INFRA S.A.

RELATÓRIO DE AVALIAÇÃO Nº 1566881
AUDITORIA INTERNA

Tema: Lei Geral de Proteção de Dados Pessoais - LGPD

Unidade examinada: PRESI e DIRAF - Estrutura de Governança do PPSI

Exercício: 2024

Missão da INFRA S.A

Planejar, projetar e executar de forma eficiente, sustentável e inovadora a infraestrutura de transporte e logística do Brasil buscando a melhoria de vida das pessoas.

Visão da INFRA S.A

Ser referência no Brasil em planejamento e projetos de infraestrutura e logística.

Valores da INFRA S.A

Excelência; Respeito à Vida; Eficiência Logística; Sustentabilidade; Integridade; Inovação; e Valorização das pessoas.

Auditoria Interna Governamental

Atividade independente e objetiva de avaliação e de consultoria, desenhada para adicionar valor e melhorar as operações de uma organização; deve buscar auxiliar a Infra S.A a realizar seus objetivos, a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de governança, de gerenciamento de riscos e de controles internos.

QUAL FOI O TRABALHO REALIZADO PELA INFRA S.A?

Em cumprimento ao Plano Anual de Auditoria Interna – PAINT/2024 e com base nas Normas Internacionais de Auditoria Interna emitidas pelo *The Institute of Internal Auditors (The IIA)* e normas internas de auditoria, avaliou-se a conformidade da adequação da empresa à LGPD.

POR QUE A INFRA S.A REALIZOU ESSE TRABALHO?

Os aspectos de conformidade com a Lei nº 13.709/2018 (LGPD) estão contemplados no PAINT 2024, considerando que a adequação à referida lei é um tema estratégico e multidisciplinar para a Infra S.A., dada a crescente importância da privacidade e proteção de dados pessoais no cenário nacional e internacional.

O objeto da presente auditoria abrange as ações e controles implementados para adequar a empresa à LGPD e às regulamentações correlatas.

A avaliação da conformidade com a LGPD é essencial para assegurar um ambiente seguro e reduzir os riscos associados à privacidade de dados pessoais.

QUAIS AS CONCLUSÕES ALCANÇADAS PELA INFRA S.A? QUAIS AS RECOMENDAÇÕES QUE DEVERÃO SER ADOTADAS?

As análises realizadas evidenciaram que a Infra S.A. demonstrou um bom nível de conformidade com a LGPD. Entretanto, identificou-se alguns pontos parcialmente adequados que demandam ajustes para garantir plena conformidade.

No que diz respeito ao compartilhamento de dados pessoais com operadores internacionais, foi recomendado que tenha um levantamento de contratos vigentes com parceiros que envolvam o armazenamento, o processamento ou a transferência de dados pessoais, identificando as empresas que os façam fora do território nacional. Também foi recomendado incorporação das cláusulas-padrão contratuais aprovadas pela ANPD dentro do período máximo tratado na Resolução nº 19 de 23 de agosto de 2024-ANPD.

Foi recomendada capacitação técnica específica para a equipe de segurança cibernética.

E por fim, uma recomendação para capacitação dos membros de todas as áreas pertencentes à estrutura do PPSI, alinhadas às suas respectivas responsabilidades.

LISTA DE QUADROS E FIGURAS

LISTA DE QUADROS

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

1.1. Apresentação

Trata-se de auditoria de conformidade, em cumprimento do Plano Anual de Auditoria Interna (PAINT/2024), assim como ao atendimento de obrigações legais previstas na Lei nº 13.709/2018 (LGPD) e regulamentações pertinentes.

A implementação da LGPD é transversal e requer uma abordagem multidisciplinar. Na Infra S.A., a adequação à LGPD está em andamento e envolve várias áreas com atribuições, papéis e responsabilidades a serem desempenhados por essas áreas.

Para o presente trabalho foram selecionadas as unidades que pertencem à estrutura de governança do Programa de Privacidade e Segurança da Informação (PPSI) da empresa, atualmente, os integrantes do PPSI no âmbito da Infra S.A. encontram-se lotados nas seguintes áreas, conforme quadro abaixo:

Quadro 1 - Unidades Auditadas

UNIDADES	ATRIBUIÇÕES E RESPONSABILIDADES
SUPTI/DIRAF	I- Gestor de Tecnologia da Informação e Comunicação, dentre outras atribuições, nos termos da Portaria nº 778, de 4 de abril de 2019 (alterada pela Portaria nº 18.152, de 4 de agosto de 2020), responsável por planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, considerando a cadeia de suprimentos relacionada à solução; II- Gestor de Segurança da Informação, dentre outras atribuições, nos termos da Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional, da Presidência da República - GSI/PR, responsável por planejar, implementar e melhorar continuamente os controles de segurança da informação em ativos de informação;
SUGEP/DIRAF	III- Encarregado pelo Tratamento de Dados Pessoais, dentre outras atribuições, nos termos do art. 41, §2º, da Lei nº 13.709, de 14 de agosto de 2018 (LGPD), também é responsável por conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis; e
SUINT/PRESI	IV- Responsável pela Unidade Controle Interno, que atua na segunda linha de defesa, representado na Infra S.A. pelo Superintendente de Integridade e Riscos, atuará no apoio, supervisão e monitoramento das atividades desenvolvidas pela primeira linha de defesa prevista pela Instrução Normativa CGU nº 3, de 9 de junho de 2017.

Fonte: elaborado pela equipe de auditoria.

Nesta auditoria, o foco será avaliar se as ações e controles implementados para adequar a empresa à Lei nº 13.709/2018 (LGPD) estão

devidamente instaurados e em conformidade com os requisitos legais.

É importante destacar que, neste momento, a auditoria concentrou-se na verificação da implementação das medidas, sem aprofundar-se na análise de sua eficácia ou eficiência. O objetivo foi confirmar se a empresa está buscando a conformidade com os princípios e diretrizes estabelecidos pela LGPD.

1.2. Objeto

A presente auditoria tem por objeto as ações e os controles implementados para adequar a empresa à Lei nº 13.709/2018 (LGPD) e aos regulamentos pertinentes.

1.3. Objetivos

1.3.1. Objetivo Geral

O objetivo desta auditoria consiste na avaliação da conformidade das práticas de tratamento de dados pessoais da Infra S.A. em relação aos requisitos estabelecidos pela LGPD e seus regulamentos.

1.3.2. Objetivos Específicos

A partir do objetivo geral deste trabalho de auditoria e considerando os critérios estabelecidos, as questões de auditoria foram formuladas considerando os elementos centrais:

- **Conformidade dos Artefatos com os princípios gerais da LGPD**: Avaliar se as políticas, normas internas, programas e a estrutura de governança criados para adequar a empresa à LGPD estão em conformidade com os princípios gerais da lei;
- **Tratamento de dados pessoais**: Verificar se as bases legais aplicadas nas operações de tratamento de dados pessoais e dados sensíveis realizadas pela empresa estão conformidade com a LGPD;
- **Direito dos Titulares**: Verificar os mecanismos adotados pela empresa para assegurar o exercício dos direitos dos titulares de dados pessoais.
- **Transferência de Dados Pessoais**: Avaliar a conformidade das transferências internacionais e o compartilhamento de dados pessoais com terceiros.
- **Agentes de Tratamento**: Verificar as atribuições e responsabilidades dos agentes de tratamento de dados pessoais, conforme estabelecido pela LGPD.
- **Segurança e Boas Práticas**: Examinar as ações e medidas de segurança, tanto técnicas quanto administrativas, implementadas para garantir a proteção dos dados pessoais.
- **Programa de Privacidade e Segurança da Informação**: Avaliar o atendimento dos requisitos de privacidade e segurança da informação, incluindo aqueles estabelecidos pela LGPD.

1.4. Escopo

Neste trabalho de avaliação foram analisados um conjunto de atividades e processos, relacionados aos elementos centrais dos objetivos específicos, buscando assegurar que todos os aspectos relevantes da implementação da LGPD sejam devidamente examinados.

Cabe ressaltar que a empresa já contratou uma consultoria especializada em LGPD (projeto de cooperação técnica internacional nº 13/013 entre a Infra S.A. e o Programa das Nações Unidas para o Desenvolvimento - PNUD) para realizar a adequação da Infra S.A. à Lei nº 13.709/2018. Em razão dessa consultoria, foram acompanhadas as seguintes atividades do contrato.

Quadro 2 – Produtos da Consultoria LGPD

NOME	PRODUTO
Produto nº 01	Relatório Técnico contendo o Inventário de dados pessoais que consiste no registro das operações de tratamento dos dados pessoais realizados pela empresa, utilizando o framework disponibilizado pela Secretaria de Governo Digital.
Produto nº 02	Relatório técnico contendo resultado do inventário, incluindo diagnóstico, lacunas e proposições para assegurar a conformidade da Infra S.A.
Produto nº 03	Relatório técnico contendo Políticas/Declarações de Privacidade e Termos de Uso para os portais, sistemas e aplicativos da Infra S.A.
Produto nº 04	Relatório de Impacto de Proteção de Dados Pessoais (RIPD) da Infra S.A., em conformidade com as diretrizes e frameworks da Autoridade Nacional de Proteção de Dados Pessoais e da Secretaria de Governo Digital e documento adicional contendo a documentação detalhada contendo os processos de tratamento de dados pessoais, medidas, salvaguardas e mecanismos de mitigação de riscos, descrição dos tipos de dados pessoais coletados ou tratados de qualquer forma, metodologia utilizada para o tratamento e para a garantia da segurança das informações e análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados.
Produto nº 05	Relatório técnico contendo as medidas de proteção de dados pessoais adotadas para mitigação do impacto à proteção de dados pessoais.
Produto nº 06	Relatório técnico contendo as diretrizes evolutivas para assegurar a cultura de privacidade na Infra S.A.
Produto nº 07	Relatório técnico com os mapeamentos de processos, documentos detalhados dos processos, lições aprendidas, manuais de utilização e sustentação, transferência de conhecimento, resultados de transferência de conhecimento sobre o Sistema de Proteção e Privacidade de Dados e a cultura da privacidade na Infra S.A. e workshop.

Fonte: elaborado pela equipe de auditoria.

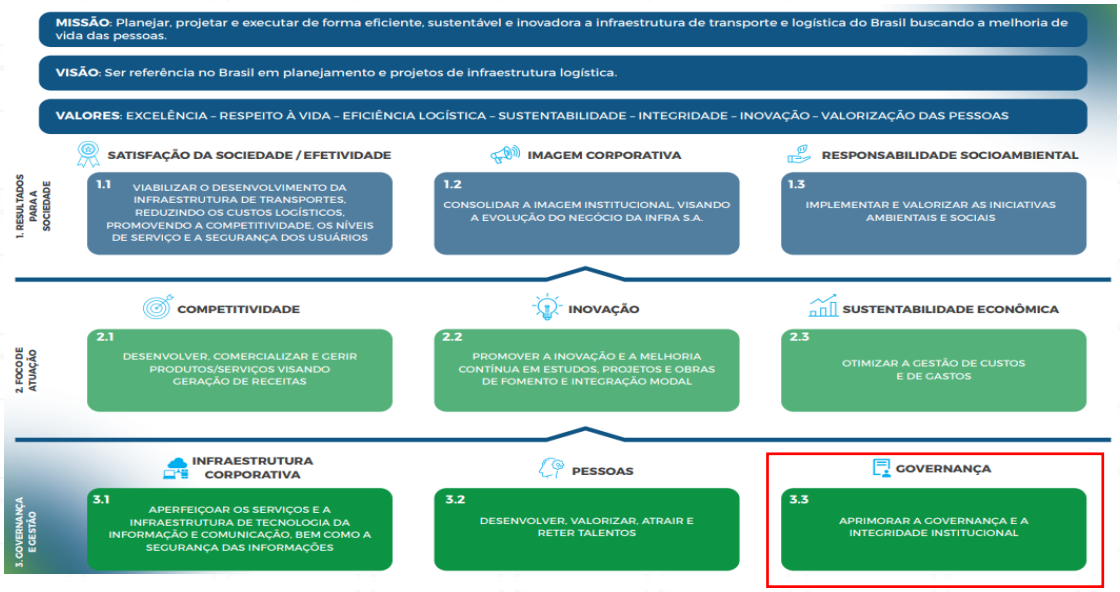
1.5. Montante Fiscalizado

A avaliação da conformidade da Infra S.A, no que tange à adequação da

Lei 13.709/2018, não se mostrou aplicável à definição de valores sob fiscalização nesta auditoria, a qual se refere ao aspecto da materialidade quantitativa.

No entanto, obtém-se a materialidade qualitativa em decorrência da importância estratégica do assunto para a organização, pois está dentro do foco Governança e Gestão do Mapa Estratégico 2023-2027, da empresa, conforme figura a seguir:

Figura 1 – Mapa Estratégico 2023-2027



Fonte: Site oficial da Infra S.A.(*link*: mapa-estrategico-2023-2027-INFRASA-20092023 (valec.gov.br)).

1.6. Metodologia

Os procedimentos e técnicas usados na execução do presente trabalho de avaliação estão registrados na Matriz de Planejamento, considerando as Normas Internacionais de Auditoria Interna emitidas pelo *The IIA* e normativos internos. As principais técnicas utilizadas nos testes foram a realização de reuniões com redução a termo e a análise documental.

1.7. Critérios de Auditoria

Os principais normativos aplicáveis ao objeto da auditoria são:

a) Lei nº 13.303/2016 e Decreto nº 8.945/2016;
b) Lei 13.709/2018 de 14 de agosto de 2018;
c) Portaria SGD/MGI nº852 de 05 de maio de 2023;
d) ABNT NBR ISO 27.701:2019 – Gestão da privacidade da informação.

1.8. Avaliação de Riscos e Controles

Com o objetivo de orientar a extensão dos testes realizados durante a execução da auditoria, a equipe de auditoria realizou a avalição dos riscos e a estrutura básica dos controles internos por meio da metodologia disponibilizada pela CGU, a qual foi estabelecida para dar suporte as Unidades de Auditorias Internas

Governamentais em seus processos de auditorias, conforme dispõe o papel de trabalho da Matriz de Riscos e Controles (MRC).

1.9. Contextualização

A implementação da Lei Geral de Proteção de Dados (LGPD) na Administração Pública Federal direta e indireta representa um avanço significativo na proteção da privacidade e dos dados pessoais dos cidadãos. Desde a sua sanção em 2018, as instituições públicas têm se mobilizado para adequar seus processos e práticas ao novo marco legal.

A Secretaria de Governo Digital (SGD/MGI) do Ministério da Economia, por meio do Programa de Privacidade e Segurança da Informação- PPSI (disposto na Portaria SGD/ nº 852 de 28 de março de 2023), empreendeu uma série de iniciativas em matéria de gestão, governança, maturidade, metodologia, pessoas e tecnologia.

A Infra S.A., como ente público integrante do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), aderiu ao Plano de Trabalho da SGD e adotou a estruturação de governança de privacidade e proteção de dados pessoais do governo federal.

No contexto da Portaria SGD nº 842/2023, O Plano de Trabalho é representado pela Ferramenta de *Framework* do PPSI, a qual contém, entre outras informações, o diagnóstico, o Plano de Ação e as informações de contatos da Estrutura de Governança do PPSI. Informações, essas, fundamentais para o acompanhamento e a evolução da privacidade e segurança da informação de cada instituição.

Vale lembrar que a adequação à LGPD não é um processo pontual, mas contínuo, exigindo atualizações constantes de acordo com novas diretrizes e a evolução das práticas de tratamento de dados.

2. RESULTADOS DOS EXAMES

2.1. Um panorama geral da LGPD na Infra S.A.

O presente trabalho de avaliação de conformidade dos processos de adequação da Infra S.A à LGPD foi conduzido com uma análise abrangente, contemplando os principais capítulos da legislação aplicável à empresa. Constatou-se que a Empresa apresenta um nível satisfatório de conformidade com a LGPD, identificando-se apenas pequenos pontos de adequação parcial.

Esse resultado positivo reflete, em grande parte, os avanços obtidos pela consultoria contratada, bem como o comprometimento e a dedicação dos membros do Programa de Privacidade e Segurança da Informação (PPSI), que desempenharam papel fundamental no progresso alcançado. A seguir, são apresentados os resultados detalhados da presente auditoria.

Quadro 3 – Avaliação de adequação da LGPD na Infra S.A.

ITEM AVALIADO DA LGPD	AÇÕES E MEDIDAS TOMADAS PARA ATENDER AOS REQUISITOS DA LGPD	SITUAÇÃO
Conformidade dos artefatos com os princípios gerais da LGPD	Política da Segurança da Informação (POSIN).	Adequado
	Política de Proteção e Privacidade de Dados Pessoais (PPPDP) e Comitê de Privacidade e Segurança da Informação.	Adequado
	Programa de Privacidade e Segurança da Informação (PPSI).	Adequado
Conformidade do Tratamento de Dados Pessoais	Inventário de Dados Pessoais contém as bases legais relacionada a cada atividade de tratamento.	Adequado
	Políticas/Declarações de Privacidade e Termos de Uso para os portais, sistemas e aplicativos.	Adequado
	Em caso de alteração de informação referente à finalidade específica do tratamento, forma e duração do tratamento, identificação do controlador ou informações acerca do uso compartilhado de dados pelo controlador e a finalidade.	Adequado
	A base legal de legítimo interesse aplicada de acordo com o §2º, art. 10, da LGPD.	Adequado
	Os bancos de dados de armazenamento de dados pessoais estão identificados e catalogados.	Adequado
	O tratamento de dados pessoais sensíveis está com as diretrizes da LGPD.	Adequado
	Existência de instrumento de consentimento para a coleta de dados sensíveis, bem como a coleta de dados sensíveis sem consentimento conforme previsão legal.	Adequado
	Os dados pessoais de crianças e adolescentes são tratados de acordo com as diretrizes da LGPD.	Adequado
	O ciclo de vida dos dados pessoais definido.	Adequado
	O término das atividade de tratamento de dados pessoais estabelecida.	Adequado

Conformidade para atender aos Direito dos Titulares	Existência de canal de comunicação direto para que os direitos dos titulares sejam exercidos de forma adequada.	Adequado
Conformidade na Transferência de Dados Pessoais	Os compartilhamentos de dados pessoais com terceiros estão adequados com as diretrizes da LGPD.	Adequado
	Os compartilhamentos de dados pessoais com operadores estão adequados com as diretrizes da LGPD.	Adequado
	Os compartilhamentos de dados pessoais com operadores internacionais estão adequados com as diretrizes da LGPD.	Adequado parcialmente
Conformidade do Agentes de Tratamento	Os registros das atividades de tratamento de dados pessoais são demonstrados por meio do inventário de dados pessoais, bem como a identificação dos respectivos controladores, co-controladores e operadores.	Adequado
	Existência de Encarregado com as atribuições e divulgação de sua identidade de contato no site oficial da empresa.	Adequado
Conformidade da Segurança e Boas Práticas	As medidas administrativas implementadas estão adequadas com as diretrizes da LGPD.	Adequado
	As medidas de segurança implementadas estão adequadas com as diretrizes da LGPD.	Adequado parcialmente
	As medidas técnicas implementadas estão adequadas com as diretrizes da LGPD.	Adequado parcialmente
Conformidade do Programa de Privacidade e Segurança da Informação	O Programa de Privacidade e Segurança da Informação (PPSI) implementado pela Infra S.A está aderente com a Portaria SGD/MGI nº 842/2023 e com outros normativos pertinentes.	Adequado
	A nomeação dos membros da estrutura de governança do PPSI está de acordo com os requisitos normativos.	Adequado
	Os membros da estrutura de governança do PPSI possuem capacidade técnica adequada.	Adequado parcialmente
	As informações das autoavaliações e do planejamento fornecidos pelo PPSI para subsidiar o acompanhamento da Secretaria de Governo Digital (SGD).	Adequado

Fonte: elaborada pela equipe de auditoria.

Antes de avançar para a análise dos resultados apresentados, é importante ressaltar que este trabalho de auditoria se concentrará no detalhamento das situações classificadas como "parcialmente adequadas", por serem consideradas achados de auditoria, em que pesem terem sido aplicados testes, devidamente documentados em papéis de trabalho, para todas as situações também indicadas como “adequadas” no Quadro 3.

2.2. Medidas Técnicas e de Segurança implementadas

Na análise dos resultados, constatou-se que as medidas de segurança e técnicas adotadas, embora parcialmente adequadas, apresentam limitações que não garantem um nível pleno de segurança, oferecendo apenas proteção parcial. Contudo, essas características são inerentes ao contexto da segurança cibernética. Por esse motivo, a equipe de auditoria não classificou essa questão como um achado de auditoria.

2.3. Achados de Auditoria

Os achados de auditoria identificados referem-se aos seguintes pontos: (a) compartilhamento de dados pessoais com operadores internacionais; e (b) capacitação técnica dos membros dessa estrutura de governança. Esses aspectos serão detalhados nos itens subsequentes.

2.3.1. Risco de compartilhamento de dados pessoais com operadores internacionais

Foi identificado risco de compartilhamento de dados pessoais com operadores internacionais, em caso em que dados sejam enviados, armazenados ou acessados de um país estrangeiro

Critério

O compartilhamento de dados pessoais com operadores internacionais é tratado na Lei nº 13.709/18 - LGPD, art. 33; e na Resolução ANPD Nº 19, de 23 de agosto de 2024

Análise e Evidências

A resolução Nº 19, de 23 de agosto de 2024/ANPD aprova o Regulamento de Transferência Internacional de Dados e define o conteúdo das cláusulas-padrão contratuais que devem ser adotadas por empresas ao realizar transferências internacionais. Essas cláusulas-padrão servem como mecanismo para garantir que os dados pessoais sejam tratados de acordo com os princípios e direitos previstos na LGPD, mesmo quando transferidos para países ou organismos internacionais.

Ocorre que, atualmente, os contratos da Infra S.A. ainda não estão adequados com a Resolução Nº 19, de 23 de agosto de 2024/ANPD.

Cabe ainda destacar que o Relatório Técnico do Produto 2 da consultoria em LGPD (Projeto PNUD BRA 13/13 – Proteção e Privacidade de Dados Pessoais), informa que foi realizada a análise em relação à possíveis transferências de dados pessoais para destinatários localizados fora do território nacional, em estrita conformidade com as disposições estabelecidas no Capítulo V da LGPD e que não foram identificadas transferências internacionais de dados.

Por outro lado, esta equipe de auditoria entende que a transferência internacional de dados pessoais também ocorre sempre que algum dado pessoal é enviado, armazenado ou acessado de um país estrangeiro. Assim, o simples armazenamento fora do país também caracteriza a transferência internacional.

Nesse sentido, é necessário o levantamento de todos os contratos vigentes com fornecedores e parceiros que envolvam o armazenamento, processamento ou transferência de dados pessoais, identificando especificamente as empresas que armazenam ou processam dados fora do território nacional.

Causa

Uma das possíveis causas para o achado é a utilização de contratos desatualizados: continuar utilizando contratos sem cláusulas específicas para atendimento da Resolução ANPD nº19/2024.

Efeitos

O descumprimento da Resolução nº19/2024/ANPD pode resultar em sanções administrativas: A ANPD pode aplicar multas e suspensões pelo descumprimento da Resolução, além de interrupção de negócios: rescisão de contratos com parceiros globais por descumprimento da LGPD e regulamentos correlatos.

Manifestação dos Gestores

1. A Infra S.A. adota uma minuta de contrato com cláusulas específicas que atendem à LGPD, incluindo a cláusula de "Transferência Internacional" (1.2.13), que estabelece: "A CONTRATADA deverá solicitar prévia e expressa autorização da Infra S.A. caso seja necessária qualquer transferência internacional de dados pessoais, pontual ou recorrente, indicando os detalhes do tratamento a ser realizado no país estrangeiro."

2. Essa cláusula reflete boas práticas e está alinhada aos princípios da LGPD, embora haja oportunidades de aprimoramento para reforçar a conformidade e a clareza em relação às diretrizes estabelecidas pela Resolução CD/ANPD nº 19/2024.

3. Sobre o prazo legal para a implementação das Cláusulas Contratuais Padrão, a Resolução CD/ANPD nº 19/2024, publicada em 23 de agosto de 2024, concede até 12 (doze) meses para que os agentes de tratamento incorporem essas cláusulas aos seus instrumentos contratuais. Portanto, o prazo regulamentar para adequação encerra-se em 23 de agosto de 2025, estando, assim, dentro do período de transição previsto na norma.

4.Dessa forma, entendemos que a situação apresentada não caracteriza descumprimento, mas integra o processo de adequação em andamento, conforme o prazo estabelecido pela Resolução CD/ANPD nº 19/2024. Assim, sugere-se ajustar na descrição sumária e eventuais outras citações o termo "descumprimento" para "em processo de adequação.

Manifestação da Equipe de Auditoria

É fato que a cláusula "Transferência Internacional" já prevista na minuta de contrato apresentada reflete boas práticas e está alinhada com os princípios da LGPD. Contudo, é importante destacar que, conforme a Resolução CD/ANPD nº 19/2024, as cláusulas-padrão contratuais não se limitam ao consentimento, mas inclui elementos adicionais, como a obrigatoriedade de cláusulas específicas quanto ao compromisso de conformidade com os requisitos da Resolução.

Embora o prazo para a adequação se estenda até 23 de agosto de 2025, recomendamos que a empresa antecipe a incorporação das cláusulas-padrão da ANPD aos contratos vigentes. Isso garantirá que os contratos estejam totalmente alinhados com os novos requisitos legais, evitando possíveis riscos futuros.

É fundamental que a empresa realize os ajustes necessários dentro do período de transição para evitar que a implementação da Resolução seja interpretada de forma incompleta ou inadequada.

Reiteramos que a adequação dentro do prazo é essencial para garantir conformidade total com a legislação vigente.

Recomendações

Recomenda-se que seja realizado levantamento de todos os contratos vigentes com fornecedores e parceiros que envolvam o armazenamento, processamento ou transferência de dados pessoais, identificando especificamente as empresas que armazenam ou processam dados fora do território nacional, a fim de assegurar a conformidade com as exigências da Resolução Nº 19/2024 da ANPD e da LGPD.

Recomenda-se a incorporação das cláusulas-padrão aprovadas pela ANPD aos instrumentos contratuais, inclusive realização de aditivos para contratos vigentes, se for o caso, no prazo de até 23 de agosto de 2025.

Benefícios Esperados

Dentre os benefícios esperados, podemos destacar a conformidade regulatória e contratual e a segurança jurídica nas transferências de dados, garantindo conformidade com a LGPD.

2.3.2. Lacunas na capacitação técnica de membros da equipe

Foram contatadas lacunas na capacitação técnica dos membros da equipe de tratamento de incidentes de segurança em redes de computadores.

Critério

A importância da capacitação é mencionada na Portaria SGD/MGI Nº 852/23, Art. 15 e na Lei nº 13.709/18 - LGPD, Art. 6 VII e Art. 50, ao enfatizar que as organizações devem adotar medidas de segurança e boas práticas para proteger os

dados pessoais.

Análise e Evidências

A Portaria SGD/MGI Nº 852, DE 28 DE MARÇO DE 2023, prevê expressamente a necessidade de capacitação das equipes de prevenção, tratamento e resposta a incidentes cibernéticos dos órgãos e das entidades pertencentes ao SISP:

> *Art. 15. As equipes de prevenção, tratamento e resposta a incidentes cibernéticos dos órgãos e das entidades pertencentes ao SISP deverão se integrar às tecnologias, padrões, procedimentos e processos estabelecidos pelo CISC Gov.br, observando os normativos do Gabinete de Segurança Institucional da Presidência da República.*

Conforme pode ser observado, na tabela abaixo, ficou identificada uma lacuna de capacitação técnica na equipe de tratamento de incidentes de segurança em redes de computadores. Ressalta-se que a tabela foi elaborada a partir das informações fornecidas pelo setor e relacionadas com a Portaria nº 389/2024/INFRASA.

Quadro 4 – Capacitação equipe ETIR

MEMBRO - ETIR	CAPACITAÇÃO EM LGPD, SEGURANÇA DE TRATAMENTO DE INCIDENTES DE SEGURANÇA EM REDE DE COMPUTADORES E ASSUNTOS CORRELATOS	DATA DE CONCLUSÃO	HORAS	INSTITUIÇÃO
Membro titular A e Agente Responsável	LGPD nas Organizações	04/24	8h	*Data Shield e O&G Bras*
Membro titular B	-	-	0h	-
Membro titular C	Fundamentos na Lei Geral de Proteção de Dados	10/2021	Não informado	*CertiProf*
	Introdução à Lei Brasileira de Proteção de Dados Pessoais	09/2019	10h	ENAP
	Treinamento PDPP- *Privacy & Data Protection Practitioner*	05/2021	16h	Portal do Treinamento
	Formação DPO - *Data Protection Officer*	04/2021	10h	Portal do Treinamento
	Gestão Ágil de Projetos LGPD	04/2021	4h	Portal do Treinamento
	Implementação do Sistema de gestão de Proteção de Dados Pessoais – SGPD	06/2021	16h	Portal do Treinamento
	ISSO 27001 *Essentials* - Segurança da Informação	04/2021	10h	Portal do Treinamento

	PDPE - *Privacy & Data Protection Essentials* – LGPD	06/2021	7h	Portal do Treinamento
	Privacy & Data Protection Foundation - PDPF	04/2021	16h	Portal do Treinamento
	LGPD nas Organizações	04/24	8h	*Data Shield e O&G Bras*
	Especialização em Privacidade e Segurança da Informação	07/2024	375h	UNB
Membro suplente A	*Advanced Technical Security Products Training Course*	09/2008	Não informado	*Tipping Point*
Membro suplente B	-	-	0h	-
Membro suplente C	Fundamentos da Segurança Cibernética - Introdução ao CIS *Controls*	09/2024	25h	ENAP
	Introdução à Lei Brasileira de Proteção de Dados Pessoais	10/2022	10h	ENAP
Agente Responsável (Suplente)	-	-	0h	-

Fonte: elaborada pela equipe de auditoria.

Nota-se que a equipe conta com um(a) integrante que que demonstrou elevado nível de capacitação técnica e domínio das competências exigidas para as funções relacionadas à proteção de dados pessoais. No entanto, os demais membros apresentam lacunas significativas em sua formação e conhecimento técnico, o que pode comprometer a atuação uniforme e eficiente da equipe.

Visto isso, fica clara a necessidade de implementação de programas de capacitação e desenvolvimento técnico para os membros da equipe, especialmente para o agente responsável e seu respectivo suplente.

Causa

A ausência de capacitação contínua do setor ou a falta de interesse dos empregados para se capacitarem podem resultar em uma estagnação das habilidades necessárias, além da falta de consciência ou entendimento sobre a importância da capacitação.

Efeitos

Alguns dos efeitos desse entendimento é o aumento do risco de falhas nos controles internos e de comprometimento da imagem organizacional, os erros e retrabalhos, além da desmotivação tanto da equipe quanto dos líderes.

Manifestação dos Gestores

A área apresentou suas considerações a respeito do achado, a seguir:

O PPSI (Estratégico) e a ETIR (Operacional) possuem abrangências, escopos, papéis e fronteiras de atuação distintos:

- PPSI: Programa de Privacidade e Segurança da Informação (Portaria Infra S.A. nº 277/2024).

- ETIR: Equipe de Tratamento e Resposta a Incidentes Cibernéticos (Portaria Infra S.A. nº 389/2025)

Cumpre informar que a sustentação operacional da infraestrutura tecnológica, segurança das operações e segurança cibernética é realizada por empresa terceirizada, que conta com quadro certificado. A empresa atual é a Central IT e está aberto processo de nova licitação.

A SUPTI considera que a capacitação contínua é fundamental. Por isso, o Plano Diretor de Tecnologia da Informação – PDTIC (2023-2025) inclui um plano de capacitação que aborda temas críticos e relevantes, como privacidade e segurança da informação (https://www.infrasa.gov.br/governança/pdtic/).

Em 2023 e 2024, os times foram continuamente incentivados a participar de cursos gratuitos de excelente qualidade, eventos, palestras e debates técnicos, inclusive ofertado a todos a inscrição para a 1º e 2ª Turma de Pós-graduação Lato Sensu em Privacidade e Segurança da Informação, promovida pelo MGI em parceria com a UNB.

A participação e o nível de aplicação prática do conhecimento variam conforme o perfil e os interesses individuais. Membros do time tem se atualizado com as capacitações disponibilizadas pelo Governo Federal: Capacita Gov.br, Eventos e Premiações, Catálogo da EVG e Materiais sobre privacidade e segurança.
Adicionalmente informa-se que o Centro de Excelência em Privacidade e Segurança da Informação (CEPS GOV.BR) realiza diversas capacitações gratuitas e webinários para os órgãos do SISP e toda a sociedade, inclusive lançou o edital para a terceira turma do Curso de Pós-graduação Lato Sensu em Privacidade e Segurança da Informação, em parceria com a Universidade de Brasília (UnB). Voltado a servidores e gestores dos mais de 250 órgãos do SISP, o curso será gratuito para os selecionados, oferece capacitação avançada e prática. O público-alvo é: Gestores, Encarregados, Auditores, Profissionais de Tecnologia da Informação, Profissionais do Direito, Profissionais de Qualquer Formação que trabalham com Privacidade e Segurança da Informação e Profissionais em Geral que tenham interesse no tema.

Inscrições: de 13 de janeiro a 10 de fevereiro.
Edital: https://ppee.unb.br/?page_id=9044
Isso posto, sugerimos a divulgação ampla dessas oportunidades e incentivo

a participação do quadro da Infra S.A. A pós-graduação aceita todas as formações superiores, destacando que privacidade e segurança da informação são responsabilidades compartilhadas.

Reafirmamos nosso compromisso com a melhoria contínua, a segurança cibernética e o cumprimento das normas aplicáveis, fortalecendo a mitigação de riscos e a resposta a incidentes de forma consistente e eficiente.

Manifestação da Equipe de Auditoria

A resposta da equipe menciona a distinção entre os escopos dos programas e as equipes envolvidas: ETIR e PPSI. Esta equipe de auditoria esclarece que o presente achado é sobre a equipe de tratamento de incidentes de segurança em redes de computadores - ETIR, contudo, também há recomendação sobre capacitação para todos os membros da estrutura do PPSI.

A área também destaca a atuação de uma empresa terceirizada com pessoas certificadas para suporte operacional, o que representa uma vantagem, mas também gera preocupações quanto à dependência de serviços externos.

A análise positiva da área sobre a conscientização referente ao plano de capacitação contínua e às oportunidades de formação, como cursos e webinários, é um ponto favorável, mas a variação na participação e aplicação prática do conhecimento pode indicar a necessidade de estratégias adicionais para engajar todos os membros da equipe.

Recomendações

Recomenda-se a implementação de um programa de capacitação específico para integrantes da Equipe de Tratamento de Incidentes de Segurança em Redes de Computadores (ETIR) que apresentem lacunas em suas competências técnicas. Treinamento regulares em segurança da informação, proteção de dados pessoais e práticas de conformidade com a LGPD, com a finalidade de equiparar e/ou complementar o nível de conhecimento entre os membros da equipe.

Recomenda-se que todas as áreas pertencentes a estrutura de governança do PPSI da Infra S.A. tenham um plano de capacitação para seus membros, alinhados às suas respectivas responsabilidades, para assim assegurar a proteção adequada dos dados pessoais e garantir o cumprimento das normas legais.

Benefícios Esperados

Espera-se a melhoria da eficiência operacional, a conformidade legal e regulatória, a redução de riscos e proteção da reputação da empresa.

3. RECOMENDAÇÕES

Apresenta-se, em síntese as recomendações oferecidas ao longo deste Relatório, correlacionando-as com os respectivos achados:

Quadro 5 – Síntese das Recomendações

RECOMENDAÇÃO	ITEM DO ACHADO
Recomenda-se que seja realizado levantamento dos contratos vigentes com fornecedores e parceiros que envolvam o armazenamento, o processamento ou a transferência de dados pessoais, identificando especificamente as empresas que armazenam ou processam dados fora do território nacional, a fim de assegurar a conformidade com as exigências da Resolução Nº 19/2024 da ANPD e da LGPD.	**2.3.1**
Recomenda-se a incorporação das cláusulas-padrão aprovadas pela ANPD aos instrumentos contratuais, inclusive realização de aditivos para contratos vigentes, se for o caso, no prazo de até 23 de agosto de 2025.	**2.3.1**
Recomenda-se que a implementação de programa de capacitação específico para integrantes da Equipe de Tratamento de Incidentes de Segurança em Redes de Computadores (ETIR) que apresentem lacunas em suas competências técnicas, fornecendo treinamento regulares em segurança da informação, proteção de dados pessoais e práticas de conformidade com a LGPD, com a finalidade de equiparar e/ou complementar o nível de conhecimento entre os membros da equipe.	**2.3.2**
Recomenda-se que todas as áreas pertencentes a estrutura de governança do PPSI da Infra S.A. tenham plano de capacitação para seus membros, alinhados às suas respectivas responsabilidades, para assim assegurar a proteção adequada dos dados pessoais e garantir o cumprimento das normas legais.	**2.3.2**

4. CONCLUSÃO

A auditoria de conformidade realizada teve como objetivo geral avaliar as ações e controles implementados para adequar a Empresa à Lei nº 13.709/2018 (LGPD) e regulamentações pertinentes.

Os resultados da presente auditoria demonstram que a Infra S.A. apresentou um nível satisfatório de conformidade com a LGPD. Entretanto, identificou-se alguns pontos parcialmente adequados que demandam ajustes para garantir plena conformidade, especialmente no que diz respeito ao compartilhamento de dados pessoais com operadores internacionais e à capacitação técnica dos membros da equipe de segurança cibernética.

Além disso, também há recomendação para capacitação dos membros das áreas que compõem o PPSI. A alta capacidade técnica é crucial para qualquer programa de governança, em especial na área de segurança da informação.

A aplicação das recomendações apresentadas visa garantir a conformidade legal e regulatória e fomentar o aperfeiçoamento das medidas técnicas e organizacionais para proteger os dados pessoais contra acessos não autorizados, vazamento de informações e outras situações de risco.

Brasília, 10 de março de 2025.