proteção de Dados Pessoal
MGI	Ministério da Gestão e da Inovação em Serviços Públicos
MPO	Ministério do Planejamento e Orçamento
MOT	Manual de Orientações Técnicas da Atividade de Auditoria Interna Governamental do Poder Executivo Federal
RCD	Resolução do Conselho Diretor do IBGE
PAINT	Plano Anual de Auditoria Interna
PGP	Programa de Governança em Privacidade
POSIC	Política de Segurança da Informação e Comunicação
PPSI	Programa de Privacidade e Segurança da Informação
PSI	Política de Segurança da Informação
PP	Política de Privacidade de Dados
RIPD	Relatório de Impacto e Proteção de Dados Pessoais
SA	Solicitação de Auditoria

SAPC	Sistema de Administração de Pessoal Censitário
SEDGG/SGD	Secretaria de Gestão e Desempenho de Pessoal da Secretaria de Governo Digital
SDA	Sistema de Dados Administrativos do IBGE
SEI	Sistema Eletrônico de Informação
SGD	Secretaria de Governo Digital
SOC	*Security Operation Center*
SFC/CGU	Secretaria Federal de Controle da Controladoria-Geral da União
TCU	Tribunal de Contas da União

SUMÁRIO

INTRODUÇÃO 8

RESULTADOS DOS EXAMES 11

RECOMENDAÇÕES 23

CONCLUSÃO 27

EQUIPE DE AUDITORIA 31

ANEXO I 32

MANIFESTAÇÃO DA UNIDADE EXAMINADA E ANÁLISE DA EQUIPE DE AUDITORIA 32

INTRODUÇÃO

A Lei n° 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), estabelece o marco legal para a proteção de informações pessoais, criando um cenário de segurança jurídica, que visa garantir transparência e proteção aos dados pessoais da pessoa natural.

De forma geral, a lei requer que as empresas e órgãos públicos (LGPD, artigos 23 ao 30) aperfeiçoem a forma como lidam com dados pessoais e informações sensíveis, prevendo requisitos legais e de segurança da informação, bem como sanções administrativas e pecuniárias àqueles que não se adequarem ao dispositivo (artigos 52 ao 54).

A partir da ponderação da Auditoria Interna sobre alguns temas para objetos auditáveis que poderiam ser selecionados e priorizados para trabalhos de auditoria no ano de 2022 com base em riscos, foi encaminhada uma lista, por meio de formulário eletrônico, aos membros dos Conselhos Diretor e Curador para que pudessem orientar e opinar para fins do plano de trabalho da Auditoria Interna do ano de 2022, sugerindo a priorização sob a ótica da avaliação de riscos estratégico, operacional e de integridade. O tema em relação à Lei Geral de Proteção de Dados foi um dos mais pontuados pelos Conselheiros, sob o ponto de vista da aderência da gestão de privacidade de dados no IBGE à mesma.

Assim, o trabalho de auditoria teve como objetivo de avaliar a governança, o gerenciamento de riscos e os controles internos, instituídos para adequação da gestão de privacidade de dados à LGPD, em todos os aspectos relevantes, de acordo com os critérios aplicáveis, em conformidade com as normas e padrões nacionais e internacionais de auditoria no setor público.

As unidades auditadas foram as diretorias e coordenações do IBGE diretamente envolvidas na condução do mencionado objeto: Diretoria de Informática (DTI) e Centro de Documentação e Disseminação de Informações (CDDI).

Os critérios gerais para avaliação da governança, processos de gestão de riscos e controles internos residem na Política de Gestão de Riscos e na Metodologia de Gestão de Riscos do IBGE, aprovadas pela Resolução do Conselho Diretor (R.CD) nº 34, de 06/09/2019, boas práticas, normas internas e externas correlatas e aplicáveis ao serviço público federal.

A metodologia de trabalho de avaliação baseou-se no disposto da Instrução Normativa da Secretaria Federal de Controle da Controladoria-Geral da União (IN SFC/CGU) nº 3, de 09/06/2017, que aprovou o Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal (MOT), que serve de guia para o planejamento dos trabalhos individuais de auditoria, com foco em riscos, de forma a agregar valor à Unidade Auditada, identificando oportunidades para aperfeiçoamento dos processos de governança, gerenciamento de riscos e de controle.

Seguindo o referencial técnico do MOT e adotando a Metodologia de Gestão de Riscos do IBGE, a Auditoria Interna avaliou os riscos e controles do tema e, por meio de Matriz de Planejamento, definiu as questões de auditoria a serem percorridas nos exames do trabalho, a saber:

1. Houve formalização de uma estrutura de governança (equipe ou grupo de trabalho) para o planejamento e consequente implementação do Programa de Proteção de Dados Pessoais (Art. 50, §2º, I), a fim de atingir minimamente o que é necessário para adequação à LGPD e aos referenciais do governo federal?

2. Os controles internos estão sendo efetivamente executados e dão razoável segurança quanto a possibilidade de ocorrer acesso não autorizado de dados pessoais ou organizacionais?

3. Os controles internos estão sendo efetivamente executados e dão razoável segurança quanto a possibilidade de roubo, perda ou modificação de dados pessoais ou organizacionais?

4. As políticas, procedimentos e/ou controles internos dão razoável segurança em considerar os direitos do titular, alinhados aos Art. 6º, Inc. VI; Art. 41 e Art. 50 e em conformidade aos artigos 17 a 23 da LGPD?

5. As políticas, procedimentos e/ou controles internos definem de forma clara e transparente a necessidade de tratamento dos dados pessoais ou organizacionais realizado por meio eletrônico ou documento em papel?

Assim, no curso do trabalho, foram editadas diversas Solicitações de Auditoria (SA) às Unidades Administrativas responsáveis e com envolvimento em cada um dos processos e subprocessos examinados, com a correspondente coleta e a análise de dados, possibilitando a documentação de evidências para eventuais provas relacionadas a achados de auditoria, registradas em papéis de trabalho.

Os resultados dos exames realizados foram apresentados e discutidos com os respectivos gestores das Unidades Administrativas, como achados de auditoria relacionados a melhorias operacionais ou eventuais falhas com exposição a riscos, tendo as manifestações sido documentadas e registradas em papéis de trabalho.

As recomendações dispostas neste Relatório consistem em propostas de ações com a finalidade de corrigir eventuais falhas e aperfeiçoar os processos, objetivando agregar valor à gestão.

Por fim, cabe destacar que foram aplicados ao IBGE 3 (três) autoavaliações de diagnósticos pelos órgãos externos de controle para avaliar o nível a aderência de suas ações às diretrizes estabelecidas pela Lei Geral de Proteção de Dados - LGPD, sendo 1 (uma) aplicada pelo Tribunal de Contas União (TCU) e as outras 2 (duas) pela Secretaria de Governo Digital do Governo Federal (SGD), do Ministério da Gestão e da Inovação em Serviços Públicos (MGI), por meio por questionamento direto ao Gestor responsável pela implementação da LGPD.

Na autoavaliação do TCU, Acórdão do Tribunal nº 1384/2022, verifica-se que o IBGE se encontra no nível de maturidade “Intermediário”, considerando 4 (quatro) níveis, Inexpressivo, Inicial, Intermediário e Aprimorado.

Já nas 2 (duas) autoavaliações da SGD/MGI, Nota Técnica SEI nº 45751/2022/ME, constata-se que o IBGE se encontra na fase “Inicial e Planejamento” tomando como referencial o “Guia de Elaboração de Programa de Governança em Privacidade” da SGD que prevê 3 (três) etapas, “Iniciação e Planejamento”, “Construção e Execução” e “Monitoramento”. Tal informação foi de alta importância para o direcionamento dos trabalhos de auditoria, que acabaram por refletir achados e recomendações no contexto e a maturidade do estágio reproduzido em sua autoavaliação da adequação da gestão da privacidade de dados à LGPD.

É importante registrar que a atuação do IBGE está amparada em legislação federal específica, a da Lei nº 5.534/1968, conhecida como Lei do Sigilo Estatístico, e também na prática da maioria dos países e nas recomendações do Instituto Internacional de Estatística. Assim, há dedicação na asseguração da privacidade das informações individuais, possibilitando ao IBGE ser reconhecido como uma Instituição como digna da fé pública, capaz de prestar serviços de qualidade, com imparcialidade e integridade.

O IBGE possui a proteção dos dados e sua confidencialidade no Brasil como um compromisso desde a sua fundação, e além de garantidas por lei, também respeitam os Princípios Fundamentais das Estatísticas Oficiais das Nações Unidas.

RESULTADOS DOS EXAMES

1) **Requisitos de privacidade estão sendo capturados e consolidados mas ainda não foram capazes de ditar e influenciar como os dados pessoais em suas mais variadas formas devem ser manuseados no seu ciclo de vida no IBGE**

A ausência da formalização das etapas iniciais na elaboração e implementação do Programa de Governança em Privacidade (PGP) e a recente criação de órgão de apoio à governança indicam o quanto tem sido desafiadores os esforços da Administração em adequar a gestão da privacidade do IBGE às diretrizes estabelecidas na LGPD.

Na avaliação referente ao contexto de governança, sobre a estrutura ou grupo de trabalho formalmente constituída na Elaboração de Programa de Governança em Privacidade alinhado à Lei n° 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), fomos informados que em agosto de 2022 foi criado informalmente um grupo de trabalho para que fosse dado início à implementação do programa em adequação à LGPD. (SA_2022.3.01.01)

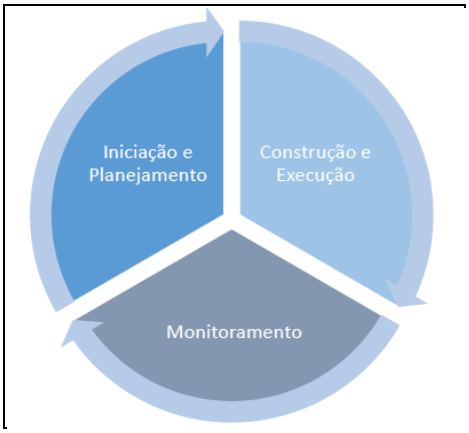
Adicionalmente, em 20/01/2023, em resposta ao OFÍCIO CIRCULAR SEI nº 1/2023/MGI da SGD, foi encaminhada a composição da estrutura de governança de segurança da informação e, em 30/03/2023, por meio da Resolução do Conselho Diretor nº 005/2023 (RCD_005/2023), foi criado formalmente o Comitê de Adequação à Lei Geral de Proteção de Dados Pessoais (CLGPD) com o objetivo de dar suporte ao encarregado de dados para o exercício das atividades de tratamento de dados pessoais do IBGE.

O comitê é composto por 2 (dois) representantes, 1 (um) titular e outro suplente, de cada Diretoria do IBGE, do Centro de Documentação e Disseminação de Informações (CDDI) e da Escola Nacional de Ciências Estatísticas (ENCE), a serem indicados pelos titulares das Unidades representadas.

Em que pese haver a estrutura de governança formalmente constituída com informações dos cargos dos gestores responsáveis por cada área de atuação para futura implementação, não foi constatado um planejamento específico com a definição das diversas etapas de forma a evidenciar a atuação do grupo de trabalho na implementação do Programa de Governança em Privacidade.

Adicionalmente, tomando como referencial o "Guia de Elaboração de Programa de Governança em Privacidade", editado pela SGD, é importante que se tenha um planejamento prévio com as etapas “Iniciação e Planejamento”, “Construção e Execução” e “Monitoramento” conforme Figura 1 e um cronograma das respectivas atividades sugeridas no guia, a fim de melhor apresentar, implementar e acompanhar a evolução da criação do Programa da instituição.

Figura 1: Etapas do Programa de Governança em Privacidade – PGP



Fonte: Guia de Elaboração de Programa de Governança em Privacidade

É importante ter um referencial para se criar um planejamento das etapas e atividades/tarefas, uma vez que facilita a implementação, pois diversas atividades/tarefas estão elencadas no próprio documento para a devida elaboração, ainda mais, sendo o referencial elaborado pela Secretaria de Governo Digital (SGD) do Governo Federal alinhando a LGPD.

Cabe ressaltar que há um esforço do grupo de trabalho para a implementação do Programa de Governança em Privacidade, porém na Nota Técnica SEI nº 45751/2022/ME, de 10/10/2022, foi informado que não houve avanços significativos entre os diagnósticos realizados em 03/03/2022 e 01/09/2022 em relação a 7 controles conforme Quadro1.

Quadro 1: Resultados do 1º e o 2º diagnósticos efetuados pela SGD

Controle	1º Diagnóstico	2º Diagnóstico
Conformidade de Privacidade	Parcialmente Implementado	Implementado
Conformidade de Segurança da Informação	Parcialmente Implementado	Parcialmente Implementado
Backup	Parcialmente Implementado	Parcialmente Implementado
Gestão de Acessos	Parcialmente Implementado	Parcialmente Implementado
Gestão de Vulnerabilidades	Parcialmente Implementado	Não Implementado
Inventário de Ativos	Implementado	Parcialmente Implementado
Auditoria	Implementado	Implementado
Quantidade de controles implementados	2	2
Quantidade de controles parcialmente implementados	5	4
Quantidade de controles não implementados	0	1

Fonte: Nota Técnica SEI nº 45751/2022/ME

Outro ponto a considerar, é o Acórdão TCU nº 1384/2022 de 06/04/2022, que por meio da autoavaliação aplicadas a 382 organizações públicas, entre novembro de 2020 e maio de 2021, a respeito de aspectos relacionados à condução de iniciativas para providenciar a adequação à LGPD e às medidas implementadas para o cumprimento das exigências estabelecidas na Lei, registra que nível de maturidade do IBGE é “intermediário”, situação não corroborada em dezembro/2022.

Por fim, considerando a ratificação do Gestor por meio da SA_2022.3.01.01/CDDI, do atual estágio do Programa de Governança em Privacidade, de “Iniciação e Planejamento”, reforça-se a necessidade do comprometimento da alta administração, conforme recomendado pelo Departamento de Privacidade e Segurança da Informação da Secretaria de Governo Digital (DPSI/SGD/SEDGG/ME) pela Nota Técnica SEI nº 45751/2022/ME, de 10/10/2022.

2) Política de Segurança da Informação e Comunicação (POSIC) encontra-se desatualizada, compreendo o período relativo aos anos de 2017 a 2018

A Política de Segurança da Informação e Comunicação (POSIC) é um documento que define os princípios e as diretrizes que norteiam a segurança de informação no IBGE, sendo que ela é suportada por diversos normativos que descrevem e implementam controles de segurança, responsabilidades, competências na aplicação, gerenciamento e monitoramento dos controles definidos.

Avaliando a POSIC, verificou-se a atualização de diversos documentos complementares ao longo desses últimos 5 anos, porém a Política propriamente dita foi aprovada em 02/08/2017, compreendendo a visão para o período compreendido dos anos de 2017 a 2018, o qual ainda permanece em vigor.

Questionado sobre a atualização da POSIC, o gestor informou que previsão de atualização seria ainda em março de 2023, ressaltando que esta seria a 4ª edição da POSIC do IBGE, e que a Instrução Normativa nº. 01 da DSIC/GSIPR, de 27/05/2020, estabelece em seu Art. 12, que o período máximo para atualização é de 4 anos. (SA_2022.3.01.02/DTI). Com todos os eventos relacionados ao Censo, a nova POSIC do IBGE foi aprovada em novembro de 2023.

Adicionalmente, o gestor informou que se deve considerar que no período relacionado ocorreram eventos relacionados à mudança na forma do uso da tecnologia da informação e comunicação no IBGE e a realização do Censo Demográfico 2022, em um contexto de equipes técnicas da DTI bastante reduzidas para o volume de trabalho apresentado.

Em que pese o exposto, foram revisados pela DTI os normativos que compõem a Política de Segurança da Informação, como as IN.DI nº 01/2021 - Acesso Físico e Lógico aos Ativos de Tecnologia do IBGE, a IN.DI nº.02/2021 - Uso de Ativos de Tecnologia da Informação, IN DI nº 03/2021 - Uso de Software, IN DI nº 08/2021 - Uso do Correio Eletrônico, IN.DI nº 09/2021 - Acesso à Internet, IN.DI nº 10/2021 - Normas e procedimentos para backup no IBGE, além das R.CD nº 11/2021 – Política de Acesso à Internet , R.CD nº 13/2021- Política sobre o uso do Correio Eletrônico e a R.CD nº 31/2021 - Política de Governança de Dados.

[redacted]

contempla a nova sessão exigida pela Instrução Normativa nº. 01 da DSIC/GSIPR de Tratamento de Informações.

Conforme IN nº. 01 da DSIC/GSIPR, 05/2020, em seu § 1º, Artº 12, estabelece que a periodicidade para a revisão da Política de Segurança da Informação não deve exceder 4 (quatro) anos, situação não evidenciada em sua completude, e objetiva possibilitar que todos os servidores da Instituição tenham conhecimentos de suas responsabilidades, visando garantir

disponibilidade, integridade, confidencialidade, autenticidade e de proteção de dados pessoais e organizacionais, dentro requisitos legais, favorecem a imagem instituição junto a sociedade.

3) Política de Privacidade de Dados (PP) encontra-se parcialmente adequada à Lei nº 13.709/2018

No decorrer do trabalho de auditoria, constava no portal do IBGE, em 07/12/2022, um documento chamado Política de Privacidade de Dados (PP), tendo como objetivo a política de privacidade dos sites e aplicativos IBGE, não refletindo uma política propriamente dita de privacidade e com alinhamento à Lei nº 13.709/2018.

Questionado sobre elaboração da Política de Privacidade alinhada à Lei 13.709/2018, o gestor informou que ela já havia sido elaborada e que, no entanto, dependeria de aprovação por parte do Conselho Diretor do IBGE (CD), o que deveria acontecer ainda em 2022, porém, não foi evidenciado a elaboração formal de documentação ou instrução sobre os procedimentos da Política de Privacidade de Dados aprovado pelo CD (SA_2022.3.01.03/CDDI).

No decorrer do trabalho, durante a fase elaboração do relatório, verificou-se que havia uma nova Política de Privacidade publicada no portal do IBGE (https://www.ibge.gov.br/acesso-informacao/acoes-e-programas/politica-de-privacidade.html), em 15/12/2022, bem mais alinhada ao normativo.

Esse novo documento, alinha-se à Lei 13.709/2018, uma vez que informa diversos aspectos como: *Compromisso do IBGE, Como coletamos os seus dados, Para que coletamos os seus dados, Compartilhamento de dados, Segurança no tratamento dos dados, Contato (Controlador, Operador e Encarregado).*

Dessa forma, a Política de Privacidade funciona como um acordo entre a Instituição e o titular dos dados pessoais, devendo esclarecer como essas informações serão utilizadas e para qual finalidade, informando os direitos e deveres da Instituição e garantindo a aceitação dos termos pelo usuário.

A Política de Privacidade funciona como uma ferramenta de transparência das organizações que custodiam dados pessoais e disponibilização do documento gera maior credibilidade e confiança.

4) Inexistência de programas de capacitação e de comunicação sobre proteção de dados pessoais

Sobre a eventual existência de planos de treinamento e de divulgação e/ou disseminação de assuntos relacionados ao tema proteção de dados pessoais, o gestor informou que o IBGE efetuou a capacitação dos coordenadores e responsáveis pelas equipes que tratam dados pessoais na Administração Central, e que seria replicado aos envolvidos nas Superintendências Estaduais, após a coleta do Censo Demográfico 2022. No dia 23/11/2022 foi realizada uma palestra sobre a LGPD para 28 servidores que aceitaram o convite, mas como a palestra não estava restrita aos convidados e estes poderiam repassar o *link* da reunião para outros funcionários, durante a palestra tiveram mais de 70 pessoas assistindo via Teams (ID da Reunião: 265 467 979 599). (SA_2022.3.01.01/CDDI).

Adicionalmente, foi informado que devido à natureza da atuação do IBGE, já existe uma conscientização dos funcionários sobre a necessidade de sigilo e tratamento dos dados coletados em pesquisas, inclusive com treinamentos de rotina que são disponibilizados aos servidores. No sentido de atender à LGPD, o desafio agora é construir uma cultura no tratamento de dados pessoais fora dessa atividade. (SA_2022.3.01.03/CDDI).

No decorrer do trabalho, durante a fase elaboração do relatório, no dia 25/05/2023 ocorreu a palestra ***"LGPD-Lei Geral de Proteção de Dados - Proteção e Privacidade de Dados no IBGE"***, em um esforço na disseminação do tema junto aos servidores do IBGE.

Em que pese as respostas acima e haver uma conscientização dos servidores sobre a necessidade de sigilo e tratamento dos dados coletados em pesquisas, não identificamos um plano de capacitação formalmente constituído e disponibilizado aos servidores, por meio da plataforma da CTA/ENCE, assim como a existência de programa de comunicação sobre o tema de proteção de dados pessoais para fins de disseminação e conscientização.

A oferta de um plano de treinamento e capacitação estruturado e o uso dos canais de comunicação já existentes no IBGE para a disseminação estruturada e contínua de informações e notícias relacionadas contribuiriam para que a segurança da informação e a privacidade de dados sejam parte integrante do ambiente de governança, gerenciamento de riscos e controles internos do IBGE.

Instituir uma cultura de capacitação, disseminação e conscientização sobre o tema que reforce as políticas, procedimentos e a importância do uso adequado e responsável das informações pessoais permitirá uma melhor custódia de dados pessoais da própria Instituição e de terceiros.

5) Ausência de processos formalmente constituídos contemplando as respostas a possíveis incidentes afetos à gestão de dados pessoais, o fluxo das atividades de trabalho, à devida comunicação aos titulares dos dados e às autoridades competentes

Em que pese a etapa em que o IBGE se encontra na condução do seu Programa de Governança em Privacidade (PGD), "Iniciação e Planejamento", observou-se a inexistência na Cadeia de Valor do IBGE e na Arquitetura de Processos, de processos relacionados à gestão da privacidade de dados que incluam desde o gerenciamento das atividades até a condução da agenda de segurança e respostas a incidentes relacionados a dados pessoais.

Questionado sobre a definição e modelagem de processos de respostas a possíveis incidentes, o fluxo das atividades de trabalho e a devida comunicação aos titulares e às autoridades competentes, o gestor informou que ainda não foi elaborado e encontra-se em avaliação para endereçamento, porém a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do IBGE (ETIR) já foi formalmente constituída conforme R.CD-IBGE nº.120/2022 de 12/12/2022. (SA_2022.3.01.01).

Em que pese a criação da ETIR, faz-se a definição e a modelagem dos processos que sustentariam a gestão de dados pessoais na Instituição é essencial para o avanço em cada etapa do PGD, permitindo maior assertividade e segurança de avaliações e endereçamentos técnicos, contribuindo na custódia dos dados pessoais e na adequada adesão do IBGE à LGPD.

É importante reforçar que a formalização e modelagem de processos com a definição das atividades inerentes tornam-se necessárias para a consecução de resposta a eventuais incidentes de vazamento dados pessoais, contemplando a definição dos incidentes, o escopo das respostas ao titular dos dados, bem como quando e quais os órgãos reguladores devem ser contatados, os papéis, as responsabilidades, a avaliação de impacto do incidente, as medidas para reduzir a probabilidade e mitigar o impacto do incidente, descrevendo a natureza dos dados pessoais eventualmente afetados.

6) Serviços de consultoria contratados para o diagnóstico, o planejamento, a avaliação da conformidade e o gerenciamento de riscos relacionados à gestão de proteção de dados pessoais no IBGE em consonância com a LGPD ainda não se iniciou

A Diretoria de Tecnologia da Informação (DTI) contratou por meio de licitação, processo nº 0000006.00000091/2021-87, a [redacted] para a realização de diversos serviços de segurança da informação e comunicações. Dentre os itens contratados está a "gestão de riscos", que entre outros subitens contém o item "Compliance à Lei Geral de Proteção de Dados" com objetivo de auxiliar o IBGE no diagnóstico, planejamento e conformidade com a LGPD, incluindo a realização de recomendações para a Instituição possa avançar neste tema.

Questionado sobre o andamento dos serviços contratados junto à Service IT previstos no item "gestão de riscos", o gestor DTI informou que, apesar da contratação da empresa para implementação relacionados ao assunto, o processo ainda não se iniciou em função das demandas do Censo Demográfico 2022, as quais necessitam de especial atenção na preparação do ambiente tecnológico para resistir a possíveis invasões, ratificando que não há processo de gestão de proteção de dados em busca do monitoramento e mitigação dos usuais riscos

relacionados ao tema e que esta etapa do processo ainda será iniciada e acontecerá em paralelo ao a criação do grupo de trabalho. (SA_2022.3.01.02/DTI)

É fato que as medidas de segurança para a proteção dos dados pessoais devem ser implementadas na etapa de "Construção e Execução", etapa posterior ao atual do IBGE, se tomarmos como referencial o "Guia de Elaboração de Programa de Governança em Privacidade".

Entretanto, considerando a importância dos temas diagnóstico, planejamento e conformidade na etapa de "Iniciação e Planejamento", no âmbito do Programa de Governança em Privacidade, para a identificação dos riscos de proteção de dados e o gerenciamento das medidas de preventivas relacionadas a incidentes e à violação dos dados pessoais, cabe enfatizar a necessidade de avançar na agenda prevista contratualmente com prestador de serviço contratado.

7) Fragilidade na concessão, revogação, monitoramento e controle periódico de acesso dos terceirizados e estagiários ao ambiente de rede de computadores e sistemas informatizados do IBGE

Avaliando o controle de acesso ao ambiente de rede do IBGE e efetuando alguns testes de desativação de contas, constata-se que o a concessão e revogação de acesso é integrado ao sistema administrativo (SDA e Base de Concurso), ao sistema de pagamento (SAPC), sistema de pessoal da ENCE, portal de sistemas e ao correio eletrônico. Assim, quando um servidor efetivo, contratado temporário, aluno ou professor da ENCE toma posse ou é desligado do IBGE, consegue-se conceder ou revogar, respectivamente, o acesso automaticamente à rede corporativa por meio de ação específica em sistema corporativo. (SA_2022.3.01.01/DTI)

[redacted]

Em reunião com a DTI, foi confirmada a dificuldade em garantir que os gestores informem quando da saída de terceirizados e estagiários para a respectiva desativação de conta, demonstrando uma dependência da DTI em relação às informações dos gestores, o que nos parece ser uma fragilidade no processo que potencializa eventuais riscos de acesso indevido à rede de computadores e sistemas informatizados do IBGE.

Por esta razão, é necessária uma reavaliação em conjunto com a área de Recursos Humanos para que mantenha um cadastro e controle dos profissionais do tipo estagiário e consultores para que os processos de TIC relacionados à criação de contas e concessão de acesso possam tomar conhecimento das movimentações desses profissionais, somente desta forma o processo poderá ser garantidamente fechado e seguro.

Cabe ressaltar que é importante conscientizar o gestor sobre a avalição da real necessidade de conceder acesso a dados/informações/sistemas a determinado servidor/colaborador em função da sua atividade dentro do órgão, bem como da imediata revogação/comunicação de sua saída, assim, minimizando riscos de acessos indevidos a dados pessoais e/ou organizações.

Quanto ao monitoramento da necessidade de acesso de usuários a rede, verificou-se que a revisão de acesso ao ambiente de rede é efetuada de forma periódica de acordo com a IN DI nº 1/2021-"Acesso Físico e Lógico aos Ativos de Tecnologia do IBGE". (SA 2022.3.01.04)

Questionado sobre a revisão de acesso as bases de dados das áreas de negócios, o gestor informou que existe a R.CD nº 31/2021-Política de Governança de Dados, a qual define que os gestores controlam as permissões e perfis de acesso aos sistemas de acordo, porém não há informação se os gestores efetuam os controles periodicamente a fim de garantir a real necessidade de manutenção de acesso a determinado servidor/colaborador em acordo com Art. 39 IN DI nº 1/2021- Acesso Físico e Lógico aos Ativos de Tecnologia do IBGE, onde os gestores de sistema devem promover no mínimo uma revisão anual dos privilégios de acesso dos usuários dos sistemas de informação sob sua gestão. (SA_2022.3.1.01).

Desta forma, reforça-se que os controles de proteção de dados pessoais devem ser monitorados e auditados periodicamente para garantir que as operações que envolvam dados pessoais estejam em conformidade com as leis, regulamentos e termos contratuais aplicáveis e que os acessos estejam adequados às atividades, garantindo que não ocorra acessos indevidos.

8) Ausência de informação na política de backup quanto aos prazos de retenção, exclusões de dados pessoais.

Sobre os prazos de retenção em relação aos dados pessoas, o gestor da DTI informou que a IN DI 010-2021 - Backup Normas e procedimentos para backup no IBGE e os Anexos I e II abordam a frequência, o período de retenção e o tipo de backup implementado por tecnologia e ambiente (SA_2022.3.01.02/DTI).

Analisando a referida norma e seus anexos, verifica-se as descrições das normas e procedimentos para backup, a frequência e o período de retenção das cópias de segurança dos ativos de informação e o tipo de backup implementado por tecnologia e ambiente, porém não é possível associar os backups das bases de dados com os sistemas e nem o período retenção das bases de dados que envolvam dados pessoais sensíveis. Ressalta-se que o IBGE ainda não tem uma Política de Classificação de Informações.

Cabe destacar que a Lei Geral de Proteção de Dados não informa a necessidade de separação dos dados pessoais para efetivação de backup, mas é importante que os backups dos sistemas e das bases de dados estejam alinhados para a necessidade de recuperação.

Quanto ao período de retenção, nos Arts. 15 e 16, a Lei 13.709/18 informa situações quando “Do Término do Tratamento de Dados”, sendo importante ter informações sobre os prazos de retenção para os dados pessoais sensíveis. Assim, é fundamental informar que os dados coletados nas pesquisas do IBGE possuem tempo de permanência indeterminado em virtude da necessidade de manutenção das séries históricas.

9) Ausência de política e inventário de dados pessoais com as informações relevantes objetivando a identificação, principalmente, dos dados sensíveis e não sensíveis, para o devido tratamento.

Considerando o IBGE ter iniciado a elaboração Programa de Governança em Privacidade, [redacted] inventário de dados pessoais por categorias, alinhado à missão institucional e à privacidade dos titulares, em uma organização, mas o IBGE ainda não havia iniciado a atividade. (SA_2022.3.01.01).

Tendo em vista ainda não ter iniciado o inventário, a Política de Inventário de Dados Pessoais deverá conter informações relevantes, atualizadas periodicamente em consonância ao Art. 5º da LGPD, além de estar relacionada à missão institucional e à privacidade dos titulares classificados como sensíveis e não sensíveis, sendo que próprio inventário de dados pessoais 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.

De acordo com o "Guia de Elaboração de Programa de Governança em Privacidade", o inventário de dados pessoais representa documento primordial no sentido de documentar o tratamento de dados pessoais realizados pela instituição, em alinhamento ao previsto pelo art. 37 da LGPD. 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.

Por fim, o tratamento de dados pessoais deverá ser realizado pela administração pública nos termos do que determina art. 23 da LGPD, unicamente para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

10) Relatório de Impacto à Proteção de Dados Pessoais (RIPD) ainda não foi elaborado em que pese a possibilidade de sua exigência por parte da Autoridade Nacional de Proteção de Dados Pessoais (ANPD)

O Programa de Governança em Privacidade (PGD) instituído pelo MGI/SGD prevê, em relação à etapa de "Construção e Execução", a elaboração do Relatório de Impacto e Proteção de Dados Pessoais (RIPD).

O RIPD representa um instrumento importante de verificação e demonstração da conformidade do tratamento de dados pessoais realizado pela instituição e serve tanto para a análise quanto para a documentação do tratamento dos dados pessoais, descrevendo os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.
(Fonte: GUIA DE ELABORAÇÃO DE PROGRAMA DE GOVERNANÇA EM PRIVACIDADE)

Em que pese o IBGE encontrar-se na etapa "Iniciação e Planejamento" do PGD, não observamos a previsibilidade da elaboração do RIPD no plano de trabalho dos gestores do processo, em que pese a possibilidade de a ANPD solicitar tal informação ao controlador, como o IBGE é qualificado.

11) Inexistência de levantamento dos contratos relacionados a dados pessoais impossibilita a avaliação e as necessárias adequações deles, em relação a serviços que coletam, transferem e processam tais dados, assim, como não orienta os termos de contratações futuras na Instituição

Observamos que em que pese o IBGE situar-se na etapa de "Iniciação e Planejamento" do PGP, ainda não foi desenvolvido o levantamento dos contratos relacionados a dados pessoais.

Sobre os contratos que possuem informações de dados sigilosos com órgãos e operadores de dados pessoais no que tange a assinatura de termos de responsabilidade e confidencialidade em consonância à LGPD, o gestor do CDDI/GEATE informou que existem termos de [redacted]

Neste sentido, identificou-se a necessidade de adequação à LGPD dos contratos nos quais o IBGE repassa dados pessoais para prestadores de serviços realizarem seu trabalho (SA_2022.3.01.01).

De acordo com "Guia de Elaboração de Programa de Governança em Privacidade", o levantamento dos serviços que tratam dados pessoais no Inventário de Dados viabiliza a realização de uma correlação com os contratos que os suportam. Esse mapeamento dos contratos que coletam, transferem e processam dados pessoais contribui para possíveis e necessárias adequações contratuais, tanto nos contratos existentes, quanto nos futuros.

A Lei Geral de Proteção de Dados Pessoais (LGPD) foi sancionada para regulamentar as atividades de tratamento de dados pessoais, impondo regras sobre a coleta, armazenamento e compartilhamento de dados por empresas e organizações para assegurar a privacidade das pessoas, garantindo que seus dados não sejam utilizados sem consentimento ou para fins indevidos.

12) Canal de comunicação e divulgação sobre informações de tratamentos e práticas do controlador (IBGE) de dados pessoais está desatualizado e com falha no acesso

Avaliando como são fornecidas aos titulares de dados pessoais informações claras e facilmente acessíveis sobre as políticas, procedimentos, práticas do controlador de dados pessoais em relação ao manuseio de dados pessoais, como os dados são protegidos, dados de comunicação com o encarregado, entre outras informações de importância a transparência e publicidade, o gestor do CDDI/GEATE informou que em relação aos dados de comunicação com o encarregado, o IBGE disponibiliza as informações em seu sítio na internet (https://www.ibge.gov.br/acesso-informacao/tratamento-de-dados-pessoais.html) e como a etapa de inventário de dados ainda está sendo construída, após essa fase as demais informações serão disponibilizadas. (SA_2022.3.01.01).

Quanto a aderência do site supramencionado com a Lei nº 13.709/2018, verifica-se que no site do IBGE informado, existem informações sobre o encarregado de dados, link ao Fala.br da CGU, menção as leis que regem as atividades do IBGE, bem como diversos documentos sobre o tema LGPD, porém o canal de comunicação sobre informações de tratamentos e práticas do controlador (IBGE) de dados pessoais está desatualizado, uma vez que a POSIC ainda se refere ao período de 2017-2018 e ocorre erro 404 ao clicar no **"Aqui"** ao final do texto "O acesso a política de privacidade do IBGE pode ser consultado".

Quanto à comunicação sobre a finalidade do tratamento ao titular dos dados pessoais, antes que as informações sejam coletadas ou usadas, o gestou informou que nesse momento essas informações não são repassadas ao titular dos dados (SA_2022.3.01.01).

É importante observar que o princípio da transparência, de acordo com art. 6º, VI, da LGPD é a *"garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial"*, assim é necessário que as informações disponíveis estejam minimamente atualizadas e acessíveis e que a finalidade do tratamento deve ser comunicada ao titular dos dados pessoais, antes que as informações sejam coletadas ou usadas.

13) Ausência de monitoramento contínuo das ações de proteção de dados pessoais de forma geral, a fim de determinar o alinhamento e o progresso no cumprimento dos requisitos de conformidade com LGPD

Sobre o monitoramento contínuo das ações de proteção de dados pessoais, a fim de determinar o progresso no cumprimento dos requisitos de conformidade com a proteção de dados pessoais e dos controles de proteção de dados pessoais, o gestor informou que devido à natureza da atuação do IBGE, existe um controle de proteção de dados pessoais em relação às pesquisas [redacted]

Constate-se que o monitoramento das ações de proteção de dados pessoais não se estende a todas as atividades ou serviços que tratam de dados pessoais da Instituição. Desta forma, não é possível avaliar o alinhamento, o progresso no cumprimento dos requisitos de conformidade com a proteção de dados pessoais, os controles de proteção de dados pessoais, a identificação

de vulnerabilidades e lacunas na política e na implementação do programa de governança e privacidade de dados.

De acordo com "Guia de Elaboração de Programa de Governança em Privacidade", o "Monitoramento" é a terceira etapa da implementação do programa de governança e privacidade de dados, sendo uma atividade contínua e necessária para os órgãos e entidades manterem Programa de Governança em Privacidade a longo prazo, que incluem, em grande parte, coleta e análise de informações, bem como elaboração de relatórios e apresentações de resultados.

Isto posto, cabe destacar que o IBGE se encontra na primeira etapa, "Iniciação e Planejamento", o que reforça a necessidade de avançar nas demais etapas do Programa de Governança em Privacidade para que se atinja um grau de maturidade adequado a um processo de monitoramento e mitigação contínuo dos usuais riscos relacionados ao tema.

14) Acúmulo de funções do Encarregado de Dados com outros cargos e atividades pode afastar a independência necessária como canal de comunicação entre o agente de tratamento, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) e fragilizar a gestão de dados pessoais no IBGE

Observou-se que o titular da Coordenação de Atendimento e Informação (COATI), do Centro de Documentação e Disseminação de Informações (CDDI), acumula a função de Encarregado de Dados do IBGE.

Destaca-se que a COATI possui as atribuições de planejar, coordenar e acompanhar o desenvolvimento, implementação e manutenção de ações e iniciativas de disseminação com componentes geoespaciais, no âmbito do CDDI, distribuindo as atividades pela Gerência de Atendimento (COATI/GEATE), Gerência de Biblioteca, Informação e Memória (COATI/GEBIM) e Gerência de Recuperação de Informações (COATI/GERI).

Recentes decisões proferidas por autoridades de proteção de dados na União Europeia, onde o tema encontra-se em maior nível de maturidade, mostraram que o acúmulo da função de encarregado com outros cargos e atividades pode ser considerada como suficiente para afastar a independência do encarregado e, portanto, constituir uma inobservância e acarretar penalidade.

Mesmo considerando que a função do encarregado é consultiva e não cabe, individualmente, tomar decisões sobre o tratamento de dados, seu papel envolve orientar e ditar as diretrizes sobre o tratamento de dados pessoais, na Instituição, exigindo constante capacitação e conhecimento da legislação de privacidade e proteção de dados, tecnologia da informação, *compliance*, governança corporativa, gestão de riscos e de políticas corporativas.

RECOMENDAÇÕES

1. Consolidar os requisitos para guiar o IBGE na aderência às exigências previstas na Lei Geral de Proteção de Dados contribuiria no processo de gerenciamento da privacidade de dados, favorecendo a condução do Programa de Governança em Privacidade, nas correspondentes fases de “Iniciação e Planejamento”, “Construção e Execução” e “Monitoramento”, apresentado como política pública e recomendado para implementação pelas Organizações Públicas Federais, pelo Departamento de Privacidade e Segurança da Informação, da Secretaria de Governo Digital, do Ministério da Gestão e da Inovação em Serviços Públicos (DPSI/SGD/MGI).

   Nível de criticidade: Alto

   Unidade Administrativa responsável: CDDI

   Achado de Auditoria: 1

2. Avaliar a priorização das atividades de elaboração (i) do inventário de dados pessoais, bem como a política associada; e (ii) do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), no âmbito do Programa de Governança em Privacidade, considerando tratar-se de documento primordial no sentido de formalizar o tratamento de dados pessoais realizados pelo IBGE e descrever os processos que podem gerar riscos à privacidade, respectivamente, contribuindo com o avanço com a aderência às previsões da LGPD.

   Nível de criticidade: Alto

   Unidade Administrativa responsável: CDDI

   Achado de Auditoria: 9 e 10

3. Rever e atualizar a Política de Segurança da Informação em sua totalidade, uma vez que o documento existente e disponibilização no Portal do IBGE na Internet está referenciando o período de 2017-2018.

   Nível de criticidade: Alto

   Unidade Administrativa responsável: DTI

   Achado de Auditoria: 2

4. Rever e complementar a Política de Privacidade Dados existente e disponibilizada no Portal do IBGE na Internet a fim de incluir aspectos que reportem maior completude de tratamento e informações sobre a transparência em alinhamento à legislação.

   Nível de criticidade: Alto

   Unidade Administrativa responsável: CDDI

   Achado de Auditoria: 3

5. Ações relacionadas à constituição de programas de (i) capacitação sobre o gerenciamento da privacidade, em linha com as previsões existentes na LGPD; e (ii) comunicação, buscando divulgar periodicamente informações em canal próprio, disseminaria o conteúdo relacionado à proteção de dados pessoais e ampliaria o conhecimento dos servidores acerca do tema favorecendo o seu aculturamento na Instituição.

   Nível de criticidade: Alto

   Unidade Administrativa responsável: CDDI

   Achado de Auditoria: 4

6. Estabelecer o processo de gestão de dados pessoais na estrutura da Arquitetura de Processos vinculada à Cadeia de Valor do IBGE, bem como a sua derivação em subprocessos, e desenvolver a modelagem alcançando, minimamente, o fluxo de atuação, o gerenciamento dos possíveis incidentes, as respostas a estas situações e devida comunicação aos titulares e às autoridades competentes.

   Nível de criticidade: Alto

   Unidade Administrativa responsável: CDDI

   Achado de Auditoria: 5

7. Prosseguir com a prestação dos serviços contratados junto à empresa Service IT em relação ao diagnóstico, o planejamento, a avaliação da conformidade e ao gerenciamento de riscos relacionados à gestão de proteção de dados pessoais no IBGE, objetivando a completude dos esforços de trabalho da Instituição na aderência às previsões da LGPD.

   Nível de criticidade: Alto

   Unidade Administrativa responsável: DTI

   Achado de Auditoria: 6

8. Revisar o processo de concessão e revogação de acesso à rede de computadores e de sistemas informatizados do IBGE de forma que se tenha alcance melhor segurança em relação às permissões concedidas a prestadores de serviços terceirizados e estagiários, objetivando que a concessão e a sua revogação ocorram de forma automática, mitigando a possibilidade do risco de acesso não autorizado a dados pessoais.

   Nível de criticidade: Alto

   Unidade Administrativa responsável: DTI e DE/CRH

   Achado de Auditoria: 7

9. Avaliar a inclusão na Política de Backup de informações referentes à previsibilidade da retenção e exclusão de dados em relação aos sistemas informatizados do IBGE que alcancem dados pessoais.

   Nível de criticidade: Alto

   Unidade Administrativa responsável: DTI

   Achado de Auditoria: 8

10. Efetuar levantamento dos contratos de serviços, bem como convênios e outros instrumentos, que coletem, transferem e processem dados pessoais para possíveis e necessárias adequações de cláusulas contratuais, de forma a se alinharem à LGPD, bem como endereçar especificações padronizadas para contratações futuras.

    Nível de criticidade: Alto

    Unidade Administrativa responsável: CDDI

    Achado de Auditoria: 11

11. Revisar o canal de comunicação atual do IBGE no Portal da Instituição na Internet, sobre informações de tratamentos de dados pessoais, considerando que se encontra desatualizado e com erro quanto da tentativa de acesso.

    Nível de criticidade: Alto

    Unidade Administrativa responsável: CDDI

    Achado de Auditoria: 12

12. Instituir o monitoramento contínuo das ações que buscam alcançar a aderência do IBGE em proteção de dados pessoais, em atendimento às previsões da LGPD, acompanhando a condução das atividades desenvolvidas no planejamento do Programa de Governança em Privacidade, de forma a possibilitar a sua transparência e comunicação para fins de supervisão.

    Nível de criticidade: Alto

    Unidade Administrativa responsável: CDDI

    Achado de Auditoria: 13

13. Avaliar a definição da função de Encarregado de Dados do IBGE como sendo de dedicação exclusiva e vinculá-la à Unidade Administrativa própria, preferencialmente subordinada diretamente ao Gabinete da Presidência, de forma a favorecer o pleno desenvolvimento de suas atribuições, como (i) aceitar reclamações e comunicações dos titulares dos dados pessoais; (ii) prestar esclarecimentos; (iii) receber comunicações; e (iv) orientar os servidores e os contratados da Instituição a respeito das práticas a serem tomadas em relação à proteção de dados pessoais

    Nível de criticidade: Alto

    Unidade Administrativa responsável: DE e GAB/PR

    Achado de Auditoria: 14

CONCLUSÃO

Apresentamos a seguir, as respostas às questões de auditoria propostas no planejamento da avaliação da gestão da privacidade de dados em atendimento às previsões contidas na Lei Geral de Proteção de Dados Pessoais (LPGD), com base no resultado dos exames (achados de auditoria) e nas causas raízes que foram possíveis de identificação.

1. Houve formalização de uma estrutura de governança (equipe ou grupo de trabalho) para o planejamento e consequente implementação do Programa de Proteção de Dados Pessoais (Art. 50, §2º, I), a fim de atingir minimamente o que é necessário para adequação à LGPD e aos referenciais do governo federal?

   Foi observada a constituição do Comitê de Adequação à Lei Geral de Proteção de Dados Pessoais (CLPGD) com o objetivo de fornecer suporte ao Encarregado de Dados do IBGE para o exercício das atividades de tratamento da privacidade de dados na Instituição, por meio da Resolução do Conselho Diretor nº 5/2023, de 30/03/2023, e esforços dos gestores à implementação do Programa de Governança em Privacidade, instituído pela SGD/MGI.

   Porém, apesar dos esforços em sua criação, não houve avanços significativos e abrangentes no planejamento e na consequente implementação da governança, gerenciamento de riscos e do controle interno, pois apesar do IBGE ainda se encontrar na etapa “Inicial e Planejamento” há diversas atividades não implementadas referente a esta etapa. (Achados nºs 1, 9, 10, 11, 12 e 13)

2. Os controles internos estão sendo efetivamente executados e dão razoável segurança quanto a possibilidade de ocorrer acesso não autorizado de dados pessoais ou organizacionais?

   e

3. Os controles internos estão sendo efetivamente executados e dão razoável segurança quanto a possibilidade de roubo, perda ou modificação de dados pessoais ou organizacionais?

   O IBGE possui uma equipe denominada Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), que possui a responsabilidade de atuar em relação à segurança cibernética, em observância à Política de Segurança da Informação e Comunicação da Instituição, bem como contratou serviços especializados de prevenção, detecção, gestão e resposta a incidentes, avaliação de vulnerabilidades e riscos ao ambiente de rede externo ao IBGE, ou seja, um *Security Operation Center* (SOC).

   Assim, o IBGE possui uma equipe terceirizada de segurança da informação (Equipe SOC), responsável por monitorar e analisar a postura de segurança da Instituição de forma

contínua, buscando detectar, analisar e colaborar com recomendações às áreas do IBGE para responder a incidentes de segurança de dados, que trabalha em conjunto com a Gerência de Segurança, e quando necessário com a ETIR, para garantir que os problemas de segurança sejam resolvidos rapidamente após serem descobertos.

Em que pese tais esforços observamos que (i) há a necessidade de o IBGE avançar no uso e na combinação de soluções de tecnologia da informação e um forte conjunto de processos e suas derivações perfeitamente mapeados e documentados; e (ii) a equipe ETIR da DTI não possui dedicação exclusiva, não se caracterizando como controle ou medidas de segurança desejável à gestão da segurança da informação.

Importante relatar ainda que, quanto ao ambiente interno da rede de computadores do IBGE e o acesso aos seus sistemas informatizados, considerando o acesso por parte de servidores, prestadores de serviços contratados temporariamente, terceirizados e estagiários, não é possível afirmar que os controles dão razoável segurança quanto ao acesso não autorizado, uma vez que foi constatado fragilidade na concessão, revogação, e revisão e monitoramento, especificamente, em relação ao acesso de colaboradores (terceirizados e estagiários). (Achado nº 7)

Adicionalmente, não há informação que sobre os prazos de retenção dos dados coletados nas pesquisas do IBGE, pois possuem tempo de permanência indeterminado em virtude da necessidade de manutenção das séries históricas.

4. As políticas, procedimentos e controles internos dão razoável segurança em considerar os direitos do titular, alinhados aos Art. 6º, Inc. VI; Art. 41 e Art. 50 e em conformidade aos artigos 17 a 23 da LGPD?

   e

5. As políticas, procedimentos e controles internos definem de forma clara e transparente a necessidade de tratamento dos dados pessoais ou organizacionais realizado por meio eletrônico ou documentos em papel?

   Considerando o atual estágio no IBGE em que se encontra a implementação do Programa de Governança de Dados (PGD) – "Inicial e Planejamento", de acordo com o "Guia de Elaboração de Programa de Governança em Privacidade" – as políticas, os procedimentos e controles internos ainda não favorecem a segurança desejada com base nos preceitos da LGPD, em relação aos direitos do titular dos dados.

   Tal situação se verifica pela não captura e consolidação dos requisitos de privacidade de forma a ditar e a influenciar como os dados pessoais em suas mais variadas formas devem ser manuseados no seu ciclo de vida no IBGE, e, especificamente, não endereçando etapas estabelecidas no PGD como (i) inventários de dados; (ii) classificação de dados em sensíveis e não sensíveis; (iii) levantamento de contratos de prestadores de serviços relacionados a dados pessoais; e (iv) monitoramento contínuo das ações de proteção de dados pessoais, avaliando e reavaliando os riscos e progresso da implementação processos. (Achados nºs 6, 9, 10, 11, 12 e 13)

Importante reportar a ausência de processos formalmente constituídos contemplando as respostas a possíveis incidentes afetos à gestão de dados pessoais, o fluxo das atividades de trabalho, à devida comunicação aos titulares dos dados e às autoridades competentes. (Achados nos 1 e 5)

Adicionalmente, (i) observou-se informações desatualizadas no Portal do IBGE na Internet referente à Política de Segurança da Informação e que a Política de Privacidade de Dados parcialmente adequada a Lei nº 13.709/2018, carecendo de maior completude; (ii) e inexiste um programa formal de comunicação sobre informações de tratamentos e práticas do IBGE em relação a dados pessoais, favorecendo a conscientização dos servidores sobre importância do adequado uso de dados pessoais. (Achados nos 2, 3 e 4)

Destaca-se a relevância do tema com a publicação no Diário Oficial da União (DOU) da Emenda Constitucional nº 115/2022, a qual altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

A materialização constitucional do tema, além de fortalecer as previsões da LGPD, obriga todos os órgãos públicos, entidades privadas e pessoas que manejam dados de pessoas naturais a reverem suas normas e políticas internas.

Desta forma, implica que as organizações deverão implementar seus próprios mecanismos para adequação à legislação, que resultará em significativas mudanças nos sistemas normativos, processos e procedimentos de trabalho, visando atender aos anseios dos titulares dos dados pessoais.

Cabe ressaltar que a Auditoria Interna identificou boas e relevantes práticas conduzidas pelos gestores do IBGE nos esforços para a aderência do tratamento de dados pessoais às previsões estabelecidas pela LGPD, que demonstram o esforço, a dedicação e o comprometimento do CDDI e da DTI na busca do alcance dos objetivos operacionais, destacando-se:

- ✓ Participação do IBGE na política pública instituída pela SGD/MGI para fins da implementação do Programa de Governança da Privacidade, em que pese o desafio da realização de treinamento de servidores no tema e das dificuldades impostas pela atual disposição da estrutura organizacional;

- ✓ Formalização e endereçamento do Comitê de Adequação à Lei Geral de Proteção de Dados Pessoais (CLPGD) e da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), no âmbito da DTI; e

- ✓ Contratação de consultoria especializada no diagnóstico, planejamento, avaliação da conformidade e gerenciamento de riscos relacionados à gestão de proteção de dados pessoais.

Por fim, a Auditoria Interna entente que os principais benefícios esperados pela implementação das recomendações apresentadas neste relatório, pelos gestores responsáveis dos processos e subprocessos avaliados, são:

- ✓ Segurança jurídica a toda cadeia de valor envolvida, isto é, desde o titular do dado até o IBGE estarão amparados pela Lei;

- ✓ Mais transparência e segurança dos dados;

- ✓ Possibilidade de visualizar os dados pessoais desnecessários, os documentos e contratos que precisam ser adequados e o melhor local para armazenamento;

- ✓ Identificar o acesso às informações pessoais e a permissão para manuseá-las e tratá-las;

- ✓ Melhoria nos processos de governança, riscos e controles, com impacto positivo no atendimento às exigências dos órgãos de fiscalização; e

- ✓ Maior credibilidade pelo cidadão quanto imagem e atividade fim do IBGE.

CARLOS ALBERTO VIANNA COSTA
Auditor-Chefe
Auditoria Interna – AUD
IBGE

EQUIPE DE AUDITORIA

Servidor	Cargo
Adilson da Silva Marques	Assistente Técnico
Ennio Amorim Serrano Junior	Tecnologista Informação Geográfica e Estatística

ANEXO I

Manifestação da Unidade Examinada e Análise da Equipe de Auditoria

Os achados de auditoria e as recomendações associadas foram discutidos com os gestores da DTI e do CDDI em uma busca conjunta de soluções, por meio de reuniões específicas nos dias 25/10 e 01/11/2023, por meio da plataforma Webex.

Na oportunidade, os referidos gestores das Unidades compreenderam as constatações apresentadas e as sugestões indicadas pela Auditoria Interna do IBGE visando a mitigação de riscos e oportunidades e melhorias operacionais.

Os gestores da DTI decidiram por manifestar-se a respeito do Relatório incluindo informações no corpo do documento, e a Auditoria Interna do IBGE, no que coube, por existirem evidências e concordância, incluiu parte dos comentários ao Relatório.

Os gestores do CDDI realizaram comentários por meio de e-mail, que foram considerados na versão final deste Relatório.

Cabe ressaltar que informações encaminhadas pelo gestor da CDDI/COATI são pertinentes, mas encaixam-se melhor como argumentação quando da manifestação em relação às recomendações de auditoria, quando estiverem em monitoramento, servindo como base para indicação de prazo para a completa implementação das recomendações.

Foi informado que, de acordo com o previsto no Art. 4º da Norma de Tratamento dos Achados e Recomendações formulados pela Auditoria Interna do IBGE e de Solicitações, Recomendações e Determinações por Órgãos Externos de Controle, aprovada pela Resolução do Conselho Curador nº 01/2022, de 23/05/2022, a partir do encaminhamento pela AUD do Relatório de Auditoria para as Unidades Auditadas, os gestores destas Unidades Auditadas indicarão o tratamento a ser dado para os respectivos achados e recomendações, no prazo máximo de até 30 dias contados do recebimento do Relatório da Auditoria Interna.

Manifestação do CDDI em relação aos Achados de Auditoria:

1. Requisitos de privacidade ainda não foram capturados e consolidados de forma a ditar e a influenciar como os dados pessoais em suas mais variadas formas devem ser manuseados no seu ciclo de vida no IBGE
    a. Este item é uma avaliação da Auditoria.
2. Política de Segurança da Informação e Comunicação (POSIC) encontra-se desatualizada, compreendo o período relativo aos anos de 2017 a 2018
    a. Situação: Uma atualização da POSIC foi aprovada pelo Conselho Diretor.

3. Política de Privacidade de Dados (PP) encontra-se parcialmente adequada à Lei nº 13.709/2018
    a. Situação: A política de privacidade foi aprovada pelo Conselho Diretor. O "Termos de uso" já foi aprovada pelo Encarregado e pelo Comitê de Adequação do IBGE à LGPD - CLGPD e deve ser apreciado pelo Conselho Diretor do IBGE ainda este mês.

4. Inexistência de programas de capacitação e de comunicação sobre proteção de dados pessoais.
    a. Situação: Foram realizados no ano de 2023 três apresentações abertas a todos os funcionários, duas apresentações específicas para as áreas que iriam realizar o inventário de dados pessoais e uma capacitação para os órgãos de RH das Superintendências Estaduais. Foi demandado à Coordenação de Marketing apoio a uma campanha de "Pílulas do Conhecimento" que deve ser iniciada ano que vem.

5. Ausência de processos formalmente constituídos contemplando as respostas a possíveis incidentes afetos à gestão de dados pessoais, o fluxo das atividades de trabalho, à devida comunicação aos titulares dos dados e às autoridades competentes
    a. Situação: Embora o Encarregado de Dados e a DTI saibam o roteiro a ser percorrido em caso de uma confirmação de vazamento, realmente ainda não há uma formalização no IBGE.

6. Serviços de consultoria contratados para o diagnóstico, o planejamento, a avaliação da conformidade e o gerenciamento de riscos relacionados à gestão de proteção de dados pessoais no IBGE em consonância com a LGPD ainda não se iniciou

    a. Situação: A DTI contratou uma consultoria e o Comitê de Adequação do IBGE à LGPD utilizou o contrato para fazer reuniões com a consultora para esclarecer dúvidas e ela fez uma palestra de conscientização sobre a LGPD para os funcionários.

    b. Ressalta-se que são executados processos de varredura de vazamento de dados pelo SOC do IBGE de forma rotineira, com tratamento efetuado pela DTI e pelo Encarregado de Dados.

7. Fragilidade na concessão, revogação, monitoramento e controle periódico de acesso dos terceirizados e estagiários ao ambiente de rede de computadores e sistemas informatizados do IBGE

    a. Situação: O IBGE tem a política de renovação de senha periódica e está implementando a dupla autenticação, o acesso interno a partir do ano que vem só se dará dor computadores do IBGE que estarão bloqueados para instalação de softwares e contarão com antivírus atualizado.

    b. Atualmente medidas de contorno são tomadas para mitigar a falta deste cadastro.

8. Ausência de informação na política de backup quanto aos prazos de retenção, exclusões de dados pessoais e sincronismo entre sistemas e os bancos de dados.

    a. Quanto ao período de retenção, nos Arts. 15 e 16, a Lei 13.709/18 informa situações quando "Do Término do Tratamento de Dados", sendo importante ter informações sobre os prazos de retenção para os dados pessoais sensíveis. É fundamental

lembrar que apesar desses dois artigos, os dados coletados nas pesquisas do IBGE não possuem tempo de permanência em virtude da necessidade de manutenção das séries históricas.

9. Ausência de política e inventário de dados pessoais com as informações relevantes objetivando a identificação, principalmente, dos dados sensíveis e não sensíveis, para o devido tratamento.

    a. Situação: O Inventário de Dados Pessoais foi realizado na Sede do IBGE e terá uma atualização anual.

10. Relatório de Impacto à Proteção de Dados Pessoais (RIPD) ainda não foi elaborado em que pese a possibilidade de sua exigência por parte da Autoridade Nacional de Proteção de Dados Pessoais (ANPD).

    a. Situação: Embora a divulgação do RIPD não seja, em regra, obrigatória, a ANPD recomenda elaborar o RIPD em todo contexto em que as operações de tratamento de dados pessoais possam gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados. Desta forma, o Encarregado de Dados e o CLGPD estão envolvidos na elaboração do RIPD do Censo Agropecuário. Este trabalho visa compreender as dificuldades que as áreas do IBGE enfrentarão para elaborar o RIPD e poder ajudá-las nesse processo.

    b. O RIPD que o IBGE deve disponibilizar na Internet deve ser mais geral e não expor nenhuma informação que comprometa a segurança das informações armazenadas no IBGE.

11. Inexistência de levantamento dos contratos relacionados a dados pessoais impossibilita a avaliação e as necessárias adequações deles em relação a serviços que coletam, transferem e processam tais dados, assim, como não orienta os termos de contratações futuras na Instituição

    a. Situação: Nos contratos novos de TIC o IBGE já segue um *template* da CGU. Os demais contratos novos passam pela Procuradoria Federal do IBGE para serem aprovados.

    b. Não foi feito, ainda, um inventário sobre os contratos vigentes.

12. Canal de comunicação e divulgação sobre informações de tratamentos e práticas do controlador de dados pessoais no IBGE está desatualizado e com falha no acesso

    a. Os links com problemas serão corrigidos hoje ainda.

13. Ausência de monitoramento contínuo das ações de proteção de dados pessoais de forma geral, a fim de determinar o alinhamento e o progresso no cumprimento dos requisitos de conformidade com LGPD

    a. Situação: 99,9% das informações de dados pessoais que o IBGE trata são oriundas das pesquisas. Por estes dados estarem sob a Lei do Sigilo o monitoramento com a sua segurança e integridade são contínuos.

b. A maturidade do IBGE na adequação da LGPD avançou bastante. Em 2020 o nível de adequação era “básico” e em 2023 estamos no nível “Em aprimoramento”.

14. Acúmulo de funções do Encarregado de Dados com outros cargos e atividades pode afastar a independência necessária como canal de comunicação entre o agente de tratamento, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) e fragilizar a gestão de dados pessoais no IBGE

    a. É um grande desafio determinar o Encarregado de Dados. Na grande maioria das instituições não existe uma estrutura independente para o encarregado. A solução que muitas instituições estão adotando é a criação de uma área de apoio ao Encarregado de Dados, como um Comitê, a mesma solução que o IBGE adotou.

Documento assinado eletronicamente por CARLOS ALBERTO VIANNA COSTA, Auditor-Chefe, em 5 de Dezembro de 2023, às 16:50:41, horário de Brasília, com fundamento legal no § 3º do Art. 4º do Decreto Nº 10.543, de 13 de Novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://transparenciasda.ibge.gov.br/docs/validador.jsf informando o código verificador 5248262927618257179 e o código CRC 3CCE86DE.