CGU
Controladoria-Geral da União

RELATÓRIO DE AVALIAÇÃO

Serviço Federal de Processamento de Dados - Serpro

Exercício 2022

18 de agosto de 2023

Controladoria-Geral da União (CGU)
Secretaria Federal de Controle Interno (SFC)

RELATÓRIO DE AVALIAÇÃO
Órgão: **Ministério da Economia**
Unidade Auditada: **Serviço Federal de Processamento de Dados - Serpro**
Município/UF: **Brasília/DF**
Relatório de Avaliação: **1360586**

Missão
Elevar a credibilidade do Estado por meio da participação social, do controle interno governamental e do combate à corrupção em defesa da sociedade.

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 à Unidade Auditada, e contribuir para o seu aprimoramento.

QUAL FOI O TRABALHO REALIZADO PELA CGU?

O objetivo das análises foi o de verificar a aplicação de boas práticas e normas de Segurança da Informação relacionadas a Lei Geral de Proteção de Dados (Lei Federal nº 13.709/2018).

Dessa forma, foram verificadas as normas de Segurança da Informação utilizadas no Serpro e as ferramentas para sua aplicação.

Ainda, foram analisados, em relação aos temas segurança da informação e LGPD, três contratos com os principais clientes da estatal (Diretoria de Administração e Logística do Ministério da Economia, Receita Federal do Brasil e Secretaria do Tesouro Nacional), bem como a aplicação da LGPD no Acordo de Cooperação Técnica com a empresa Drumwave e no serviço Datavalid.

POR QUE A CGU REALIZOU ESSE TRABALHO?

O presente trabalho tem como foco a segurança da informação aplicada ao tema Proteção de Dados, o qual tem sua relevância positivada na Lei Geral de Proteção de Dados (Lei Federal nº 13.709/2018).

Considerou-se também que o Serpro tem como visão: "Ser reconhecida como a empresa que viabiliza o governo digital" e como um de seus objetivos estratégicos: "Ser líder em soluções biométricas e de identificação digital no Brasil". Além disso, o Serpro é um dos principais operadores de bases de dados pessoais da administração pública federal, tornando-o peça chave na aplicação da LGPD no Brasil.

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

No geral, a estatal editou normas relativas à Gestão de Vulnerabilidades, *Backup*, *Logs,* ETIR - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos, Encarregado de Dados, Controles de Acesso, além de utilizar *softwares* específicos como ferramentas de apoio.

Esses temas também foram analisados nos contratos com clientes do Serpro, momento em que se verificou a ausência de tratamento de alguns deles em determinados contratos. Com isso, foi recomendada a realização de estudos para atualizar e uniformizar o tratamento dos temas segurança da informação e LGPD nos contratos do Serpro com seus clientes, de forma a se adequar às melhores práticas relacionadas ao assunto.

LISTA DE SIGLAS E ABREVIATURAS

ANPD - Agência Nacional de Proteção de Dados

Backup - Cópia de segurança de dados

CEH - *Certified Ethical Hacker*

CHFI - *Computer Hacking Forensic Investigator*

CISSP - *Certified Information Systems Security Professional*

CIS V8 CONTROLS - CIS *Critical Security Controls Version* 8

COGRS - Comitê Estratégico de Governança, Riscos, Controles e Segurança da informação

CGU - Controladoria Geral da União

DDoS - *Distributed Denial of Service*

ETIR - Equipe de Tratamento de Incidentes e Riscos

GDPR - *General Data Protection Regulation*

IPS - *Intrusion prevention system*

LGPD - Lei Geral de Proteção de Dados

Log - Registro de eventos ou atividades

PAM - *Privileged Access Management*

PGPPD - Programa de Governança em Privacidade e Proteção de Dados Pessoais do Serpro

PNSI - Política Nacional de Segurança da Informação

PPD - Privacidade e Proteção de Dados Pessoais

PPPD - Política Serpro de Privacidade e Proteção de Dados

SIEM - *Security Information and Event Management*

SOC - *Security Operation Center*

SUPPD - Superintendência Proteção de Dados Pessoais

SUMÁRIO

INTRODUÇÃO

O Serviço Federal de Processamento de Dados – Serpro é uma empresa pública, vinculada ao Ministério da Fazenda, e tem por objeto, nos termos da Lei nº 5.615, de 13 de outubro de 1970, a execução de serviços de tratamento de informações e processamento de dados, através de computação eletrônica ou eletromecânica e a prestação de assistência no campo de sua especialidade.

O presente trabalho teve como foco a segurança da informação aplicada ao tema Proteção de Dados, o qual tem sua relevância positivada na Lei Federal nº 13.709/2018, denominada Lei Geral de Proteção de Dados (LGPD). Considerou-se também que o Serpro tem como visão: "Ser reconhecida como a empresa que viabiliza o governo digital" e como um de seus objetivos estratégicos: "Ser líder em soluções biométricas e de identificação digital no Brasil". Além disso, o Serpro é um dos principais operadores de bases de dados pessoais da administração pública federal, tornando-o peça chave na aplicação da LGPD no Brasil.

O objetivo das análises foi o de verificar a aplicação de boas práticas e normas de Segurança da Informação relacionadas a Lei Geral de Proteção de Dados – LGPD (Lei Federal nº 13.709/2018). Dessa forma, foram verificadas as normas de Segurança da Informação utilizadas pelo Serpro e as ferramentas para sua aplicação. Ainda, foram analisados, em relação aos temas segurança da informação e LGPD, três contratos com os principais clientes da estatal (Diretoria de Administração e Logística do Ministério da Economia, Receita Federal do Brasil e Secretaria do Tesouro Nacional), bem como a aplicação da LGPD no Acordo de Cooperação Técnica com a empresa Drumwave e no serviço Datavalid, oferecido a clientes pela estatal.

Dessa forma, buscou-se responder as seguintes questões de auditoria:

1. Os controles relacionados à segurança da informação adotados pela empresa, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, são suficientes?
2. Há um compromisso claro da alta administração em definir e fazer cumprir altos padrões de segurança da informação e de privacidade?
3. São adotadas medidas de segurança, técnicas e administrativas suficientes e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito?
4. As atividades de tratamento de dados pessoais observam a boa-fé, a necessidade e a limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados?

De modo a suportar as respostas às questões de auditoria propostas, foram analisadas as normas internas do Serpro e a legislação aplicável ao tema. Complementarmente, foram

realizadas reuniões com a equipe técnica da estatal e emitidas solicitações de informações adicionais, além de pesquisas de melhores práticas do setor.

Durante a auditoria foram utilizados os critérios a seguir, entre outros pertinentes:

- O Decreto nº 9.637/2018 e a IN GSI nº 01, de 27/05/2020, juntamente com suas normas complementares, os quais estabelecem diretrizes e políticas para a proteção da informação e segurança cibernética.
- O Acórdão nº 1.109/2021 do Tribunal de Contas da União (TCU) que é uma referência para auditorias em segurança da informação, enquanto o Guia do *Framework* de Segurança – CIS *Controls* v8 e a ABNT NBR ISSO/IEC 27002/2013 são referências internacionais nos temas Segurança da Informação, Segurança Cibernética e Proteção da Privacidade.
- As políticas de segurança da informação, *backup*, gestão de vulnerabilidades, gestão de logs, EITR (Equipe de Tratamento e Resposta a Incidentes) e controles de acesso são cruciais para proteger as informações e dados da organização. Essas políticas são regulamentadas por diversas normas e regulamentos, incluindo o Decreto nº 9.637/2018, IN GSI Nº 01, NC nº 05/IN01/DSIC/GSIPR, e NC nº 21/IN01/DSIC/GSIPR, entre outros.
- Além disso, a Lei nº 12.965 – Marco Civil da Internet, Art. 13, e a NC nº 21/IN01/DSIC/GSIPR Art. 6.6 e 7.2, juntamente com o artigo 5º da LGPD (Lei Geral de Proteção de Dados), que define os papéis de controlador e operador, e o artigo 7º, que estabelece o enquadramento legal para o tratamento de dados, são fundamentais para assegurar a proteção adequada de informações pessoais.
- As transferências de dados, tanto para pessoa jurídica de direito privado (artigos 26 e 27) quanto internacionais (artigo 33), também são regulamentadas pela LGPD e outras normas e regulamentos.

No geral, a estatal editou normas, seguindo boas práticas e normativos pertinentes, relativas à Gestão de Vulnerabilidades, *Backup*, *Logs,* ETIR, Encarregado de Dados, Controles de Acesso, além de utilizar *softwares* específicos como ferramentas de apoio. Além de ter tratado especificamente, por meio de normas e controles, da privacidade de dados e temas específicos da LGPD.

Cabe destacar que a auditoria foi executada conforme os padrões previstos no Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal, IN SFC nº 03/2017, e no Manual de Orientações Técnicas da Atividade de Auditoria Interna Governamental do Poder Executivo Federal, IN SFC nº 08/2017. Nenhuma restrição foi imposta aos trabalhos ao longo da auditoria.

RESULTADOS DOS EXAMES

1. Normatização adequada do papel do Encarregado de Dados – LGPD

O Encarregado de Dados (ou *Data Protection Officer*, em inglês) é uma função crítica para empresas de TI que processam dados pessoais de clientes, funcionários e parceiros de negócios. É responsável por garantir que a empresa esteja em conformidade com as leis de proteção de dados, como a LGPD no Brasil e a GDPR na União Europeia. Além disso, ele deve garantir que a empresa esteja implementando as melhores práticas de privacidade de dados, realizando avaliações de impacto na privacidade, gerenciando incidentes de segurança de dados e educando os funcionários sobre suas responsabilidades em relação à proteção de dados.

No Serpro o próprio encarregado de dados conceituou a função: "O encarregado, como o guardião da privacidade, tem a responsabilidade de preservar os princípios da segurança da informação e da privacidade no âmbito interno e na relação com controladores e ANPD. Pelo ineditismo desse relacionamento, é um grande desafio"[1].

A LGPD informa que o encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)[2]. Ademais, o art. 41 da LGPD dispõe acerca das funções do Encarregado de Dados.

Nesse diapasão, verificou-se que o Serpro foi mais além e editou norma instituindo a Rede Serpro De Privacidade E Proteção De Dados – GE011.V01: rede de profissionais formada pelos subencarregados e DPO locais, que tem como objetivo internalizar, sob a coordenação e supervisão da equipe do encarregado, as ações necessárias para adequação do Serpro à Lei Geral de Proteção de Dados – LGPD, bem como a disseminação de conhecimento, adoção de boas práticas e a elaboração (em conjunto com a SUPPD) e implementação de normas e processos relacionadas à privacidade e proteção de dados pessoais (PPD) em todas as áreas da Empresa. Definiu ainda que, por padrão, o encarregado de dados é o Superintendente titular da SUPPD que exerce, com o apoio do Comitê Estratégico de Governança, Riscos, Controles e Segurança da informação – COGRS, a coordenação da Governança de Privacidade, sob a égide da Política Serpro de Privacidade e Proteção de Dados – PPPD, dando cumprimento ao Programa de Governança em Privacidade e Proteção de Dados Pessoais do Serpro – PGPPD.

[1] https://www.serpro.gov.br/lgpd/noticias/2020/dpo-encarregado-dados-serpro-entrevista. Acesso em 25mai2023.
[2] Lei Geral de Proteção de Dados (Lei Federal nº 13.709/2018), art. 5º, inciso VII.

Diante disso, a alta administração da estatal demonstra compromisso em definir e fazer cumprir padrões de segurança da informação e de privacidade no que diz respeito ao cargo de Encarregado de Dados.

2. A Política de Segurança da Informação e as Normas Complementares foram estabelecidas de forma adequada

O Decreto nº 9.637/2018, art. 15, inciso II, estabelece que, aos órgãos e às entidades da administração pública federal, em seu âmbito de atuação, compete elaborar sua política de segurança da informação e as normas internas de segurança da informação, observadas as normas de segurança da informação editadas pelo Gabinete de Segurança Institucional da Presidência da República.

Já Instrução Normativa nº 01 do GSI, de 27/05/2020 estabelece as principais diretrizes para elaboração da Política de Segurança da Informação (PSI) especificamente em seu capítulo III. O artigo 9º define a obrigatoriedade de instituição de PSI em todos as entidades da administração pública, a qual deve ter por objetivo estabelecer diretrizes, responsabilidades, competências e subsídios para a gestão da segurança da informação.

Dessa forma, o Serpro editou a Política Corporativa De Segurança Da Informação – SG018/2019, com previsão de revisões a cada 3 anos, conforme item 7.4. da norma, a qual visou cumprir a diretriz normativa citada na completude de seus comandos. Além disso, foram editadas normas relativas aos aspectos técnicos de segurança que serão verificados no decorrer deste relatório. Ademais foi editada a Política Serpro De Privacidade e Proteção De Dados – PPPD (GE18/2020).

Ainda é possível citar a elaboração da Política Corporativa de Gestão de Riscos e Controles Internos; do Programa De Governança Em Privacidade E Proteção De Dados Pessoais Do Serpro – PGPPD – GE 060/2022.

Diante disso, a alta administração da estatal demonstra compromisso em definir e fazer cumprir altos padrões de segurança da informação e de privacidade no que diz respeito à Políticas de Segurança da Informação e Privacidade.

3. Adequada previsão do Comitê e Gestor de Segurança da Informação

Para tomada de decisão e operacionalização das políticas relacionadas à segurança da informação foi instituído o Comitê Estratégico De Governança, Riscos, Controles e Segurança Da Informação – COGRS. Órgão de assessoramento à Diretoria Executiva, define como coordenador titular o Diretor Jurídico e de Governança e Gestão – DIJUG e seu substituto

Diretor de Operações – DIOPE. Em sua composição constam os superintendentes das diversas áreas da estatal que deliberam e discutem sobre:

a) Política Corporativa de Gestão de Riscos e Controles Internos;
b) Política de Conformidade;
c) Política de Governança Corporativa do Serpro;
d) Política Corporativa de Segurança da Informação do Serpro;
e) Política Corporativa de Continuidade do Negócio;
f) Política Corporativa de Governança de Dados; e
g) Política Corporativa de Privacidade e Proteção de Dados Pessoais.

Dito isso, verifica-se a conformidade com o Decreto nº 9.637/2018, art. 15, inciso III e IV, os quais estabelecem a necessidade de os órgãos da administração pública federal definirem gestores de segurança da informação e o comitê de segurança da informação.

4. Implementação de processos de Gestão de *Backup*s

O *backup* ou cópia de segurança é um mecanismo fundamental para garantir a disponibilidade da informação, caso as bases onde a informação esteja armazenada sejam danificadas, roubadas ou estejam indisponíveis. A gestão de *backup* é parte chave da segurança da informação e deve passar por pelas seguintes etapas segundo o referencial *CIS V8 Controls*: estabelecer e manter um processo de recuperação de dados, fazer *backup*s automatizados, proteger os dados de recuperação, estabelecer e manter uma instância isolada de dados de recuperação, teste de recuperação de dados.

Para tanto, o Serpro elaborou a Norma CD 017 V06 – *Backup* e restauração de dados, a qual define o escopo de dados a serem retidos dividindo em plataformas (alta e baixa) e ambiente (homologação, testes, treinamento, desenvolvimento e produção). É também definida a duração de retenção e periodicidade realização de cada *backup*. São definidos critérios de acesso físico e lógico, além de estabelecer que os *backup*s devem ser mantidos em sala cofre. Por fim, são definidas as regras para testes de recuperação de dados.

Além disso, o Serpro informou que utiliza (*Informações suprimidas por solicitação do Serpro, em função de sigilo, na forma das Leis nº 5.615/1970, 9.279/1996, 9.609/1998, 9.874/1999, 10.180/2001, 12.527/2011, entre outras)* para gestão de *backup*s no âmbito operacional. Ainda foi realizada visita técnica ao *datacenter*[3] de Brasília, onde foi possível observar os servidores de *backup* em funcionamento.

[3] Centro de processamento de dados: um centro de processamento de dados (CPD), também conhecido como *data center*, é um local onde estão concentrados os sistemas computacionais de uma empresa ou organização, como um sistema de telecomunicações ou um sistema de armazenamento de dados, além do fornecimento de energia para instalação.

Vale destacar que o *datacenter* está passando por processo de certificação UPTIME[4], Tier III[5], com projeto aprovado, o qual busca certificar o referido datacenter. Além disso, a estatal informou que na Regional São Paulo – Socorro, está sendo implementado um novo Data Center modular, contratado junto à empresa Green4T, (*Informações suprimidas por solicitação do Serpro, em função de sigilo, na forma das Leis nº 5.615/1970, 9.279/1996, 9.609/1998, 9.874/1999, 10.180/2001, 12.527/2011, entre outras)*. Após o início dessa operação será iniciada a migração dos ativos hospedados no Data Center atual para as novas instalações.

Diante disso, a alta administração da estatal demonstra compromisso em definir e fazer cumprir padrões de segurança da informação e de privacidade no que diz respeito à gestão de *backup*s, tendo como referência especialmente Acórdão 1.109/2021 – Plenário Tribunal de Contas da União (TCU) e Guia do *Framework* de Segurança – CIS *Controls* v8 – Controle 11: Recuperação de Dados. Destaca-se ainda que cabem melhorias a exemplo da busca pela certificação dos *datacenters* da estatal.

5. Adequação do processo de Gestão de Vulnerabilidades e previsão de Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR

A Norma SG 031, versão 03 de 2021 – TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO, a qual tem por finalidade regulamentar a estrutura, a forma de trabalho, as responsabilidades e os relacionamentos para o tratamento de incidentes de segurança da informação no Serpro. Segundo o item 3 alínea "m" dessa norma, o *Security Operation Center* – SOC representa a ETIR do Serpro. Dessa forma, é importante delimitar conceitos gerais.

SOC é um centro de operações de segurança que consiste em uma equipe especializada de profissionais responsáveis por monitorar, detectar, analisar e responder a incidentes de segurança em sistemas de informação e redes de computadores. A equipe SOC é responsável por garantir a segurança cibernética da organização, identificando possíveis ameaças cibernéticas e tomando medidas para mitigar os riscos. No Serpro, este é dividido em 3 níveis conforme a complexidade dos incidentes de segurança[6].

Uma equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos é essencial para garantir a segurança cibernética em organizações públicas e privadas. De acordo com a Política Nacional de Segurança da Informação (PNSI) estabelecida pelo Decreto Nº 9.637/2018, a ETIR é uma das principais medidas para garantir a proteção dos sistemas de informação e redes

[4] *Uptime Institute Tier Classification System - Uptime Institute* < https://pt.uptimeinstitute.com/tiers> acesso em 25.04.2023

[5] Um datacenter Tier III é *concurrently maintainable* com componentes redundantes como um diferenciador de chaves, com caminhos de distribuição redundantes para atender ao ambiente crítico. Diferentemente dos Tier I e Tier II, essas instalações não exigem desligamentos quando o equipamento precisar de manutenção ou substituição. Os componentes do Tier III são adicionados aos componentes Tier II de modo que qualquer peça possa ser desligada sem afetar a operação de TI. < https://pt.uptimeinstitute.com/tiers> acesso em 25.04.2023

[6] Norma SG 031, versão 03 de 2021, item 3, 'j', 'k', 'l'.

contra-ataques cibernéticos. A ETIR é responsável por identificar e avaliar a natureza dos incidentes, coordenar ações para a mitigação e recuperação dos danos causados, bem como propor medidas preventivas para evitar que incidentes similares ocorram no futuro.

A Instrução Normativa Nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, estabelece que a ETIR deve ser composta por membros qualificados e treinados, capazes de identificar e analisar possíveis vulnerabilidades nos sistemas de informação. Além disso, a equipe deve possuir conhecimento técnico e expertise para lidar com diversos tipos de ataques cibernéticos, desde os mais simples até os mais sofisticados. É importante destacar que a equipe também deve estar preparada para lidar com incidentes graves e de grande impacto, como vazamento de dados pessoais sensíveis.

Por fim, a equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos deve estar sempre atualizada sobre as melhores práticas de segurança da informação e as novas tendências em cibersegurança. A NC nº 05/IN01/DSIC/GSIPR estabelece que a ETIR deve realizar treinamentos e exercícios periódicos, a fim de manter seus membros capacitados e preparados para lidar com incidentes cibernéticos. Além disso, a equipe deve manter contato com outras organizações e autoridades responsáveis pela segurança da informação, a fim de compartilhar conhecimentos e informações relevantes para a prevenção de incidentes cibernéticos.

Informações suprimidas por solicitação do Serpro, em função de sigilo, na forma das Leis nº 5.615/1970, 9.279/1996, 9.609/1998, 9.874/1999, 10.180/2001, 12.527/2011, entre outras[7].

Ainda, verifica-se a vigência de normas de segurança relativas à gestão de vulnerabilidades:

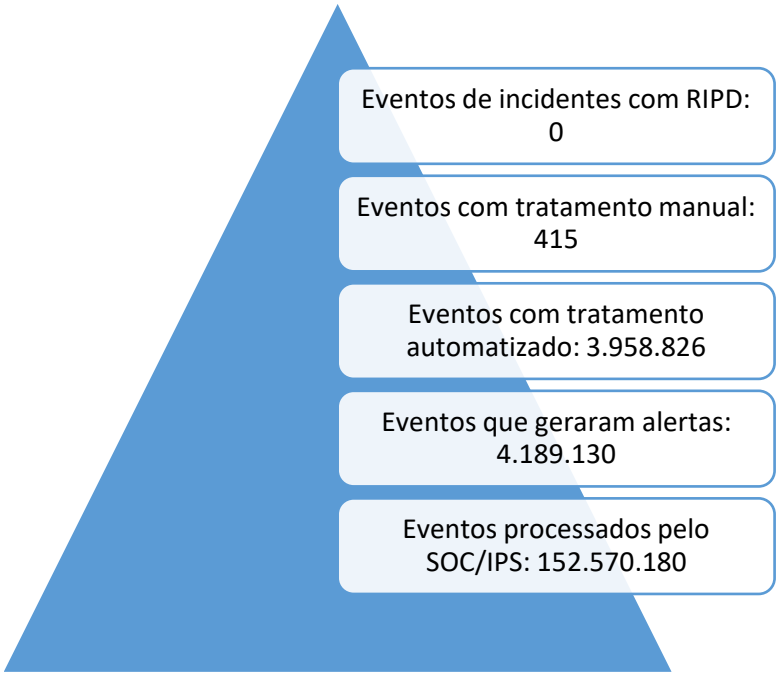
- Norma SG 09, versão 4, Processo Forense Computacional do Serpro – Determina a melhoria de gestão de vulnerabilidades por meio de retroalimentação do processo com base em recomendações advindas do processo forense;
- Norma SG 20, versão 2, Segurança do Ambiente Virtualizado em Plataforma Avançada – Determina que a máquina servidora virtual deve passar por todos os processos de segurança, incluindo análise de vulnerabilidades;
- Norma SG 22, versão 5, Regras de Acesso à Rede – Trata de possíveis vulnerabilidades na rede;
- Norma SG 30, versão 2, Segurança de Ambiente de Contêineres em Nuvem Privada – Determina requisitos de análise de vulnerabilidade no uso de nuvem privada;

[7] Informações suprimidas por solicitação do Serpro, em função de sigilo, na forma das Leis nº 5.615/1970, 9.279/1996, 9.609/1998, 9.874/1999, 10.180/2001, 12.527/2011, entre outras.

- Norma SG 31, versão 3, Tratamento de Incidentes de Segurança da Informação – trata das competências da equipe de segurança da informação e do fluxo que deve ser adotado no tratamento dos incidentes;
- Norma SG 35, versão 1, Segurança de Soluções Digitais – Trata de análise de vulnerabilidade de *softwares*;

Ademais a equipe de segurança da informação apresentou os números do "funil" de SOC para os últimos 12 meses (setembro de 2021 a agosto de 2022):

Figura 1 – Funil de SOC no âmbito do Serpro



Fonte: Elaboração própria a partir de resposta à Solicitação de Auditoria nº 03/1107672.

Informações suprimidas por solicitação do Serpro, em função de sigilo, na forma das Leis nº 5.615/1970, 9.279/1996, 9.609/1998, 9.874/1999, 10.180/2001, 12.527/2011, entre outras[8].

[8] Informações suprimidas por solicitação do Serpro, em função de sigilo, na forma das Leis nº 5.615/1970, 9.279/1996, 9.609/1998, 9.874/1999, 10.180/2001, 12.527/2011, entre outras.

Diante do exposto, verifica-se que a alta administração da estatal demonstra compromisso em definir e fazer cumprir padrões de segurança da informação e de privacidade no que diz respeito ao processo de gestão de vulnerabilidades.

6. Gestão adequada de Controle de Acessos

O art. 12, inciso IV, alínea "f" da Instrução Normativa GSI nº 1, de 27 de maio de 2020, prevê a necessidade de estabelecer regras de acesso aos sistemas e informações da organização na Política de Segurança da Informação.

A Norma Complementar Nº 07/IN01/DSIC/GSIPR define os requisitos para o controle de acesso, incluindo a necessidade de autenticação, autorização e registro de atividades de acesso (*logs*), o que está alinhado ao CIS *Controls* v8 – Controle 06: Gestão do controle de acesso e a ABNT NBR ISSO/IEC 27002/2013 – 9 – Controle de Acesso.

Assim, visando normatizar o acesso lógico e o acesso físico, o Serpro editou a Norma SG 37, versão 1, Gestão de Identidade e Controle de Acesso Lógico aplicada às informações, sistemas e serviços corporativos do Serpro, visando a proteção dos ativos de informação contra o acesso não-autorizado e editou a Norma SG 33, versão 3, Segurança e Controle de Acesso às Instalações dos Data Centers do Serpro. Além disso, foi editada a Norma SG 32, versão 2, Segurança e Controle de Acesso às Instalações das Salas de Equipamentos.

Por fim, verificou-se que para auxílio na implantação das referidas normas e políticas de segurança o Serpro utiliza Solução de PAM (*Privileged Access Management*)[9] por meio de Cofre de Senhas, que deve ser uma área segura para armazenar e gerenciar as senhas de contas privilegiadas. Com o cofre de senhas, os administradores devem controlar o acesso às senhas e garantir que apenas usuários autorizados possam acessá-las.

[9] Solução de PAM (*Privileged Access Management*) é uma ferramenta de segurança que gerencia e controla o acesso a contas privilegiadas em sistemas e redes, limitando o risco de comprometimento ou roubo de informações sensíveis.

Diante disso, a alta administração da estatal demonstra compromisso em definir e fazer cumprir padrões de segurança da informação e de privacidade no que diz respeito à gestão de controles de acesso.

7. Ausência de cláusulas relativas à Segurança da Informação e LGPD nos contratos com maiores clientes do Serpro.

Além da verificação do conteúdo normativo de segurança da informação do Serpro, buscou-se analisar a presença do tema segurança da informação e LGPD nas regras contratuais com seus maiores clientes (Secretaria da Receita Federal do Brasil, Secretaria do Tesouro Nacional e Diretoria de Administração e Logística do Ministério da Economia), considerando seu papel como fornecedor e prestador de serviços de Tecnologia da Informação.

Foram objeto de análise os instrumentos contratuais do Serpro com cada cliente e verificada a presença de regras relativas a: gestão de *logs*; controles de acesso; gestão de *backup*s; ETIR e gestão de vulnerabilidades; e LGPD.

O contrato com a Receita Federal (Serviços de TI nº 19/2018), exceto no que se refere à ETIR e Gestão de Vulnerabilidades, não está atualizado em relação aos principais temas de segurança da informação citados no parágrafo anterior. Não foram identificadas clausulas que tratem de gestão de *logs*; controles de acesso; e gestão de *backups*. Ademais, é importante a definição de requisitos de segurança da informação não só a nível de contrato, como também a nível de cada aplicação ou *software* de serviço do cliente.

No caso da Secretaria do Tesouro Nacional (Serviços Estratégicos de Tecnologia da Informação e Comunicação – TIC – 03/2022) o contrato aborda os principais temas de segurança da informação atendendo a boas práticas de gestão de segurança. Destaca-se, porém, que não há menção à gestão de logs, uma das principais ferramentas forenses para responsabilização no caso de incidentes de segurança da informação. Essa situação poderia tratada com a previsão de cláusulas como prazo de retenção e prazo de recuperação ou mesmo por indicadores de nível de serviços, além de delimitação das responsabilidades entre fornecedor e cliente.

Por fim, o contrato com a Diretoria de Administração e Logística do Ministério da Economia (Prestação de Serviços Estratégicos de Tecnologia da Informação e Comunicação TI #173237) aborda os principais temas de segurança da informação atendendo a boas práticas de gestão de segurança. Há uma definição de requisitos de segurança da informação não só a nível de contrato, como também a nível de cada aplicação ou *software* de serviço do cliente.

As deficiências apontadas em relação aos contratos com a RFB e a STN podem gerar insegurança jurídica para ambas as partes em eventual ocorrência de um incidente de segurança da informação. A ausência de regras específicas também pode acarretar deficiências no tratamento de incidentes.

Não obstante as situações consignadas neste achado em relação aos três contratos objetos de análise pela equipe de auditoria, o Serpro destacou em manifestação ao relatório preliminar que para os “contratos padronizados”, que respondem por cerca de 95% dos

acordos da empresa, existem clausulas específicas dos temas Segurança da Informação e LGDP, conforme previsão em minuta padrão.

As cláusulas exemplificadas de Segurança da Informação, trazidas pela empresa em sua manifestação, têm como foco apenas a confidencialidade das informações, restando ausentes outros temas específicos (gestão de backups, de logs, de vulnerabilidades etc), de modo que se mitigue o risco de ineficiência no tratamento de incidentes de segurança da informação.

Já as cláusulas sobre LGPD trazem a necessidade de o Cliente garantir os princípios da LGPD no seu relacionamento com o Titular do Dado, inclusive destacando ao Titular a finalidade do uso da informação para evitar suspensão contratual junto ao Serpro, denotando a necessidade de garantir ao titular dos dados o exercício de seus direitos elencados na Lei e a necessidade de informar a finalidade do tratamento de dados ao titular dos dados.

Portanto, ainda que o Serpro adote documento modelo com previsão de tratamento dos temas segurança da informação e LGPD, entende-se que há possibilidade de aprimoramento tanto nas clausulas previstas nas minutas padrão quanto no tratamento de contratos específicos com grandes clientes (sem desconsiderar que o contrato é um acordo firmado entre as partes e há um processo negocial nas respectivas clausulas a serem previstas).

8. Avaliação da adequação dos serviços Datavalid e Biovalid aos requisitos da LGPD.

Considerando que o Serpro é operador de bases de dados cadastrais governamentais, a estatal oferece os serviços pagos de validação de dados chamados Datavalid e Biovalid. Segundo a estatal[10], o Datavalid faz "validações a partir de dados, imagens e fotos, em bases oficiais e atualizadas do governo". Já o Biovalid realiza "prova de vida (*liveness*) com validação biométrica facial junto às bases oficiais do governo, assegurando a individualização do titular dos dados com alto grau de confiabilidade e segurança."

Esses serviços têm por finalidade auxiliar, por exemplo, na prevenção a fraude, abertura de contas e contratação de produtos financeiros e têm como público, segundo a estatal: instituições financeiras; locadoras de veículos; aplicativos; companhias aéreas; seguradoras; *e-commerce*; empresas de tecnologia; empresas de varejo[11].

Os serviços apresentados realizam operações que se enquadram no conceito de tratamento de dados pessoais trazidos pela LGPD em seu art. 5º, inciso X, portanto, estão sujeitos aos mandamentos desta lei.

> Lei 13.709/2018 - LGPD
>
> Art. 5º Para os fins desta Lei, considera-se:
>
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento,

[10] https://www.loja.serpro.gov.br/biovalid
[11] https://www.loja.serpro.gov.br/biovalid

> eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Diante disso, destaca-se a necessidade de conformidade da atuação da estatal, na sua função de operador do dado, aos requisitos legais. Verifica-se que a LGPD, em seu art. 7º, enumera esses requisitos:

> Lei 13.709/2018 - LGPD
>
> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> I - mediante o fornecimento de consentimento pelo titular;
>
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
>
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
>
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
>
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
>
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
>
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiros;
>
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência
>
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
>
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Verifica-se, como requisito de conformidade com a LGPD, o enquadramento que a estatal identifica para o tratamento de dados, conforme os incisos listados no art. 7.

Informações suprimidas por solicitação do Serpro, em função de sigilo, na forma das Leis nº 5.615/1970, 9.279/1996, 9.609/1998, 9.874/1999, 10.180/2001, 12.527/2011, entre outras.

Diante disso, a fim de evitar duplicação de esforços da administração pública sobre o mesmo tema, além das tratativas em andamento da autoridade de dados junto ao Serpro para melhor enquadrar os serviços aos ditames da LGPD, este relatório de auditoria não se aprofundou na análise da cobformidade dos serviços de validação de dados da estatal.

9. Acordo de Cooperação Drumwave.

Em 10 de junho de 2022 foi publicado no Diário Oficial da União extrato de Acordo de Cooperação do Serpro com a empresa Drumwave. Identificou-se que o Acordo faria parte de uma das iniciativas de interoperabilidade de dados dentro do poder público por meio do programa Conecta gov.br. Segundo a Secretaria de Governo Digital do Ministério da Economia - SGD[12], considerando o arcabouço normativo do Governo Digital e a LGPD, a Secretaria teria realizado análises e ações no âmbito de um projeto chamado Governo como Plataforma, que prevê o empoderamento do cidadão no uso de seus dados para ter acesso a serviços públicos e privados. Nesse contexto, a Secretaria teria identificado, junto com o Serpro, modelo da empresa Drumwave que disponibiliza uma carteira de dados ao cidadão (*data wallet*), em que ele pode administrar seus dados pessoais.

Diante do escopo do acordo e de que a empresa participante seria sediada no exterior foram verificados alguns pontos de atenção no Acordo de Cooperação considerando a conformidade com a LGPD e os aspectos de segurança da informação adotados durante o Acordo. Ainda foi analisado o processo de seleção do parceiro no Acordo.

Assim, no que diz respeito aos aspectos da LGPD, verificou-se que a ANPD analisou o caso por meio da Nota Técnica 75/2022/CGF/ANPD[13], de 14 de setembro de 2022, na qual a Agência concluiu pela sua desnecessidade de atuação considerando que, no escopo do Acordo de Cooperação, somente seriam compartilhados metadados e não dados pessoais, sendo os primeiros não abrangidos pela LGPD. De toda forma, a Agência alertou que o Serpro deveria emitir comunicação no caso de, em momento posterior, avançar no projeto de *data wallet* com efetivo compartilhamento de dados pessoais.

Já a equipe de auditoria desta Controladoria emitiu Solicitação de Auditoria elencando “riscos ao SERPRO decorrentes de possíveis falhas no Acordo de Cooperação Serpro – Drumwave (2022)”. Foram apontados os dois riscos a seguir:

Risco 01: Desequilíbrio no direito à propriedade intelectual do produto a ser desenvolvido.

Risco 02: Prejuízo à isonomia, competitividade e vantajosidade na seleção de futuro fornecedor na etapa de comercialização do produto desenvolvido no atual Acordo de Cooperação.

Sobre os riscos apontados pela equipe de auditoria, o Serpro informou, em resposta à Solicitação de Auditoria, que não são aplicáveis a esta fase do projeto, a qual trata-se de prova de conceito. Caso o projeto avançasse para a fase comercial, os riscos apontados na Solicitação

[12] Nota Técnica SGD 34131/2022/ME (SEI nº 3536667)

[13] Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/nota-tecnica-no-75-2022-cgf-anpd-serpro-e-drumwave.pdf.

de Auditoria restam explicitados e inescusáveis de serem ignorados. A estatal ainda informou que o projeto foi concluído.

Após questionamento pela equipe de auditoria, o Serpro elaborou e apresentou Relatório Final do Acordo de Cooperação. Destaque-se que o relatório descreve o histórico do acordo e aponta riscos e oportunidades de um projeto *data wallet,* e, embora não tenha sido objeto da auditoria se debruçar sobre seu teor, entende-se que poderia ter havido maior aprofundamento da estatal acerca da viabilidade técnica do projeto.

Diante do exposto, restou claro o intuito do projeto de *data wallet* como ferramenta empoderamento do cidadão e alinhamento com o projeto de Governo como Plataforma, assim como ficou clara a sensibilidade do tema por se tratar de dados pessoais.

RECOMENDAÇÕES

1 – Realizar estudo com o objetivo de identificar melhorias no âmbito dos contratos com clientes do Serpro em relação aos temas segurança da informação e LGPD, avaliando a possibilidade de atualizar e uniformizar entendimentos, bem como prever requisitos mínimos nos acordos, aderentes às melhores práticas do assunto.

Achado n° 7

CONCLUSÃO

O presente trabalho teve por objetivo verificar a aplicação de boas práticas e normas de Segurança da Informação relacionadas a Lei Geral de Proteção de Dados – LGPD (Lei Federal nº 13.709/2018) no âmbito do Serpro.

Em suma, durante os exames, buscou-se responder às seguintes questões de auditoria:

1. Os controles relacionados à segurança da informação adotados pela empresa, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, são suficientes?
2. Há um compromisso claro da alta administração em definir e fazer cumprir altos padrões de segurança da informação e de privacidade?
3. São adotadas medidas de segurança, técnicas e administrativas suficientes e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito?
4. As atividades de tratamento de dados pessoais observam a boa-fé, a necessidade e a limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados?

Nesse sentido, verificou-se que a alta administração da estatal demonstra compromisso em definir e fazer cumprir padrões de segurança da informação e de privacidade no que diz respeito ao cargo de Encarregado de Dados, no que diz respeito à Políticas de Segurança da Informação e Privacidade.

Ainda se verificou a conformidade com o Decreto nº 9.637/2018, art. 15, incisos III e IV, os quais estabelecem a necessidade de os órgãos da administração pública federal definirem gestores de segurança da informação e o comitê de segurança da informação.

A nível tático, a alta administração da estatal demonstra compromisso em definir e fazer cumprir padrões de segurança da informação e de privacidade no que diz respeito à gestão de *backups*, tendo como referência, especialmente, o Acórdão 1.109/2021 – Plenário Tribunal de Contas da União (TCU) e Guia do *Framework* de Segurança - CIS *Controls* v8 - Controle 11: Recuperação de Dados. Destaca-se, ainda, que cabem melhorias a exemplo da busca pela certificação dos *datacenters* da estatal. Além disso, o Serpro também definiu padrões e estabeleceu controles e ferramentas para o processo de gestão de vulnerabilidades e para o processo de gestão de controles de acesso.

Por outro lado, ao se examinar a aplicação da temática no âmbito de três contratos do Serpro com os seus principais clientes, verificou-se a oportunidade de realizar estudos para identificar melhorias, bem como propor atualização e uniformização dos contratos da estatal com seus clientes no tocante aos temas segurança da informação e LGPD, para que se aumente a segurança jurídica no tratamento e finalidade do uso de dados, bem como se mitigue o risco de ineficiência no tratamento de eventuais incidentes de segurança.

Ademais, no âmbito do Acordo de Cooperação Serpro – Drumwave, restou claro o intuito do projeto de *data wallet* como ferramenta empoderamento do cidadão e alinhamento com o projeto de Governo como Plataforma, assim como ficou clara a sensibilidade do tema por se tratar de dados pessoais.

Destaca-se ainda a necessidade de cumprimento das determinações emitidas pela ANPD, para que o SERPRO alcance maior nível de conformidade com a LGPD e evite consequências adversas no seu plano de negócios.

Conclui-se então que, de forma geral, a estatal adota boas práticas de mercado e cumpre normas pertinentes à segurança da informação. De todo modo, foi emitida recomendação na situação em que se vislumbrou oportunidade de melhorias a serem realizadas pela estatal nos contratos junto a seus clientes.

ANEXOS

I – MANIFESTAÇÃO DA UNIDADE AUDITADA E ANÁLISE DA EQUIPE DE AUDITORIA

Achado nº 7 - Ausência de cláusulas relativas à Segurança da Informação e LGPD nos contratos com maiores clientes do Serpro

Manifestação da unidade auditada

Por meio de Manifestação no e-Aud nº 1470519, de 23/06/2023, o Serpro apresentou a seguinte manifestação:

"[...]

Achado nº 7 - Página 15 do Relatório de Auditoria n° 1360586

Ausência de cláusulas relativas à Segurança da Informação e LGPD nos contratos com maiores clientes do Serpro.

Recomendação nº 1 – Realizar estudo com o objetivo de identificar melhorias no âmbito dos contratos com clientes do Serpro em relação aos temas segurança da informação e LGPD, avaliando a possibilidade de atualizar e uniformizar entendimentos, bem como prever requisitos mínimos nos acordos, aderentes às melhores práticas do assunto".

Manifestação Serpro:

Em relação ao achado nº 7 - Ausência de cláusulas relativas à Segurança da Informação e LGPD nos contratos com maiores clientes do Serpro, encaminhamos em anexo (apontamentos_itensSIeLGPD_contratos) documento com apontamentos de cláusulas e/ou itens que abordam os temas Segurança da Informação e LGPD nos contratos auditados.

Cabe destacar ainda que todo o processo de contratação possui documentação vinculante, desde o início das tratativas que ensejam na assinatura de termo contratual. Neste sentido, as propostas comerciais encaminhadas pelo Serpro são compostas por itens específicos que tratam de Segurança da Informação e LGPD. Especificamente quanto aos contratos auditados, incluímos, em anexo, a documentação contratual completa, inclusive com as propostas comerciais vinculadas, nas páginas abaixo identificadas:

• STN - página 209

• Ministério da Economia - página 383

• RFB – arquivo separado

Cabe ressaltar no contrato da RFB não há anexo específico de LGPD. Entretanto, está em negociação com o órgão novo termo contratual, que vigerá a partir de outubro de 2023. As negociações partem da minuta de corpo de contrato da AGU, com seção específica de LGPD e cláusula de propriedade intelectual.

Adicionalmente, menciona-se que os contratos padronizados, que, quantitativamente, representam cerca de 95% dos contratos do Serpro, possuem cláusulas específicas dos temas Segurança da Informação e LGPD.

Quanto à cláusula específica de Segurança da Informação, as minutas atuais dos contratos padronizados trazem o seguinte trecho:

> 8 DO SIGILO E DA SEGURANÇA DAS INFORMAÇÕES
>
> 8.1 As PARTES se comprometem a manter sob estrita confidencialidade toda e qualquer informação trocada entre si em relação à presente prestação de serviços, bem como toda e qualquer informação ou documento dela derivado, sem prejuízo de qualquer outra proteção assegurada às PARTES pelo ordenamento jurídico.
>
> 8.2 Sobre a confidencialidade e a não divulgação de informações, fica estabelecido que:
>
> 8.2.1 Todas as informações e os conhecimentos aportados pelas PARTES para a execução do objeto deste contrato são tratadas como confidenciais, assim como todos os seus resultados.
>
> 8.2.2 A confidencialidade implica a obrigação de não divulgar ou repassar informações e conhecimentos a terceiros não envolvidos nesta relação contratual, sem autorização expressa, por escrito, dos seus detentores.
>
> 8.2.3 Não são tratadas como conhecimentos e informações confidenciais as informações que forem comprovadamente conhecidas por outra fonte, de forma legal e legítima, independentemente da iniciativa das PARTES no contexto deste contrato.
>
> 8.2.4 Qualquer exceção à confidencialidade só será possível caso prevista neste contrato ou com a anuência prévia e por escrito das PARTES em disponibilizar a terceiros determinada informação. As PARTES concordam com a disponibilização de informações confidenciais a terceiros nos casos em que tal disponibilização se mostre necessária para o cumprimento de exigências legais.
>
> 8.2.5 Para os fins do presente contrato, a expressão 'Informação Confidencial' significa toda e qualquer informação revelada, fornecida ou comunicada (seja por escrito, de forma eletrônica ou por qualquer outra forma) pelas PARTES entre si, seus representantes legais, administradores, diretores, sócios, empregados,
>
> consultores ou contratados (em conjunto, doravante designados 'REPRESENTANTES') no âmbito deste contrato.

8.2.6 Todas as anotações, análises, compilações, estudos e quaisquer outros documentos elaborados pelas PARTES ou por seus REPRESENTANTES com base nas informações descritas no item anterior serão também considerados 'Informação Confidencial' para os fins do presente contrato.

8.3 A informação que vier a ser revelada, fornecida ou comunicada verbalmente entre as PARTES deverá integrar ata lavrada por qualquer dos seus representantes para que possa constituir objeto mensurável e dotado de rastreabilidade para efeito da confidencialidade ora pactuada.

8.4 O descumprimento desta cláusula por qualquer das PARTES poderá ensejar a responsabilização de quem lhe der causa, nos termos da lei, inclusive em relação aos eventuais danos causados à parte contrária ou a terceiros.

8.4.1 Sem prejuízo de eventuais sanções aplicáveis nas esferas cível e administrativa, a conduta que represente violação a essa cláusula pode vir a ser enquadrada no crime de concorrência desleal previsto no art. 195, inc. XI, da Lei nº 9.279/1996.

8.4.2 O dever de confidencialidade estabelecido nesse contrato inclui a necessidade de observância da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD).

8.5 A responsabilidade por danos causados às PARTES ou a terceiros por eventual vazamento de dados ou outro tratamento de dados inadequado ou ilícito, será direcionada a quem comprovadamente tenha dado causa, por sua ação, omissão, ou sob sua responsabilidade.

8.6 O SERPRO não será responsabilizado por quaisquer prejuízos causados por eventuais erros, fraudes ou má qualidade dos dados compartilhados, bem como pelo uso indevido por terceiros das ferramentas que compõem a solução.

Além disso, também nas minutas atuais, há cláusula específica relativa à LGPD, conforme abaixo:

21 DA ADERÊNCIA À LEI Nº 13.709/2018

21.1 As condições relativas à aderência das PARTES à Lei Geral de Proteção de Dados – LGPD estão discriminadas no anexo "Tratamento e Proteção de Dados Pessoais" deste contrato.

21.2 O CLIENTE deve garantir os princípios da LGPD no seu relacionamento com o Titular do Dado, inclusive destacando ao Titular a FINALIDADE do uso da informação para evitar suspensão contratual junto ao SERPRO.

O anexo 'Tratamento e Proteção de Dados Pessoais' varia de acordo com os serviços contratados.

Vale ressaltar que trabalhamos com rigoroso processo de *compliance* interno para mantermos a conformidade nas tratativas de contratos de receita. Eventuais negociações são registradas dentro de instrumento e processo próprios que subsidiam a assinatura dos nossos representantes legais em nossos instrumentos contratuais.

1.1. Providências a serem Implementadas:

Embora a proposta comercial já seja instrumento vinculado a contrato, o SERPRO envidará esforços para que os textos de privacidade e segurança que nela estão transcritos possam ser levados aos termos contratuais.

Assim, em tempo de contrato, atua-se com a solicitação e negociação de cláusulas que constam em nossas propostas comerciais. Para tanto, e considerando que contratos são instrumentos bilaterais, sempre é aberto processo de discussão e alinhamento junto ao que o cliente nos demanda e o que ele espera que conste nos contratos a serem firmados, uma vez que os clientes possuem padrões de termos contratuais de aquisição que, muitas vezes, não condizem com os direcionamentos do SERPRO.

Fica mantida a atuação com rigoroso processo de *compliance* interno para manutenção da conformidade nas tratativas de contratos de receita da empresa.

1.2. Prazo de Atendimento:

Imediato, aplicável às futuras negociações."

Análise da equipe de auditoria

A manifestação do Serpro sobre os contratos analisados pela equipe de auditoria corrobora o achado de auditoria, não trazendo dados novos sobre esse ponto.

Ademais, o Serpro ainda informa que os "contratos padronizados", que respondem por cerca de 95% dos acordos da empresa, possuem cláusulas específicas dos temas Segurança da Informação e LGPD.

As cláusulas exemplificadas de Segurança da Informação têm como foco apenas a confidencialidade das informações, restando ausentes outros temas específicos já discutidos no achado de auditoria (gestão de backups, de logs, de vulnerabilidades etc).

As cláusulas sobre LGPD trazem a necessidade de o Cliente garantir os princípios da LGPD no seu relacionamento com o Titular do Dado, inclusive destacando ao Titular a finalidade do uso da informação para evitar suspensão contratual junto ao Serpro, denotando a necessidade de garantir ao titular dos dados o exercício de seus direitos elencados na Lei e a necessidade de informar a finalidade do tratamento de dados ao titular dos dados.

Diante do exposto, o achado mantém-se como consta do Relatório Preliminar enviado ao Serpro.

Achado nº 9 - Acordo de Cooperação Drumwave

Manifestação da unidade auditada

Por meio de Manifestação no e-Aud nº 1470519, de 23/06/2023, o Serpro apresentou a seguinte manifestação:

"[...]

Ausência de relatório final no tocante ao Acordo de Cooperação Drumwave.

2 – Elaborar relatório final do Acordo de Cooperação SERPRO – Drumwave, conforme disposto letra ‘c’, item 2, da cláusula segunda do Acordo e compartilhar com a SGD, unidade gestora da política pública ‘Governo como Plataforma’ e controladora dos metadados utilizados no projeto.

Manifestação Serpro: Relatório final elaborado, conforme anexo. Assim, entendemos que o achado se encontra sanado, e, portanto, a recomendação perde seu objeto.

2.1. Providências a serem Implementadas: Não se aplica

2.2. Prazo de Atendimento: Não se aplica”

Análise da equipe de auditoria

Em manifestação ao Relatório Preliminar de Auditoria o Serpro encaminhou o Relatório Final do Acordo de Cooperação Técnica do Serpro com a Drumwave o qual ainda não havia sido elaborado a época da emissão do Relatório Preliminar. Com isso, a recomendação do respectivo achado de auditoria perdeu o objeto e foi retirada para versão final deste Relatório de Auditoria. Sobre o conteúdo do Relatório Final do Acordo de Cooperação Técnica, destaque-se que o documento descreve o histórico do acordo e aponta riscos e oportunidades de um projeto *data wallet*, e, embora não tenha sido objeto da auditoria se debruçar sobre seu teor, entende-se que poderia ter havido maior aprofundamento da estatal acerca da viabilidade técnica do projeto.