GOVERNO DO DISTRITO FEDERAL

COMPANHIA IMOBILIÁRIA DE BRASÍLIA

Conselho de Administração

Auditoria Interna

Relatório de Auditoria n.º 8/2022 - TERRACAP/CONAD/AUDIT Brasília-DF, 15 de dezembro de 2022.

Relatório de Auditoria Operacional n° 08/2022 - AUDIT
PROCESSO: 00111-00002602/2022-11
INTERESSADO: AUDIT/CONAD/TERRACAP
ASSUNTO: Análise dos controles primários no que se refere ao Cumprimento da Lei LGPD - Lei Geral de Proteção de Dados, no âmbito da TERRACAP.

Apresentamos o relatório de auditoria operacional que trata da análise dos controles primários no que se refere ao Cumprimento da Lei LGPD - Lei Geral de Proteção de Dados, no âmbito da TERRACAP, instaurada pela Ordem de Serviço nº 001/2022– AUDIT, documento SEI (84830803), alterada pela Ordem de Serviço 006/2022 (100339711) para ajustes no cronograma, em cumprimento ao Plano Anual de Atividades de Auditoria Interna - PAINT/2022 (84161934), constante no processo (00111-00012799/2021-16).

Ressaltamos que o PAINT/2022 aborda as ações que a Auditoria Interna da Terracap considera relevantes para o fortalecimento e aprimoramento da gestão, assim como o adequado relacionamento com parceiros e instituições externas.

O presente relatório foi emitido após a edição do relatório preliminar nº 06/2022-AUDIT - 101110822, e enviado às áreas para conhecimento , ciência e manifestação em 5 dias corridos, após o envio.

I - ESCOPO DO TRABALHO

Trata-se da avaliação nos controles primários dos processos e procedimentos no que se refere Cumprimento da Lei LGPD - Lei Geral de Proteção de Dados, no âmbito da TERRACAP, instaurada pela Ordem de Serviço nº 001/2022– AUDIT, documento SEI (84830803), alterada pela Ordem de Serviço 006/2022 (100339711), em cumprimento ao Plano Anual de Atividades de Auditoria Interna aprovado pelo Conselho de Administração – CONAD (PAINT/2022), conforme documento SEI (84162518).

A questão abordada por ocasião deste trabalho é referente à necessidade de avaliação do cumprimento da LGPD, em especial ao fiel cumprimento da legislação de regência.

Em consulta *preliminar* ao site da TERRACAP, observou-se que os principais normativos afetos ao tema estão disponíveis, e em especial foram juntados ao presente processo a Lei nº 13.709/2018 (85928184) que dispõe sobre a Lei Geral de Proteção de Dados Pessoais - LGPD, bem como o Decreto nº 42.306/2021 (85928184), que versa sobre à aplicação da aludida Lei Federal de Proteção de Dados, no âmbito da Administração Pública Direta e Indireta do Distrito Federal e dá outras providências.

É importante ressaltar que o site oficial da empresa sofre atualizações constantes com relação ao tema em questão.

Além disso, a citada Lei é aplicável a todas as pessoas jurídicas de direito público e privado, quando ocorrer o tratamento de dados de pessoal natural, de pessoal natural com fins econômicos, pois os dados pertencem ao titular, e não às empresas, vedando assim o vazamento de dados. Portanto, busca-se promover uma cultura organizacional que estimule a conduta ética no tratamento de dados pessoais, que prime pela proteção dos direitos fundamentais da liberdade, da privacidade, do livre desenvolvimento da personalidade da pessoa natural, e, por fim, no estrito compromisso de cumprimento da lei. Assim, esta auditoria operacional visa avaliar a implementação das ferramentas para cumprimento da LGPD no tocante à TERRACAP, incluindo rotinas, mecanismos de checagem, processos e procedimentos implementados, e ampla divulgação para o corpo técnico, analisando, assim, os controles primários existentes.

Voltando especificamente para as ações promovidas no âmbito da TERRACAP, podemos verificar que a Companhia Imobiliária de Brasília possui uma Política de Segurança da Informação e Comunicações (POSIC), aprovada para atender ao que preconiza a LGPD - Lei Geral de Proteção de Dados Pessoais - Lei n° 13.709/2018, objetivando possibilitar o gerenciamento da segurança em uma organização, estabelecendo regras e padrões para proteção da informação. A política possibilita ainda manter a confidencialidade, assim como garantir que a informação não seja alterada ou perdida, e, por fim, permitir que a informação esteja disponível quando necessário.

A Companhia Imobiliária de Brasília realiza o tratamento de dados pessoais, avaliando a necessidade e proporcionalidade da coleta dos dados, ou seja, limitando o 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, conforme preconiza os princípios e bases legais da LGPD (para o Cumprimento de obrigação legal ou regulatória, nos termos do art. 7º, II, LGPD; Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular dos dados, conforme o art. 7º, V, da LGPD).

Por fim, a presente auditoria teve como ESCOPO a avaliação dos controles primários referentes ao cumprimento e implementação da Le Geral de Proteção de Dados - LGPD, no âmbito da TERRACAP.

II – CONTEXTUALIZAÇÃO

a Lei n° 13.709 (LGPD - Lei Geral de Proteção de Dados), criada em 14 de agosto de 2018, dispõe sobre o tratamento de dados pessoais, tanto em meios físicos quanto digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A Lei tem como propósito regulamentar todo o tratamento de dados pessoais dos cidadãos brasileiros e suas penalidades, caso haja descumprimento, são muito severas podendo chegar até 2% do faturamento da empresa limitado a 50 milhões de reais por infração. Além disso, a ANPD (Autoridade Nacional de Proteção de Dados), agência reguladora criada para fiscalizar a aplicação da lei, poderá determinar a suspensão temporária das atividades da empresa infratora.

A LGPD criou regras claras sobre os processos de coleta, armazenamento e compartilhamento das informações pessoais. Assim, Governo e empresas terão que garantir maior segurança a esses dados. Ainda, a nova lei assegura à pessoa natural a titularidade de seus dados pessoais, exigindo o consentimento prévio para o uso e prevendo penalidades no caso de descumprimento.

Entre os principais **direitos do titular dos dados pessoais** (Art. 18), vale destacar que ele tem direito a obter a qualquer momento e mediante requisição:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;

VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VII - informação das entidades públicas e privadas com as quais a TERRACAP realizou uso compartilhado de dados (informação sobre compartilhamento);

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

Com relação às infrações, as principais **sanções** as quais a Terracap poderá ser submetida são (Art. 52):

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, **de até 2% (dois por cento) do faturamento da pessoa jurídica** de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, **limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração**;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;

XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

III - PLANEJAMENTO DA AUDITORIA

Conforme o Plano de Auditoria Interna - PAINT/2022, (84144379), aprovado pelo Conselho de Administração – CONAD, Parecer 2, (83477186), processo 00111-00012799/2021-16, foi prevista a realização da presente Auditoria Operacional. Neste sentido, foi criado o Processo Sei nº 00111-00002602/2022-11 e, por meio do Memorando Nº 3/2022 - TERRACAP/CONAD/AUDIT (85379960), deu publicidade aos envolvidos acerca do início das atividades de revisão processual.

Na fase preliminar, foi elaborado o Plano de Trabalho - TERRACAP/CONAD/AUDIT (86632529), contendo as diretrizes geral e específicas para execução dos trabalhos. Para tanto, o referido planejamento incluiu a matriz SWOT, que considera os ambientes externo e interno, bem como as forças e oportunidades, levando em consideração as fraquezas e ameaças, procedimento de auditoria esse, que consideramos apropriados neste momento para testar os mecanismos de controles internos afetos à análise, a fim de otimizar a gestão, sem, contudo, emitir uma conclusão estanque sobre os controles internos da Agência de desenvolvimento do Distrito Federal.

Ressalta-se que a Administração da Terracap possui liberdade para conduzir os controles internos necessários, contudo possui o um Controle Interno presente e atuante, e em especial à gestão de riscos que acompanha minuciosamente os pilares da boa gestão, bem como dos cumprimentos de legislação.

Contudo, cabe à gestão fazer constantemente avaliações no sentido de determinar a profundidade, extensão e relevância dos mecanismos de controles internos a serem implementados pelas unidades orgânicas responsáveis, de acordo com as atribuições regimentais, considerando aspectos como: relação custo-benefício; estabelecimento de responsabilidades; segregação de funções; acesso a ativos; estabelecimento de comprovações; testagens autônomas; ferramentas e métodos de processamento de dados; capacidade instalada de pessoal, dentre outros critérios não estáticos. O conceito de custo-benefício reconhece que o custo de um controle não deve exceder os benefícios que ele possa proporcionar. Portanto, há que se avaliar se determinadas recomendações merecem ou não prosperar, ao momento de sua proposição, considerando aspectos técnicos e situacionais, sob à ótica da Administração.

Portanto, delimitou-se o Objetivo Geral assim:

A presente auditoria tem como objetivo geral examinar os controles primários das ações realizadas pela TERRACAP, visando o cumprimento da Lei Geral de Proteção de Dados - LGPD.

Já os objetivos específicos foram estabelecidos, baseados no objetivo geral:

1. Verificar a existência de fluxo/rotina específico para cumprimento da Lei nº 13.709/2018;
2. Verificar a captura e tratamento dos dados pessoais realizados pela Terracap;
3. Verificar os direitos dos titulares dos dados pessoais junto à Terracap;
4. Verificar as situações em que a TERRACAP compartilha dados pessoais dos titulares;
5. Verificar as unidade(s) responsável (eis) pela rotina, tratamento, guarda, e controle dos dados pessoais dos titulares;
6. Verificar as formas de acesso aos dados pessoais dos titulares;
7. Verificar os normativos específicos para realização da rotina;
8. Verificar os bancos de dados disponíveis ou relatórios estruturados de dados pessoais;

9. Verificar a estrutura disponível para tratamento de dados pessoais, suporte eletrônico, informatizado, ou físico;
10. Verificar a existência de ações voltadas à garantia de anonimização de dados pessoais sensíveis;

No tocante aos métodos e técnicas empregados na Auditoria em questão, os trabalhos seguiram as práticas usuais de auditagem. No que se refere às técnicas e aos procedimentos de auditoria foram analisados documentos, banco de dados, processos, observações, relatórios e justificativas de gestores.

Por fim, foram analisados e inseridos no presente processo os seguintes documentos, ainda durante o planejamento:

- Lei nº 13709/2018 - 85928184;

- Decreto nº 42306/2021 - 85929207;

- Norma Organizacional OUV - 04 - 87071188.

IV - SOLICITAÇÕES DE AUDITORIA

No decorrer dos trabalhos foram emitidas as seguintes Solicitações de Auditorias:

- Solicitação de Auditoria nº 50 - 87192458 - Ao GABIN, com vistas ao COGER;

- Solicitação de Auditoria nº 62 - 95862769 - À UNLGPD**;**

- Solicitação de Auditoria nº 68 - 100190970 - À COINT, com vistas à DIGER.

V - DESENVOLVIMENTO DA AUDITORIA

Inicialmente, em resposta à Solicitação de Auditoria nº 50, foi disponibilizado o processo Sei nº 00111-00006361/2019-76, que trata da constituição dos procedimentos de adequação à Lei Geral de Proteção de Dados - LGPD.

Neste processo foi possível detectar que os pedidos de providências visando o cumprimento da citada Lei foram iniciados em março de 2020 - 36301616.

Já em maio de 2021, foi confeccionada a Portaria nº 037/2021 - PRESI (62491769), onde foi criado o Grupo de Trabalho multissetorial com o objetivo de iniciar os procedimentos para implantação da LGPD (Lei Geral de Proteção de Dados) na TERRACAP.

Ato contínuo, ainda no mês de maio daquele ano, foi emitida e publicada a Portaria nº 39/2021 - 62859837, com a designação do Encarregado Setorial pelo tratamento de dados pessoais previstos na legislação em tela.

Ainda em análise ao citado processo, dentre algumas providências foram identificados e juntados ao processo sei nº 00111-00002602/2022-11, os seguintes documentos de maior relevância:

- Matriz de Risco Preliminar LGPD - 101158166;

- Plano de Ação para adequação à LGPD - 91052195;

- Decisão DIRET nº 234/2022, que aprova a matriz e Plano de ação - 101158863;

- Relatório de Impacto - LGPD - 101170855;

- Programa de Governança em Privacidade - 90509011;

- Decisão nº 09/22 - CONAD, que aprova o Programa - 101159509.

É importante frisar que todos os documentos acima foram amplamente divulgados internamente, conforme e-mails no bojo do presente processo, bem como em apresentações realizadas periodicamente nos Conselhos e Comitês da empresa.

Posteriormente, foi emitida a Solicitação de Auditoria nº 62, que teve por objetivo entrevistar o encarregado setorial para tratamento dos dados pessoais, visando apurar as dificuldades, possíveis gargalos, bem como apuração do cumprimento do cronograma proposto. As respostas vieram nos seguintes termos, por meio do Coordenador do Comitê de Proteção em Privacidade de Dados - CPRID:

1. Como anda o cronograma de execução? Está seguindo dentro do previsto?

Para execução dos marcos de conformidade do Plano de ação abaixo discriminados foram autuados 19 processos e encaminhados às unidades responsáveis para execução. Encontram-se no status EM EXECUÇÃO E DENTRO DO PREVISTO.

2. Quantos encontros/oficinas já foram realizados para os empregados da TERRACAP? Há previsão para mais encontros ainda neste exercício?

Já foi realizado um encontro virtual para os gestores e demais empregados com a participação da Ouvidoria e oferecimento de palestra sobre a LGPD – Lei Geral de Proteção de Dados Pessoais. Também foi oferecido treinamento exclusivo ao Comitê de Proteção em Privacidade de Dados – CPRID com duração de 20 horas na Escola de Governo do DF.

Ainda de acordo com a tabela abaixo existe a previsão da realização de treinamentos às unidades relacionadas para a execução do inventário de dados.

UNIDADE	DATA
OUVID	20/09
GERAT/NUDOC/RECEPÇÃO	28/09
GEPES	06/10
GEATE	06/10
GEATE	07/10
GECOM	13/10

GEVED	13/10

3. Os integrantes da Unidade Gestora LGPD já fizeram cursos/treinamentos/seminários sobre o tema?

A UGLGPD não existe como Unidade Gestora. Existe um **ambiente no Sistema Eletrônico de Informações – SEI,** criado com o nome de **UGLGPD** para comunicação direta com o perfil CACI/LGPD (Casa Civil), cujo acesso é somente do Encarregado Setorial (lotado na Ouvidoria) e Suplente (lotada no GABIN), tendo em vista a necessidade de comunicação direta com o Encarregado Governamental e os Encarregados Setoriais dos órgãos. Esse ambiente no SEI foi criado por determinação da Circular n.º 4/2021 - CACI/LGPD, no processo SEI 00002-00003634/2021-09. No entanto, para a administração dos processos relacionados à LGPD na empresa foi constituido o CPRID que é coordenado pelo Encarregado de Proteção de Dados e suplente. A Terracap não possui unidade orgânica específica para esse assunto até o momento.

Para o Comitê de Proteção em Privacidade de Dados – CPRID, formado por pessoas de todas as diretorias foi realizado um treinamento na escola de governo com uma turma exclusiva para a Terracap.

4. Qual a avaliação que a UGLGP faz a respeito da recepção por parte dos empregados em relação à aplicação da LGPD?

A avaliação tem sido muito boa, porém, sabemos da dificuldade em implantar uma nova cultura de proteção de dados na empresa. Isso demanda tempo e esforço de todos.

5. Existe a necessidade de ferramentas tecnológicas para execução do plano criado? se sim, quais?

Sim. Existe a necessidade da aquisição de ferramenta tecnológica para que a empresa esteja apta a executar alguns pontos de conformidade com a LGPD como o tarjamento de documentos para anonimização e proteção de dados pessoais no sistema SEI, Descoberta, classificação e mapeamento Automatizado de Dados Pessoais e Sensíveis, Gerência de pedidos e respostas às requisições de acesso aos dados do Titulares, Gestão do consentimento do usuário, etc. Tais ferramentas deverão ter a orientação da ASIF para definição dessa necessidade.

6. Existe uma comunicação programada para dar ciência à alta direção sobre o andamento dos trabalhos? Se sim, é feita de quanto em quanto tempo e para quem?

Sim. Existe a previsão do CPRID encaminhar um relatório trimestralmente ao Presidente da Terracap, bem como à DIRET e CONAD sobre o andamento da implantação da LGPD na empresa. O 1º relatório será encaminhado até o dia 15 do mês de outubro relatando as realizações do trimestre anterior.

7. Qual o percentual de ações programadas já executadas?

Cerca de 30% das ações incluindo os processos encaminhados para a execução do Plano de Ação.

8. Qual a estrutura da UNLGP hoje? está sendo suficiente?

Para o acompanhamento da execução do Plano de Ação e demais ações de adequação da LGPD a empresa não possui uma estrutura própria para tratar do tema, estando o Encarregado de Proteção de Dados (DPO) lotado na Ouvidoria e a suplente lotada no GABIN, sendo que ambos realizam as atividades relativas à LGPD e também as atividades das suas unidades onde estão lotados. O Encarregado e Suplente ainda coordenam o CPRID - Comitê de Proteção em Privacidade de Dados, que é o Comitê responsável pelo acompanhamento da implantação da LGPD.

Para que os trabalhos do CPRID e as atribuições do Encarregado e Suplente possam ser desempenhados com maior qualidade seria necessário a criação de uma estrutura própria, tendo em vista que o CPRID é formado por membros de todas as diretorias que se reunem uma vez a cada mês.

9. Qual a avaliação da UGLGPD sobre o plano em si?. Está prevista alguma alteração ou ajuste no plano?

Possíveis alterações ou ajustes no atual Plano de ação surgirão após a realização do inventário de dados pessoais que está sendo executado nas unidades OUVID, ASINF, ASCOM, NUDOC, GEATE, GERAT, GECOM, GEVED e GEPES, ou a qualquer tempo a depender da necessidade.

10. Existe a programação de um curso exclusivo para os empregados da TERRACAP na Escola de Governo – Egov-DF?

Foi realizado um curso exclusivo para os empregados da TERRACAP na Escola de Governo – Egov-DF que contou com a participação de cerca de 30 empregados da Terracap incluindo o CPRID.

11. Qual avaliação da UGLGPD sobre a atuação da TERRACAP em relação à aplicação da LGPD?

Estamos em um processo inicial de adequação da empresa à essa nova realidade principalmente no que se refere à criação de normas e procedimentos. Os marcos de conformidade estão sendo executados pelas unidades, os contratos e editais passando por adequaçoes e após essa fase inicial de execução do Plano de ação proposto, entraremos em uma fase importante de treinamento de todos os empregados para que a mudança de cultura em proteção de dados realmente aconteça.

12. Já há a previsão de algum tipo de fiscalização ou avaliação por parte de algum órgão de controle sobre o tema na TERRACAP?

Sim.

13. Quais as dificuldades e ou gargalos identificados até agora para êxito do plano?

A falta de uma estrutura de apoio própria para que o CPRID possa desempenhar suas atividades.

Dando sequência ao desenvolvimento da presente auditoria, foi emitida a Solicitação de Auditoria nº 68 - 100190970, que direcionou à DIGER, para envio do Relatório Gerencial de acompanhamento da Gestão de Riscos, em especial à implementação da LGPD, que respondeu juntando ao presente processo o documento - 100241115, no qual recortamos especificamente:

Abaixo destacam-se algumas das principais medidas desenvolvidas, no 3º Trimestre, como ações de tratamento de riscos da matriz de riscos de LGPD:

ID	Fator/Causa	Produto/Entrega	Processo
LG009	NÃO HÁ CONTROLE DE ACESSO DEFINIDO PARA OS DADOS CONSTANTES DOS SISTEMAS, INCLUSIVE DE DADOS SENSÍVEIS, DE CLIENTES/ EMPREGADOS/ CIDADÃOS/ VISITANTES	Diretrizes de controle de acesso implementadas conforme previsão na Política de Segurança da Informação e Comunicações - POSIC	00111- 00004212/2022-78

Os demais riscos previstos (4 riscos) para desenvolvimento na 1ª fase, dois estão sendo realizados pela ASINF e 3 estão por unidades da DIRAF, são os seguintes:

ID	Fator/Causa	Produto	Data/Data Processo Prorrogada	Processo
LG004	NÃO HÁ PROCEDIMENTO PARA QUE O TITULAR DOS DADOS CONCORDE COM OS TERMOS DE USO DOS DADOS COLETADOS. INCLUSIVE PARA FINS COMERCIAIS E ESTRATÉGIA DE MARKETING	1. Formulários de cadastro adequados (físicos e digitais, para público interno e externo) com Termo de Consentimento de Uso de Dados Pessoais ou informação da finalidade de uso dos dados;	20/10/2022	00111-00004212/2022-78
LG004	NÃO HÁ PROCEDIMENTO PARA QUE O TITULAR DOS DADOS CONCORDE COM OS TERMOS DE USO DOS DADOS COLETADOS. INCLUSIVE PARA FINS COMERCIAIS E ESTRATÉGIA DE MARKETING	2. Artigos/panfletos de publicidade direcionados a serem enviados aos clientes com a inclusão de opção de opt-out em peças de publicidade direcionada enviadas a clientes.	20/10/2022	00111-00003542/2022-46
LG015	TRANSFERÊNCIA DE DADOS ARMAZENADOS A EMPRESAS PARCEIRAS/OUTROS ÓRGÃOS	1. Contratos vigentes adequados;	20/10/2022	00111-00006705/2022-42
LG015	TRANSFERÊNCIA DE DADOS ARMAZENADOS A EMPRESAS PARCEIRAS/OUTROS ÓRGÃOS	3. Minutas padrão de contratos atualizadas	20/10/2022	00111-00006705/2022-42
LG015	TRANSFERÊNCIA DE DADOS ARMAZENADOS A EMPRESAS PARCEIRAS/OUTROS ÓRGÃOS	2. Política de transações com partes relacionadas atualizada (Art. 39, 42, 44, 50);	20/10/2022	00111-00003638/2022-12 (DIRAF) 00111-00005254/2022-78 (item 2-DIRAF)
LG016	MANIPULAÇÃO DE DADOS PESSOAIS E SENSÍVEIS POR PARTE DE EMPRESAS TERCEIRIZADAS	1. Contratos vigentes adequados;	20/10/2022	00111-00006705/2022-42
LG016	MANIPULAÇÃO DE DADOS PESSOAIS E SENSÍVEIS POR PARTE DE EMPRESAS TERCEIRIZADAS	3. Minutas padrão de contratos atualizadas	20/10/2022	00111-00006705/2022-42
LG016	MANIPULAÇÃO DE DADOS PESSOAIS E SENSÍVEIS POR PARTE DE EMPRESAS TERCEIRIZADAS	2. Política de transações com partes relacionadas atualizada (Art. 39, 42, 44, 50);	20/10/2022	00111-00006705/2022-42
LG018	AUSÊNCIA DE POLÍTICA DE MANUTENÇÃO E DESCARTE DOS DADOS DE CLIENTES/ EMPREGADOS/CIDADÃOS/ VISITANTES	Política de retenção e descarte de dados pessoais	20/10/2022	00111-00005254/2022-78

Após avaliação da DIGER, verificou-se que a entrega do risco LG004 necessita de complementação.

Quanto aos riscos LG015 e LG016, tratados no bojo do Processo SEI 00111-00006705/2022-42, as minutas apresentadas pela CPLIC, NUCCA e GECOP estão sendo avaliadas pela COJUR para prosseguimento.

No que se refere ao risco LG018, em trâmite no Processo SEI 00111-00005254/2022-26, o NUDOC informou que, para a elaboração da política de retenção e descarte de dados pessoais, existe a necessidade de aprovação da Tabela de Temporalidade por parte do Arquivo Público do DF, cujo exame está em fase final de aprovação (Despacho DIRAF 94759089).

Considerando que as ações dos planos de respostas estão em fase inicial não foram retratados benefícios neste relatório.

Por fim, a DIGER concluiu que ***"os avanços dos planos de respostas estão dentro do esperado e que os resultados vêm atendendo ao objetivo proposto de auxiliar na mitigação dos riscos, razão pela qual enumeram-se os benefícios obtidos ao longo desses exercícios"***

VI - ANÁLISE

Da documentação analisada, preliminarmente, destaca-se o Plano de Ação para adequação à Lei Geral de Proteção de Dados - LGPD (91052195), o qual delimitou a sequência de ações visando dar início ao cumprimento da legislação.

Sublinha-se os objetivos específicos previstos:

. Identificar as atividades prioritárias a serem desenvolvidas para o atendimento das disposições previstas na LGPD;

. Indicar as medidas necessárias para a adequação da Terracap à Lei Geral de Proteção de Dados Pessoais;

. Fixar parâmetros para assegurar a transparência, a segurança e o respeito aos direitos dos titulares de Dados Pessoais nos serviços prestados pela empresa;

. Fomentar a cultura de Privacidade e Proteção de Dados Pessoais junto aos empregados da Terracap; e

. Promover o engajamento interssetorial no atendimento aos marcos de conformidade atinentes à LGPD.

Quando da divulgação do referido plano de ação, foram informados também os trabalhos já realizados pelo GT/LGPD:

1) Mapeamento e tratamento dos dados pessoais no âmbito da Terracap;

2) Mapeamento dos riscos dos tratamentos de dados na Terracap (matriz de riscos);

3) Relatório de Impacto à Proteção de Dados Pessoais - RIPD;

4) Programa de Governança em Privacidade de Dados;

Por fim, o mencionado Plano também traz os seguintes compromissos:

1. Política de retenção e descarte de dados pessoais;
2. Política de privacidade (interna e externa);
3. Registro de atividades de tratamento de dados pessoais;
4. Inventário de Dados Pessoais;
5. Adequação de formulários de cadastro (físicos e digitais);
6. Inclusão de opção de opt-out em peças de publicidade enviadas aos clientes;
7. Relatório de impacto à proteção de dados pessoais - RIPD);
8. Implementação das Diretrizes de controle de acesso previstas na POSIC;
9. Norma de procedimento de atendimento aos pedidos dos titulares;
10. Norma sobre permissão de acesso aos processos administrativos;
11. Monitoramento e controle das soluções de segurança da informação;
12. Implementação de LOG'S de auditoria nas tabelas de dados críticos;
13. termos de confidencialidade;
14. Adequação dos contratos;
15. Minutas padrão de contratos;
16. Norma de anonimização de dados pessoais;
17. Plano de respostas a incidentes de segurança;
18. Comitê de Proteção em Privacidade de Dados - CPRID;
19. Treinamentos internos sobre a LGPD;
20. Comunicação interna para divulgação da LGPD;
21. Nomeação de DPO (Encarregado setorial de dados);

22. Concepção de novos produtos (principio de privacy by design).

Ato contínuo, detectou-se a confecção da Matriz de Risco preliminar LGPD - 101158166, a qual foi elaborada visando dar cumprimento aos dispostos da Lei nº 13.709/2018, incluindo não só os riscos já previstos na legislação, mas os que podem afetar de fato a saúde da empresa.

Dos riscos com severidade classificada como **EXTREMA**, destacam-se:

- NÃO HÁ CONTROLE DE ACESSO DEFINIDO PARA OS DADOS CONSTANTES DOS SISTEMAS, INCLUSIVE DE DADOS SENSÍVEIS, DE CLIENTES/ EMPREGADOS/ CIDADÃOS/ VISITANTES ;

- NÃO HÁ ACORDO DE SERVIÇO, QUANTO AO USO DA INFRAESTRUTURA DO SISTEMA SEI, QUE IDENTIFICA OS CRITÉRIOS DE ARMAZENAMENTO E ACESSO AOS DADOS DE CLIENTES/ EMPREGADOS/ CIDADÃOS/ VISITANTES CONTIDOS NOS PROCESSOS.;

- NÃO HÁ ACORDO DE SIGILO E CRITÉRIOS DE SEGURANÇA PARA OS PROCESSOS QUE CONTÉM DADOS DE CLIENTES/EMPREGADOS/CIDADÃOS/VISITANTES, QUANTO AO USO DA INFRAESTRUTRA DO SISTEMA SEI;

- AUSÊNCIA DE POLÍTICA DE MANUTENÇÃO E DESCARTE DOS DADOS DE CLIENTES/EMPREGADOS/CIDADÃOS/VISITANTES;

Já dos riscos com severidade classificada como **ALTA**, destacam-se:

- COLETA DE DADOS DE CLIENTES/ EMPREGADOS/ CIDADÃOS/ VISITANTES SEM A DEFINIÇÃO CLARA DOS TIPOS DE DADOS PESSOAIS (COMUNS, SENSÍVEIS OU ANONIMIZADOS);

- AUSÊNCIA DE NORMA PARA CLASSIFICAÇÃO DE CRITICIDADE DE DADOS COLETADOS DE CLIENTES/ EMPREGADOS/ CIDADÃOS/ VISITANTES PARA USO NO PROCESSO RESPONSÁVEL PELA COLETA;

- AUSÊNCIA DE POLÍTICA DE FINALIDADE DE COLETA E TRATAMENTO DOS DADOS DE CLIENTES/ EMPREGADOS/ CIDADÃOS/ VISITANTES COLETADOS;

- NÃO HÁ PROCEDIMENTO PARA QUE O TITULAR DOS DADOS CONCORDE COM OS TERMOS DE USO DOS DADOS COLETADOS. INCLUSIVE PARA FINS COMERCIAIS E ESTRATÉGIA DE MARKETING;

- OS DADOS NÃO POSSUEM CLASSIFICAÇÃO DE CRITICIDADE QUE PERMITAM TRATAMENTO ESPECÍFICO NOS SISTEMAS DE INFORMAÇÕES.

- OS DADOS SENSÍVEIS NÃO POSSUEM CRIPTOGRAFIA;

- TRANSFERÊNCIA DE DADOS ARMAZENADOS A EMPRESAS PARCEIRAS/OUTROS ÓRGÃOS;

- MANIPULAÇÃO DE DADOS PESSOAIS E SENSÍVEIS POR PARTE DE EMPRESAS TERCEIRIZADAS;

- AS ATIVIDADES INTERNAS UTILIZAM DADOS ALÉM DOS ESSENCIAIS PARA A FINALIDADE DO PROCESSO.

Há de se registrar que para todos os riscos, já há produtos em execução para entrega, dentro do prazo estipulado, com resposta satisfatória para o monitoramento de riscos.

Neste ínterim, é importante ressaltar que houve a ampla divulgação interna de cada ação, buscando não só informar os empregados da empresa, mas iniciar concomitantemente a nova cultura organizacional.

Com relação à análise do Relatório de Impacto - LGPD - 101170855, destaca-se que é um documento bem detalhado de todas as ações realizadas, em desenvolvimento e a executar, que demonstraram o impacto atual e futuro, destacando as seguintes medidas para tratamento dos riscos:

1. Elaboração de Política de retenção e descarte de dados pessoais (Art. 6, II, III, IV; Art. 9, II; Art. 15; Art. 16; Art. 37; Art. 40);

2. Registro de atividades de tratamento (Art. 6, II, III, IV; Art. 9, II; Art. 15; Art. 16; Art. 37; Art. 40);

3. Inventário de dados pessoais (Art. 6, II, III, IV; Art. 9, II; Art. 15; Art. 16; Art. 37; Art. 40);

4. Adequação de formulários de cadastro (físicos e digitais, para público interno e externo) com Termo de Consentimento de Uso de Dados Pessoais e/ou informação da finalidade de uso dos dados (Art. 39, 42, 44, 50 Art.6º, V);

5. Inclusão de opção de opt-out em peças de publicidade direcionada enviadas a clientes (Art. 7º, I; 8º; 11º, I; 14º);

6. Elaboração e revisão periódica do Relatório de Impacto a Proteção de Dados Pessoais (RIPDP) (Art. 10, § 3º; Art. 32 e 38) – trata-se do presente Relatório, que deverá ser atualizado periodicamente;

7. Implementação das diretrizes de controle de acesso já previstas na Política de Segurança da Informação e Comunicações (POSIC);

8. Formalização de Termo de cooperação com a Secretaria de Economia do DF sobre o uso seguro do SEI;

9. Elaboração de norma interna com o procedimento para garantir o atendimento dos pedidos dos titulares quanto aos seus direitos (incluindo formulário) (Art. 8, § 5º, 9, § 2º, 17, 18, 19, 20, 21, 22);

10. Elaboração de norma interna sobre a permissão de acesso a processos administrativos no âmbito da Terracap em harmonia da LGPD com a LAI;

11. Monitoramento e controle das soluções de segurança da informação da Terracap (firewall, anti-spam, antivírus, etc), a fim de manter estrutura segura para armazenamento dos dados;

12. Implementação de Logs de auditoria em todas as tabelas de dados críticos;

13. Termos de confidencialidade assinados por todos os empregados e terceirizados que farão o uso de dados reais de clientes/empregados/cidadãos/etc para o desenvolvimento e teste de sistemas;

14. Adequação dos contratos vigentes às exigências da LGPD;

15. Atualização da Política de transações com partes relacionadas (Art. 39, 42, 44, 50);

16. Atualização das minutas padrão de contratos às exigências da LGPD (Art. 39, 42, 44, 50 Art.6º, V);

17. Elaboração de instrumento interno de orientação para os casos em que seja necessária fazer a anonimização de dados durante o seu tratamento (sugestão, atualização de previsão geral no Código de Conduta e Integridade);

18. Criação de Comitê interno permanente, formado de maneira interdisciplinar por representantes dos setores envolvidos na implementação da LGPD (sugerimos que tenha participação do GABIN, OUVID, ASINF, CPLAM, COJUR, GEATE, GECOM, GEVED, GEARI e GERAT prioritariamente, podendo ter

participação das demais gerências), para acompanhamento contínuo do processo de implementação da Lei, com a participação do Encarregado Setorial de Dados;

19. Realização de treinamento inicial do Comitê acerca da LGPD e seus impactos na rotina de trabalho para disseminação do conhecimento, com vistas ao alinhamento de todos os membros do Comitê acerca do escopo dos trabalhos;

20. Desenvolvimento de ações de comunicação interna, visando à divulgação da LGPD, das adaptações em normativos e procedimentos internos a ela relacionados e das atividades do Comitê;

21. Certificação do DPO (Titular e suplente) na LGPD e ISO 27.001 (com sugestão de treinamento para todos os participantes do Comitê).

Por fim, registra-se que o citado relatório de impacto tem previsão de revisão e atualizado anual.

Ato contínuo, o documento analisado foi o Programa de Governança em Privacidade - 90509011, que define diretrizes para a gestão da segurança do tratamento dos dados pessoais, nos meios físicos e digitais, em tratamentos manuais ou automatizados, com o propósito de proteger a privacidade de todos os titulares de dados pessoais tratados pela empresa, disciplinando as políticas e as boas práticas sobre privacidade e proteção de dados pessoais, alinhando-se ao Programa de Governança Corporativa da Terracap.

Deve ser implementado por todas as unidades organizacionais, de acordo com as instruções estabelecidas nos documentos de privacidade e orientação do Comitê de Proteção em Privacidade de Dados Pessoais – CPRID, contemplando responsabilidades e prazos, e ainda, compor a Prestação de Contas Anual.

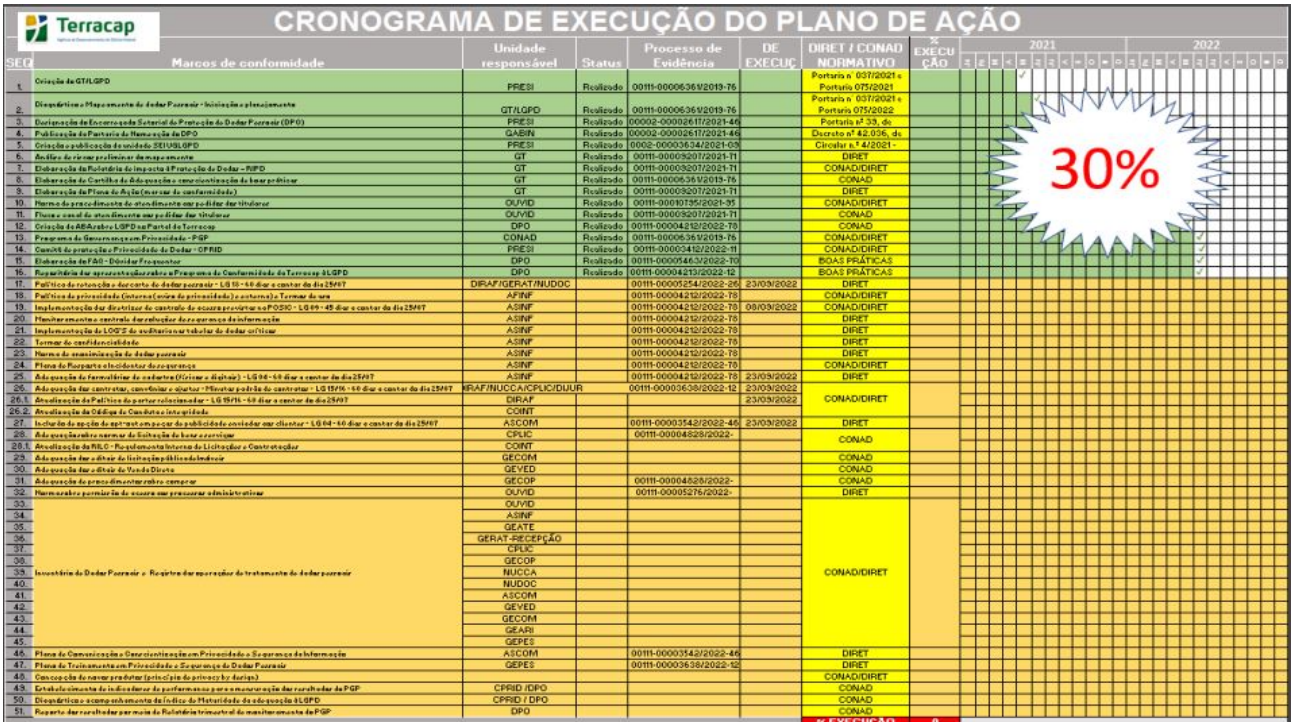
O monitoramento e a divulgação dos resultados do Programa, interna e externamente, devem ser realizados pelo Comitê de Proteção em Privacidade de Dados Pessoais – CPRID, e o plano de respostas a incidentes de segurança da Terracap será estabelecido em normativo próprio, contendo o protocolo a ser seguido em caso de ocorrência de violação ou incidente de segurança em privacidade que possa acarretar risco ou dano relevante ao titular.

O referido programa apresenta estrutura sólida e passível de execução, caracterizando como satisfatório dentro do pretendido.

JÁ no que diz respeito as informações apresentadas pelo Coordenador do Comitê de Proteção em Privacidade de Dados - CPRID, em resposta á entrevista, destaca-se que a implementação está sendo feita de modo segmentado, com etapas previstas para cumprimento, e até a data da manifestação ocorre de forma regular, **totalizando 30%** do cronograma já executado.

Ressalta-se a opinião expressa do Coordenador da necessidade de uma estrutura de apoio própria para que o CPRID possa desempenhar suas atividades, onde atualmente só há a existência no sistema SEI para comunicação interna e externa.

As informações prestadas vão de encontro á apresentação feita pelo próprio Comitê (91304715), onde de forma clara, objetiva e didática ficou demonstrada a evolução das ações e compromissos previstos no Plano de Ação - LGPD, bem como o desempenho do cronograma:



SEQ	Marcos de conformidade	Unidade responsável	Status	Processo de Evidência	DE EXECUÇ	DIRET / CONAD NORMATIVO	% EXECUÇÃO
1.	Criação do GT/LGPD	PRESI	Realizado	00111-00006361/2019-76		Portaria n° 037/2021 e Portaria 075/2021	
2.	Diagnóstico e Mapeamento do dodar Psoreair - Iniciação e planejamento	GT/LGPD	Realizado	00111-00006361/2019-76		Portaria n° 037/2021 e Portaria 075/2022	
3.	Designação do Encarregado Setorial de Proteção do Dodar Psoreair (DPO)	PRESI	Realizado	00002-00002611/2021-46		Portaria nº 39, de	
4.	Publicação da Portaria de Nomeação do DPO	GABIN	Realizado	00002-00002611/2021-46		Decreto nº 42.036, de	
5.	Criação e publicação de unidade SEI/USLGPD	PRESI	Realizado	0002-00003634/2021-03		Circular n.º 41/2021 -	
6.	Análise de risco preliminar do mapeamento	GT	Realizado	00111-00003207/2021-71		DIRET	
7.	Elaboração da Política de Impacto à Proteção do Dodar - RIPD	GT	Realizado	00111-00003207/2021-71		CONAD/DIRET	
8.	Elaboração da Cartilha de Adequação e conscientização de boas práticas	GT	Realizado	00111-00006361/2019-76		CONAD	
9.	Elaboração do Plano de Ação (mensuração do cumprimento)	GT	Realizado	00111-00003207/2021-71		DIRET	
10.	Normas de procedimento de atendimento ao público (ao titular)	OUVID	Realizado	00111-00010135/2021-91		CONAD/DIRET	
11.	Fluxo e canal de atendimento ao público (ao titular)	OUVID	Realizado	00111-00003207/2021-71		CONAD	
12.	Criação do ABA/subtro LGPD no Portal da Terracap	DPO	Realizado	00111-00004212/2022-76		CONAD	
13.	Programa de Governança em Privacidade - PGP	CONAD	Realizado	00111-00006361/2019-76		CONAD/DIRET	
14.	Comitê de proteção à Privacidade do Dodar - CPRID	PRESI	Realizado	00111-00003412/2022-11		CONAD/DIRET	
15.	Elaboração do FAQ - Dúvidas Frequentes	DPO	Realizado	00111-00005440/2022-70		BOAS PRÁTICAS	
16.	Responsável por apresentar subsídios a Programa de Conformidade da Terracap à LGPD	DPO	Realizado	00111-00004213/2022-12		BOAS PRÁTICAS	
17.	Política de retenção e descarte do dodar psoreair - LG 10 - 10 dias a contar da dia 25/07	DIRAF/GERAT/NUDOC		00111-00005254/2022-26	23/03/2022	DIRET	
18.	Política da privacidade (interna (visão da privacidade) e externa) e Termos de uso	AFINF		00111-00004212/2022-76		CONAD/DIRET	
19.	Implementação das diretrizes de controle de acesso previstas na POSIC - LG 09 - 45 dias a contar da dia 25/07	ASINF		00111-00004212/2022-76	08/03/2022	CONAD/DIRET	
20.	Monitoramento e controle da evolução de governança da informação	ASINF		00111-00004212/2022-76		DIRET	
21.	Implementação da LOG'S de ordenamento e tabelas do dodar or/ilcar	ASINF		00111-00004212/2022-76		DIRET	
22.	Termos de confidencialidade	ASINF		00111-00004212/2022-76		DIRET	
23.	Norma de anonimização de dodar psoreair	ASINF		00111-00004212/2022-76		DIRET	
24.	Plano de Resposta a incidentes de segurança	ASINF		00111-00004212/2022-76		CONAD/DIRET	
25.	Adequação de formulários de cadastro (físicos e digitais) - LG 04 - 60 dias a contar da dia 25/07	ASINF		00111-00004212/2022-76	23/03/2022	DIRET	
26.	Adequação dos contratos, convênios e ajustes - Minutas padrão de contratos - LG 15/16 - 60 dias a contar da dia 25/07	DIRAF/NUCCA/CPLIC/DIJUR		00111-00003638/2022-12	23/03/2022	CONAD/DIRET	
26.1	Atualização da Política de proteção de dados - LG 15/16 - 60 dias a contar da dia 25/07	DIRAF			23/03/2022		
26.2	Atualização do Código de Condutas e Integridade	COINT					
27.	Inclusão da opção de opt-out em peças de publicidade enviadas aos clientes - LG 04 - 60 dias a contar da dia 25/07	ASCOM		00111-00003542/2022-46	23/03/2022	DIRET	
28.	Adequação dos normas de Solicitação de bens e serviços	CPLIC		00111-00004828/2022-		CONAD	
28.1	Atualização do RILC - Regulamento Interno de Licitações e Contratações	COINT					
29.	Adequação das áreas de licitações públicas do dodar	GECOM				CONAD	
30.	Adequação das áreas de Venda Direta	GEVED				CONAD	
31.	Adequação de procedimentos dos compras	GECOP		00111-00004828/2022-		CONAD	
32.	Normas dos permissão de acesso aos processos administrativos	OUVID		00111-00005276/2022-		DIRET	
33.		OUVID					
34.		ASINF					
35.		GEATE					
36.		GERAT-RECEPÇÃO					
37.		CPLIC					
38.		GECOP					
39.	Inventário do Dodar Psoreair e Registro das operações de tratamento do dodar psoreair	NUCCA				CONAD/DIRET	
40.		NUDOC					
41.		ASCOM					
42.		GEVED					
43.		GECOM					
44.		GEARI					
45.		GEPES					
46.	Plano de Comunicação e Conscientização em Privacidade e Segurança da Informação	ASCOM		00111-00003542/2022-46		DIRET	
47.	Plano de Treinamento em Privacidade e Segurança do Dodar Psoreair	GEPES		00111-00003638/2022-12		DIRET	
48.	Concepção de normas produtos (princípio de privacy by design)					CONAD/DIRET	
49.	Estabelecimento de indicadores de performance para mensuração dos resultados do PGP	CPRID /DPO				CONAD	
50.	Diagnóstico acompanhamento do índice de Maturidade da adequação à LGPD	CPRID / DPO				CONAD	
51.	Reporte dos resultados por meio do Relatório trimestral de monitoramento do PGP	DPO				CONAD	

Posto isso, é transparente o compromisso e empenho do Comitê, ainda que sem estrutura orgânica, para um tema permanente.

Por conseguinte, analisou-se os dados informados no Relatório Gerencial de Riscos, em especial à implementação da LGPD, confeccionado pela DIGER - 100241115 :

Dos riscos monitorados pela Divisão de Riscos, unidade orgânica da Controlaria Interna - COINT, e já demonstrados **no item V**, destaca-se a avaliação da DIGER, conforme a seguir:

Risco LG 04 - NÃO HÁ PROCEDIMENTO PARA QUE O TITULAR DOS DADOS CONCORDE COM OS TERMOS DE USO DOS DADOS COLETADOS. INCLUSIVE PARA FINS COMERCIAIS E ESTRATÉGIA DE MARKETING - *Necessita de complementação;*

Riscos LG 015 e 016 - TRANSFERÊNCIA DE DADOS ARMAZENADOS A EMPRESAS PARCEIRAS/OUTROS ÓRGÃOS, TRANSFERÊNCIA DE DADOS ARMAZENADOS A EMPRESAS PARCEIRAS/OUTROS ÓRGÃOS, MANIPULAÇÃO DE DADOS PESSOAIS E SENSÍVEIS POR PARTE DE EMPRESAS TERCEIRIZADAS, MANIPULAÇÃO DE DADOS PESSOAIS E SENSÍVEIS POR PARTE DE EMPRESAS TERCEIRIZADAS, MANIPULAÇÃO DE DADOS PESSOAIS E SENSÍVEIS POR PARTE DE EMPRESAS TERCEIRIZADAS - *estão sendo avaliadas pela COJUR, para prosseguimento.*

Risco LG 18 - AUSÊNCIA DE POLÍTICA DE MANUTENÇÃO E DESCARTE DOS DADOS DE CLIENTES/ EMPREGADOS/CIDADÃOS/ VISITANTES - *há a necessidade de uso de tabela de temporalidade por parte do ARPDF, cujo exame está em fase de aprovação pela DIRAF.*

Diante do exposto, a conclusão da DIGER está em consonância com os dados apresentados, ratificando que as ações dos planos de respostas estão em fase inicial, ocorrendo dentro do planejado.

VII - RECOMENDAÇÕES

R.1 - Recomendar à COINT/DIGER *que monitore constantemente, em especial os prazos previstos na matriz de riscos, as recomendações elencadas no Relatório Gerencial - 3º trimestre /2022-DIGER, com relação aos riscos: LG's 04, 015, 016 e 018, noticiando esta AUDIT trimestralmente;*

R.2 - Recomendar à DIRAF *estudo visando a possibilidade de criação de estrutura orgânica nos moldes da CPRID, visando melhorar a eficácia e eficiência das ações referentes à implementação da LGPD;*

R.3 - Recomendar à PRESI *que promova junto às áreas responsáveis (OUVID, CPRID), com a supervisão da COINT/DIGER, revisão do Plano de Ação - LGPD, a cada semestre nos 2 primeiros anos de implementação da LGPD, bem como constante monitoramento do cronograma de execução proposto visando a efetiva implementação da LGPD na TERRACAP;*

R.4 - Recomendar à PRESI e DIRAF, *a adoção de medidas visando a capacitação periódica dos empregados e colaboradores envolvidos na implementação da LGPD;*

R.5 - Recomendar à DIJUR/COJUR, *que promova a análise das minutas acostadas no processo sei nº 00111-00006705/2022-42, visando mitigar os riscos LG 015 e 016;*

R.6 - Recomendar à PRESI, com vistas à ASINF, *providências visando a* aquisição de ferramenta tecnológica para que a empresa esteja apta a executar alguns pontos de conformidade com a LGPD como o tarjamento de documentos para anonimização e proteção de dados pessoais no sistema SEI, Descoberta, classificação e mapeamento Automatizado de Dados Pessoais e Sensíveis, Gerência de pedidos e respostas às requisições de acesso aos dados do Titulares, Gestão do consentimento do usuário, etc

R.7 - Recomendar à PRESI, *ações visando o aperfeiçoamento constante dos normativos internos relacionados à LGPD, inclusive com a divulgação interna de cartilhas, afim de promover a conscientização da importância da LGPD;*

VIII - MANIFESTAÇÃO DAS ÁREAS

Após o envio do Relatório preliminar nº 06/2022-AUDIT - 101110822, e apesar do tempo exíguo para manifestação, as seguintes áreas diretamente envolvidas no objeto responderam:

COINT/DIGER - 101887533

"Em atenção ao Relatório de Auditoria 6 (101110822), quanto a recomendação:

"R.1 - Recomendar à COINT/DIGER *que monitore constantemente, em especial os prazos previstos na matriz de riscos, as recomendações elencadas no Relatório Gerencial - 3º trimestre /2022-DIGER, com relação aos riscos: LG's 04, 015, 016 e 018, noticiando esta AUDIT trimestralmente; (...).*

Esclarecemos que esta Divisão monitora mensalmente todos os prazos constantes na Matriz de Riscos, por meio de avaliação dos processos que constam as ações executadas para o tratamento dos riscos. Esclarecemos ainda que as atividades realizadas por essa Divisão são descritas em relatório e enviadas trimestralmente ao CONFI e ao COAUD. Estamos à disposição caso sejam necessários maiores esclarecimentos."

PRESI/ASINF - 102038956

"R.6 - Recomendar à PRESI, com vistas à ASINF, *providências visando a aquisição de ferramenta tecnológica para que a empresa esteja apta a executar alguns pontos de conformidade com a LGPD como o tarjamento de documentos para anonimização e proteção de dados pessoais no sistema SEI;"*

Esclarecemos que a ASINF realizou uma análise técnica sobre esse serviço. Essa análise consta no Doc. SEI 101732945.

Em relação ao a segunda parte da recomendação:

"R.6 - Recomendar à PRESI, com vistas à ASINF, *providências visando a aquisição de ferramenta tecnológica para que a empresa esteja apta a executar alguns pontos de conformidade com a LGPD como a Descoberta, classificação e mapeamento Automatizado de Dados Pessoais e Sensíveis, Gerência de pedidos e respostas às requisições de acesso aos dados do Titulares, Gestão do consentimento do usuário, etc."*

A ASINF irá utilizar os elementos apontados em subsídio ao trabalhos desta unidade.

PRESI/CPRID - 101647658

"Em atenção ao **Relatório de Auditoria n.º 6/2022 - TERRACAP/CONAD/AUDIT**(101110822), este Comitê registra que tomou conhecimento e considera muito pertinente as observações realizadas, em especial as recomendações encaminhadas para as unidades envolvidas. Quanto a isso, na reunião do dia 15/012/2022, este CPRID analisou tais recomendações e gostaria de realizar algumas considerações a titulo de colaboração o que segue:

Quanto à R2 - Este CPRID achou muito pertinente tal recomendação, pois entende que a criação de uma unidade específica sobre o tema é necessária, tendo em vista que o assunto **Privacidade e Proteção de Dados Pessoais** no âmbito dos órgãos e entidades do DF, ou mesmo em todas as grandes empresas, é algo permanente e merece muita atenção por parte da direção desta Companhia. Além disso, no processo de adequação em LGPD realizado na Terracap, além da sua importância, surgiu uma grande quantidade de novos processos de trabalho, sendo extremamente necessária a criação de estrutura mínima que dê suporte ao volume de trabalho atualmente existente. Além disso, após esse período de adequação, seguiremos com o monitoramento permanente, ou seja esse é um processo sem volta. Hoje não tem unidade orgânica na estrutura orgânizacional para tratar do tema pois o CPRID é um comitê com pessoas de todas as diretorias que se reunem periodicamente. Sugerimos que tal estrutura não seja "nos moldes da CPRID", pois esse comitê não é unidade orgânica.

Quanto ao R.3 - Independentemente do acompanhamento das nossas unidades de controle interno, *Compliance*, Riscos, Audit e etc, o CPRID em seu planejamento de trabalho já prevê a supervisão da execução do **Programa de Governança em Privacidade - PGP** e do **Plano de Ação para adequação da Terracap à LGPD**, estando previsto também o acompanhamento/monitoramento permanente tanto das ações de adequação quanto das unidades da empresa nas ações relacionadas à LGPD."

IX - ANÁLISE DA AUDITORIA INTERNA

Diante dos esclarecimentos prestados pelas áreas no item VIII, esta AUDIT avalia que as justificativas estão em consonância com o apurado neste documento, e ainda há alguns despachos em andamento até a presente data, o que não permitiu a análise até o fechamento do presente relatório.

X- CONCLUSÃO

Considerando o contexto organizacional da TERRACAP, neste trabalho a Auditoria Interna avaliou a observância, adequação, implementação e aplicação em âmbito interno das diretrizes contidas na Lei Geral de Proteção de Dados, que dispõe sobre o tratamento de dados pessoais, tanto em meios físicos quanto digitais, com o objetivo de proteger os direitos fundamentais de liberdade, de privacidade, dentre outros, culminando, dessa forma, em um diagnóstico atualizado da realidade da Empresa, com o objetivo de aperfeiçoar a gestão e minimizar os riscos contidos no processo.

Portanto, esta unidade de controle interno se debruçou no exame de controles primários, de fluxograma dos processos e procedimentos relativos ao gerenciamento dos riscos associados à proteção de dados, considerando aspectos como a fragilidade no sistemas de gestão corporativos; insuficiência de funcionalidades nos sistemas; ausência de identificação e classificação necessários; ausência de integração automática de sistemas; insuficiência de relatórios integrados específicos que atendam a Lei 13.709/2018; possibilidade de customização dos sistemas em utilização na empresa; possibilidade de migração de sistemas; possibilidade de substituição de sistemas; depuração dedados da empresa;; dentre outras criticidades exploradas ao longo deste relatório.

Após os esclarecimentos apresentados pelas áreas envolvidas diretamente, há as ações em andamento para a implementação da LGPD, a qual poderá atingir o aprimoramento em larga escala com melhores resultados. Para isso, ratifica-se as recomendações de melhorias nas rotinas e controles internos, devidamente recepcionadas pelas áreas envolvidas no processo

Diante do exposto, conclui-se pela implementação adequada da Lei Geral de Proteção de Dados - LGPD no âmbito da TERRACAP, ainda em execução, no que diz respeito aos controles primários, desde que atendidas as seguintes recomendações:

R.1 - Recomendar à COINT/DIGER *que monitore constantemente, em especial os prazos previstos na matriz de riscos, as recomendações elencadas no Relatório Gerencial - 3º trimestre /2022-DIGER, com relação aos riscos: LG's 04, 015, 016 e 018,* ***noticiando esta AUDIT trimestralmente;***

R.2 - Recomendar à DIRAF *estudo visando a possibilidade de criação de estrutura orgânica para execução dos trabalhos referentes à implementação da LGPD de forma permanente, visando melhorar a eficácia e eficiência das ações;*

R.3 - Recomendar à PRESI *que promova junto às áreas responsáveis (OUVID, CPRID), com a supervisão da COINT/DIGER, revisão do Plano de Ação - LGPD, a cada semestre nos 2 primeiros anos de implementação da LGPD, bem como constante monitoramento do cronograma de execução proposto visando a efetiva implementação da LGPD na TERRACAP;*

R.4 - Recomendar à PRESI e DIRAF *a adoção de medidas visando a capacitação periódica dos empregados e colaboradores envolvidos na implementação da LGPD;*

R.5 - Recomendar à DIJUR/COJUR *que promova a análise das minutas acostadas no processo sei nº 00111-00006705/2022-42, visando mitigar os riscos LG 015 e 016;*

R.6 - Recomendar à PRESI, com vistas à ASINF *providências visando a* aquisição de ferramenta tecnológica para que a empresa esteja apta a executar alguns pontos de conformidade com a LGPD como o tarjamento de documentos para anonimização e proteção de dados pessoais no sistema SEI, Descoberta, classificação e mapeamento Automatizado de Dados Pessoais e Sensíveis, Gerência de pedidos e respostas às requisições de acesso aos dados do Titulares, Gestão do consentimento do usuário, etc

R.7 - Recomendar à PRESI, com vistas à CPRID *e* ***ASCOM,*** *ações visando o aperfeiçoamento constante dos normativos internos relacionados à LGPD, inclusive com a divulgação interna de cartilhas, afim de promover a conscientização da importância da LGPD;*

DIVULGAÇÃO DOS RESULTADOS DA AUDITORIA

A divulgação dos resultados da auditoria é medida de transparência ativa privilegiada pelos Artigos 3º, I e II; 7º, VII, "b"; 8º, §2º, todos da Lei nº 12.527/2011 e deve ter lugar após a aprovação do Relatório Final, incorporando-se eventuais correções e acréscimos.

À superior consideração.

CLAUDIA TOLENTINO

PEDRO LUIZ ROCHA DE NORONHA

1. Aprovo a íntegra do presente Relatório de Auditoria Operacional nº 08/21022-AUDIT.

2. Encaminhe-se o presente **Relatório de Auditoriia nº 08/2022-** AUDIT à **PRESI, DIJUR, DIRAF,** e **COINT**, com vistas as suas respectivas unidades, para conhecimento e providências quanto às recomendações apontadas no item X, concedendo **prazo de 03 (três) meses**, **a saber: 19/03/2023**, nos termos da IS nº 03/2021 - PRESI.

À **ASSOC**, com vistas ao **COAUD,** para conhecimento.

DENI AUGUSTO PEREIRA FERREIRA e SILVA

Chefe da Auditoria Interna

Documento assinado eletronicamente por **DENI AUGUSTO PEREIRA FERREIRA E SILVA - Matr.0002060-5**, **Chefe da Auditoria Interna**, em 16/12/2022, às 19:24, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **CLAUDIA THEREZA ROCHA TOLENTINO BARROS - Matr. 0002819-3**, **Assessor(a)**, em 16/12/2022, às 19:33, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **PEDRO LUIZ ROCHA DE NORONHA - Matr.0002514-3**, **Assessor(a)**, em 16/12/2022, às 19:55, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

A autenticidade do documento pode ser conferida no site: http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 verificador= **101977533** código CRC= **4B2AF094**.

"Brasília - Patrimônio Cultural da Humanidade"

SAM BLOCO F EDIFICIO SEDE - Bairro Brasilia - CEP 70620-000 - DF

33421819