NOTA TÉCNICA XX - CONACI

PAPEL DOS ÓRGÃOS DE CONTROLE NA ADEQUAÇÃO À LGPD

1. INTRODUÇÃO

A **Câmara Técnica 03 – Estudos sobre a implementação da Lei Geral de Proteção de Dados Pessoais (LGPD)** foi criada com o objetivo de assessorar o Conselho Nacional de Controle Interno (Conaci) em assuntos relacionados à LGPD, notadamente quanto ao fomento à cultura da privacidade e proteção de dados; monitoramento da implementação da LGPD nos órgãos de controle interno do Poder Executivo e entes federativos; promoção de capacitação aos associados sobre privacidade e proteção de dados; promoção de apoio interinstitucional e intercâmbio de informações; além de instituição de banco de conhecimento para fonte de pesquisa com modelos de documentos e arquivos relacionados à privacidade e proteção de dados.

No contexto dos debates na Câmara Técnica e até mesmo da plenária, levantou-se questionamento quanto ao papel do Controle Interno no tocante à adequação e ao monitoramento das instituições públicas em relação à LGPD. Em resumo, o que se busca responder é *em que medida deve o controle interno se ater às questões relativas à adequação das instituições públicas à LGPD e ao monitoramento desta adequação*.

A presente Nota Técnica apresenta o resultado das discussões técnicas entre os membros da CT a fim de subsidiar o Conaci com elementos para compreender claramente os papéis e responsabilidades das Unidades Centrais de Controle Interno (UCCI) no que concerne à adequação da Administração Pública aos dispositivos exigidos pela LGPD.

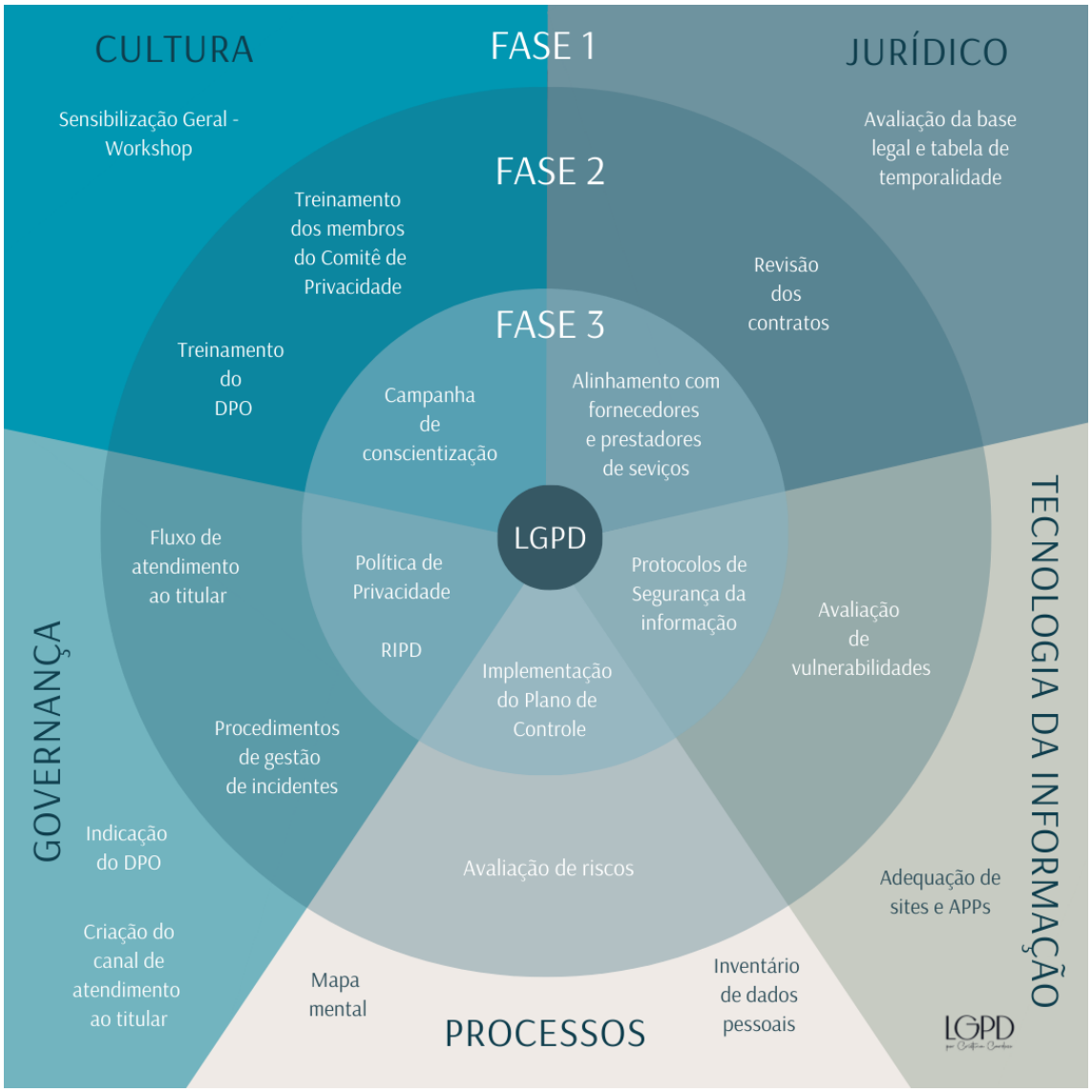
Como base teórica para os posicionamentos aqui traçados, foi adotado o Modelo de Três Linhas por ser "*uma forma simples e eficaz de melhorar a comunicação do gerenciamento de riscos e controle por meio do esclarecimento dos papéis e responsabilidades essenciais*", como salienta a declaração de posicionamento do Institute of Internal Auditors (IIA) sobre o tema.

A adoção do modelo das três linhas de defesa proporciona uma estrutura clara para gerenciar riscos e fortalecer controles internos, dividindo responsabilidades entre a gestão operacional, funções de controle e auditoria interna.

Antes mesmo de abordar os papéis de cada uma das linhas de defesa no que se refere à adequação do órgão à LGPD, é necessário tratarmos ainda que de maneira resumida, das tarefas que o órgão precisa percorrer até que se possa considerar efetivamente adequado. **Importante também ressalvar que a adequação de uma instituição à LGPD não é estanque: estar adequado à LGPD significa estar inserido em um contexto de contínuo monitoramento e revisão de controles, de caráter cíclico**.

Feitas as devidas ressalvas, é essencial abordar as dimensões que envolvem a adequação à LGPD. A esse respeito, vale trazer a figura abaixo, que aborda de maneira didática como se dividem as tarefas de adequação à LGPD, distribuindo-as

em cinco dimensões (Cultura, Jurídico, Tecnologia da Informação, Processos e Governança), cada uma delas dividida em 3 fases. A porção mais externa da figura representa as fases iniciais e as porções mais próximas do centro, as fases finais do ciclo de adequação.



Fonte: criada pela autora Cristina Cardoso

Assim, quanto à dimensão da cultura em LGPD, uma ação inicial do órgão é promover uma sensibilização geral dos servidores; em um estágio mais avançado, proporcionará um treinamento específico para o encarregado de dados (DPO) assim como para os membros do comitê de privacidade ou grupo de trabalho; e em última instância, terá produzido e divulgado uma campanha de conscientização de seus servidores quanto à LGPD. O mesmo raciocínio se aplicará às demais dimensões da figura acima.

Identificadas as vantagens da utilização do modelo das três linhas de defesa e distribuídas as ações necessárias à implementação entre as cinco dimensões, **é importante pontuar o quanto a adequação à Lei Geral de Proteção de Dados perpassa pela gestão de riscos**. Isso fica evidente a partir da observância do conteúdo dos princípios da segurança (artigo 6º, VII), da prevenção (artigo 6º, VIII) e da

responsabilização e prestação de contas (artigo 6º, X), bem como a partir da leitura da Seção III do Capítulo VI e do Capítulo VII da lei brasileira, que, respectivamente, dispõem sobre a responsabilidade e ressarcimento dos danos e sobre a segurança dos dados dos titulares.

Além disso, a necessidade de previsão das medidas de segurança adotadas em determinados processos de tratamento de dados - medida estas que serão consignadas no inventário de dados pessoais - é outro exemplo de como a Lei Geral de Proteção de Dados é pautada na gestão de riscos.

Com efeito, ao produzir o inventário de dados, deverá o responsável por sua elaboração registrar as medidas de segurança adotadas no processo ao qual se refere. Com base nessa informação, caberá ao agente de tratamento determinar a inclusão de novas medidas de segurança ou, eventualmente, aceitar o risco.

De modo semelhante, o responsável (ou grupo responsável) pela 2ª linha, que fornece apoio complementar, com uma visão mais ampla do processo, e se propondo a monitorar e dar apoio, mas sem o envolvimento direto nas operações (1ª linha) nem na auditoria (3ª linha). É o caso, por exemplo, da condução da realização do diagnóstico preliminar e da elaboração do plano de trabalho para implementação das adequações à LGPD, que compreendem sistematizar e planejar o conjunto de ações que envolvem pessoas, processos e sistemas naquilo que se refere à coleta, processamento, análise, armazenamento e compartilhamento de dados dentro da organização. Essa atividade deverá ser realizada com o patrocínio da alta gestão e a cooperação dos gestores, porém será conduzida pela 2ª linha, no exercício do seu papel de assessoria.

Diante da vinculação entre a LGPD e a gestão de riscos trazidas no bojo da própria lei, bem como da relação intrínseca desta gestão de riscos com as atividades do controle interno, apresenta-se adequada a utilização do modelo das 3 linhas de defesa enquanto substrato teórico para adequação do órgão ou instituição pública à LGPD.

2. MODELO DAS 3 LINHAS E A LGPD

2.1 A primeira linha: os donos dos processos

Estabelecida a premissa de que é adequada a utilização do modelo das três linhas de defesa para a adequação dos órgãos à LGPD e ao monitoramento desta adequação, cabe avaliar como deverão ser efetivados esses processos.

Segundo o IIA, a responsabilidade da gestão de atingir os objetivos organizacionais compreende os papéis da primeira e segunda linhas. Os papéis de primeira linha estão mais diretamente alinhados com a entrega de produtos e/ou serviços aos clientes da organização, incluindo funções de apoio. Os papéis de segunda linha fornecem assistência no gerenciamento de riscos. [1]

[1] IIA. (2020). MODELO DAS TRÊS LINHAS DO IIA 2020. Retrieved novembro, 2024, from https://iiabrasil.org.br/korbilload/upl/editorHTML/uploadDireto/20200758glob-th-editorHTML-00000013-20082020141130.pdf

Em geral, sendo a primeira linha aquela responsável pelo gerenciamento operacional, é ela quem lida com os riscos e com a execução das medidas diariamente. No que se refere à LGPD, é a primeira linha quem deverá **identificar e avaliar os riscos de suas operações diárias de tratamento de dados** e **executar as medidas de segurança** conforme as diretrizes estabelecidas, sendo responsável pela execução dos processos diários e pela implementação dos controles internos, além de garantir que os controles estejam operando conforme planejado para mitigar esses riscos.

Desta forma, é possível dividir as atribuições da 1ª linha de defesa, quando referida à LGPD, em três grupos ou categorias.

O primeiro deles é relativo ao **dirigente máximo** do órgão ou entidade. No exercício do papel de 1ª linha, é do dirigente máximo o dever de designar o Encarregado de Dados, criar o grupo de apoio ao Encarregado, definir processos prioritários a serem mapeados, dar transparência ativa em relação à proteção de dados pessoais, instituir Campanhas institucionais, instituir Política Proteção de Dados Pessoais e instituir Política de Classificação de Informação.

Em relação à LGPD, os **gestores dos processos de negócio** que tratam dados pessoais são os responsáveis, como prepostos dos controladores[2], por manterem o registro das operações de tratamento de dados pessoais que realizarem e devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (art. 37, LGPD).

Quanto à responsabilidade, o controlador – 1ª linha – que causar a outrem dano patrimonial, moral, individual ou coletivo, em razão do exercício de atividade de tratamento de dados pessoais, em violação à legislação de proteção de dados pessoais, será obrigado a repará-lo.

Ainda, caberá à 1ª linha, garantir que os sistemas utilizados para o tratamento de dados pessoais sejam estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na LGPD e às demais normas regulamentares. Esse é o terceiro dos três grupos mencionados acima, ocupado pelo (ou pelos) **gestor da área de tecnologia da informação**.

Destaque-se que, diante de imposição da LGPD, o controlador deve assegurar que qualquer pessoa que intervenha em uma das fases do tratamento estará obrigada a garantir a segurança da informação em relação aos dados pessoais, mesmo após o seu término.

Em entendimento pacificado da ANPD, a LGPD "*atribuiu aos órgãos públicos obrigações típicas de controlador, indicando que, no setor público, essas obrigações devem ser distribuídas entre as principais unidades administrativas*

---

[2] Art. 5º Para os fins desta Lei, considera-se:

...

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais

despersonalizadas que integram a pessoa jurídica de direito público e realizam tratamento de dados pessoais." [3]

É certo, portanto, que o ente público (União, Estado ou Município) será o controlador para fins de LGPD; mas, em face da desconcentração administrativa, o órgão é quem exercerá as vezes de controlador, exercendo, no âmbito de sua estrutura, as atribuições de controlador designada na lei.

Sendo assim, o titular da UCCI, como condutor das ações e decisões no âmbito do órgão público despersonalizado em razão de suas competências legais, assume o papel de garantir o cumprimento da LGPD.

Vale ressaltar que não são controladoras as pessoas naturais que atuam como agentes nos órgãos públicos, sejam titulares ou subordinados. De igual modo, não se trata de operadores (art. 5º, VII, LGPD), que agem em nome do controlador, mas mediante instrumento específico - por exemplo, por força contratual.

O fato de não serem agentes de tratamento, entretanto, não significa que os agentes públicos que eventualmente violem a LGPD não possam ser responsabilizados pela violação. Para além da simples responsabilização administrativa, o Supremo Tribunal Federal já se manifestou no sentido de responsabilizar como improbidade administrativa o ato do servidor que, dolosamente, violar dever de publicidade previsto em dispositivo específico da lei (art. 23, I).[4]

Desta forma, como visto, há vinculação a deveres relativos à LGPD a agentes públicos da primeira linha de defesa, no âmbito dos órgãos em que ocorre o tratamento de dados pessoais. Esta vinculação está prevista em vários artigos da própria lei. De igual modo, há responsabilidade desses agentes no que toca ao cumprimento desses deveres. Nesse sentido, é natural - e recomendável - que o controle se estabeleça, como já defendido, no modelo das três linhas de defesa.

2.2 A 2ª linha: a assessoria : orientação e monitoramento

Segundo o IIA, são papéis de segunda linha:

- Fornecer expertise complementar, apoio, monitoramento e questionamento quanto ao gerenciamento de riscos, incluindo:
    - Desenvolvimento, implantação e melhoria contínua das práticas de gerenciamento de riscos (incluindo controle interno) nos níveis de processo, sistemas e entidades.
    - O atingimento dos objetivos de gerenciamento de riscos, como: conformidade com leis, regulamentos e comportamento ético aceitável; controle interno; segurança da informação e tecnologia; sustentabilidade; e avaliação da qualidade.
- Fornecer análises e reportar sobre a adequação e eficácia do gerenciamento de riscos (incluindo controle interno).

---

[3] ANPD. (2022). Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Retrieved 01 20, 2025, from https://www.gov.br/

[4] ADI 6649; ADPF 695.

Com base nesse entendimento, a proposta ora exposta defende que o plano de implementação da LGPD será acompanhado pela estrutura da 2ª linha, que deverá contar com estrutura de trabalho adequada, prerrogativas e condições necessárias à atuação, a fim de conhecer e avaliar a eficácia dos controles internos da entidade quanto à sua capacidade para evitar ou reduzir o impacto ou a probabilidade da ocorrência de eventos de risco na execução de seus processos e atividades, que possam impedir ou dificultar o alcance de objetivos estabelecidos.

Tendo em vista o fluxo de adequação à LGPD, as atividades necessárias se referem a áreas como compliance, gestão de riscos, transparência e controles internos, cujo papel é monitorar se a organização está se adequando corretamente à lei, além de fornecer suporte e orientação para garantir conformidade.

No que concerne à proteção de dados, internamente, no seu âmbito organizacional, a UCCI deverá garantir que o tratamento de dados esteja ocorrendo da maneira correta, assim como criar estratégias para a identificação dos riscos, prevenção de incidentes, de vazamento de dados e estratégia para resolver e mitigar os riscos quando aparecerem. [5]

Assim, a implementação das ações relativas à adequação à LGPD se caracteriza como uma função de 2ª linha, pois engloba atividades de monitoramento e apoio, sem o envolvimento direto nas operações (1ª linha) nem na auditoria independente (3ª linha).

As estruturas de 2ª linha atuam no monitoramento constante do cumprimento da legislação. Elas devem garantir que as áreas operacionais (1ª linha) estejam implementando as políticas e procedimentos necessários para a proteção de dados pessoais. Ainda, devem fornecer orientação técnica e normativa sobre como as áreas operacionais podem atingir conformidade com a LGPD, estabelecendo controles e frameworks de gestão de riscos de dados.

Em outra frente de ações, também deverão coordenar o desenvolvimento e a implementação de processos de auditoria interna para verificar se os controles da LGPD estão funcionando conforme esperado, reportando o andamento por meio de relatórios de conformidade para a alta gestão.

Um aspecto a ser considerado é a introdução, pela LGPD, da figura do Encarregado como pessoa indicada para atuar como canal de comunicação entre o agente de tratamento (controlador e operador) e os titulares e a autoridade nacional, dispondo sobre suas atribuições, entre as quais destaca-se a orientação aos funcionários e contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais, além de executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Nesse sentido, caberá ao Encarregado aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, receber comunicações da ANPD, mas também poderá ser incumbido de propor à Alta Gestão a Política Interna de Proteção de Dados Pessoais; fornecer termos de uso, manuais de instruções e treinamento, coordenar o mapeamento dos processos de tratamento de dados pessoais realizados no âmbito do órgão ou entidade, inclusive dos compartilhamentos com

[5] IIA. (2020). MODELO DAS TRÊS LINHAS DO IIA 2020. Retrieved novembro, 2024, from https://iiabrasil.org.br/korbilload/upl/editorHTML/uploadDireto/20200758glob-th-editorHTML-00000013-20072020131817.pdf

entidades públicas ou privadas e realizar as ações necessárias para adequação do órgão ou entidade à LGPD, bem como a implantação do Programa de Governança em Privacidade, exigido pela legislação.

Pelo exposto, pode-se observar que o Encarregado tem competências, atribuições e responsabilidades típicas do papel de 2ª linha.

De acordo com o Guia do Framework de Privacidade e Segurança da Informação, publicado pela Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos, a Estrutura Básica de Gestão em Privacidade e Segurança da Informação contempla os seguintes atores:

- Gestor de Tecnologia
- Encarregado
- Gestor de Segurança da Informação
- Responsável pela Unidade de Controle Interno
- Comitê de Segurança da Informação ou estrutura equivalente
- Equipe de Tratamento e Resposta a Incidentes Cibernéticos

Com o intuito de compor uma proposta que possa se adequar aos diversos modelos de governança existentes nas UCCIs, optamos por adotar o entendimento de que essa Estrutura Básica de Gestão em Privacidade e Segurança da Informação será o grupo de apoio ao Encarregado a ser indicado pelo Dirigente Máximo da instituição.

Quanto à composição da Estrutura Básica de Gestão em Privacidade e Segurança da Informação, a presente proposta recomenda que contemple, no mínimo, os seguintes atores:

- Encarregado;
- Responsável pelo Controle Interno;
- Responsável pelo Planejamento;
- Gestor de TI.

Podem fazer parte desta estrutura, representantes de outras áreas como Assessoria jurídica, Ouvidoria ou outras que possam contribuir com o plano de implementação da LGPD.

2.3 A 3ª linha:

A terceira linha desempenha papel importante no que se refere a proporcionar o estímulo e a obediência das normas legais, diretrizes administrativas, instruções normativas, estatutos e regimentos. De maneira análoga, podemos inferir que, no contexto das estruturas de governança em proteção de dados, o Órgão Central de Controle Interno tem o condão de contribuir com o papel de executar atividade de auditoria independente, com vistas à avaliação do grau de maturidade dos controles implementados quando da adequação dos órgãos à Lei Geral de Proteção de Dados.

Como boa prática, sugere-se a inclusão dos riscos à privacidade como objeto de avaliação de controles no bojo da elaboração do Plano de Auditoria, conforme preconiza a metodologia IA-CM (KPA-2.4 - Planos de auditoria baseados em prioridades da gestão e das partes interessadas).

> Objetivo do KPA-2.4 - Desenvolver planos periódicos (anuais ou plurianuais) para os quais serão fornecidas auditorias e/ou outros serviços, baseados em consultas com a gestão e/ou com outras partes interessadas (stakeholders).

Nesta linha de reflexão, entende-se que, para que a execução da atividade de auditoria interna em privacidade e proteção de dados transcorra adequadamente, é indispensável o alinhamento com o Chefe do Poder/Entidade, de modo a consolidar o direito fundamental à privacidade enquanto valor a ser preservado pela administração.

> Atividade Essencial 4 - Por meio de consultas à alta administração e/ou a outras partes interessadas - stakeholders (por exemplo, altos funcionários do governo ou auditores externos), identificar as áreas/temas considerados prioritários a serem abordados pela atividade de auditoria interna.
>
> Fonte: Entendimentos da Câmara Técnica de Auditoria e IA-CM o Conaci sobre os Macroprocessos-chave (KPA) do Nível 2 do Modelo IA-CM (2024)
>
> https://conaci.org.br/wp-content/uploads/2024/12/Entendimentos-Nivel-2-IA-CM-2024.11.07-2.pdf

Com base nesta lógica, pode ser observado o papel da UCCI, com repercussão externa à instituição, relativa à atuação sistemática de auditoria interna com vistas a aumentar e proteger o valor organizacional do Poder, fornecendo avaliação, assessoria e conhecimento objetivos baseados em riscos. E, ainda, atuar na coordenação e orientação acerca da normatização das rotinas e dos procedimentos de controle inerentes aos processos de trabalho, bem como realizar auditorias de avaliação dos controles internos dos sistemas administrativos e dos processos de trabalho do ente, visando promover sua melhoria contínua.

Desse modo, a terceira linha, composta pela auditoria interna, cumprirá seu papel conforme conceito da Instrução Normativa Conjunta **MP/CGU – 2016:**

> *Auditoria interna: atividade independente e objetiva de avaliação e de consultoria, desenhada para adicionar valor e melhorar as operações de uma organização. Ela auxilia a organização a realizar seus objetivos, a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, de controles internos, de integridade e de governança.*

A exemplo do Governo Federal, na terceira linha, atuam a CGU, Auditoria Interna (Audin) e a Secretaria de Controle Interno - Ciset, detalhes sobre atuação dessa linha podem ser observados na IN CGU nº 3, de 2017.

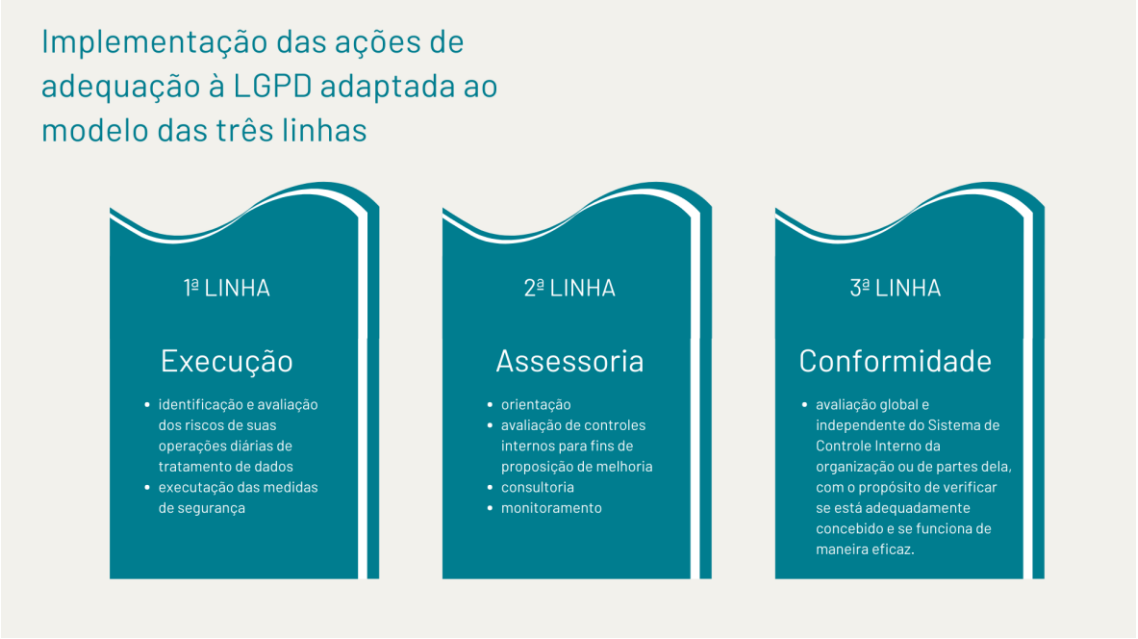
As Unidades de Auditoria Interna Governamental - UAIG devem apoiar os órgãos e as entidades do Poder Executivo Federal na estruturação e efetivo funcionamento da primeira e da segunda linha de defesa da gestão, por meio da prestação de serviços de consultoria e avaliação dos processos de governança, gerenciamento de riscos e controles internos.

Os trabalhos de avaliação dos processos de gestão de riscos e controles pelas UAIG devem contemplar, em especial, os seguintes aspectos: adequação e suficiência dos mecanismos de gestão de riscos e de controles estabelecidos; eficácia da gestão dos principais riscos; e conformidade das atividades executadas em relação à política de gestão de riscos da organização.

Por natureza, os serviços de consultoria representam atividades de assessoria e aconselhamento, realizados a partir da solicitação específica dos gestores públicos. Os serviços de consultoria devem abordar assuntos estratégicos da gestão, como os processos de governança, de gerenciamento de riscos e de controles internos e ser condizentes com os valores, as estratégias e os objetivos da Unidade Auditada. Ao prestar serviços de consultoria, a UAIG não deve assumir qualquer responsabilidade que seja da Administração.

Os resultados da auditoria têm, portanto, como um dos seus objetivos conscientizar os gestores e verificar o nível de preparo e conformidade das organizações públicas em relação às exigências da Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

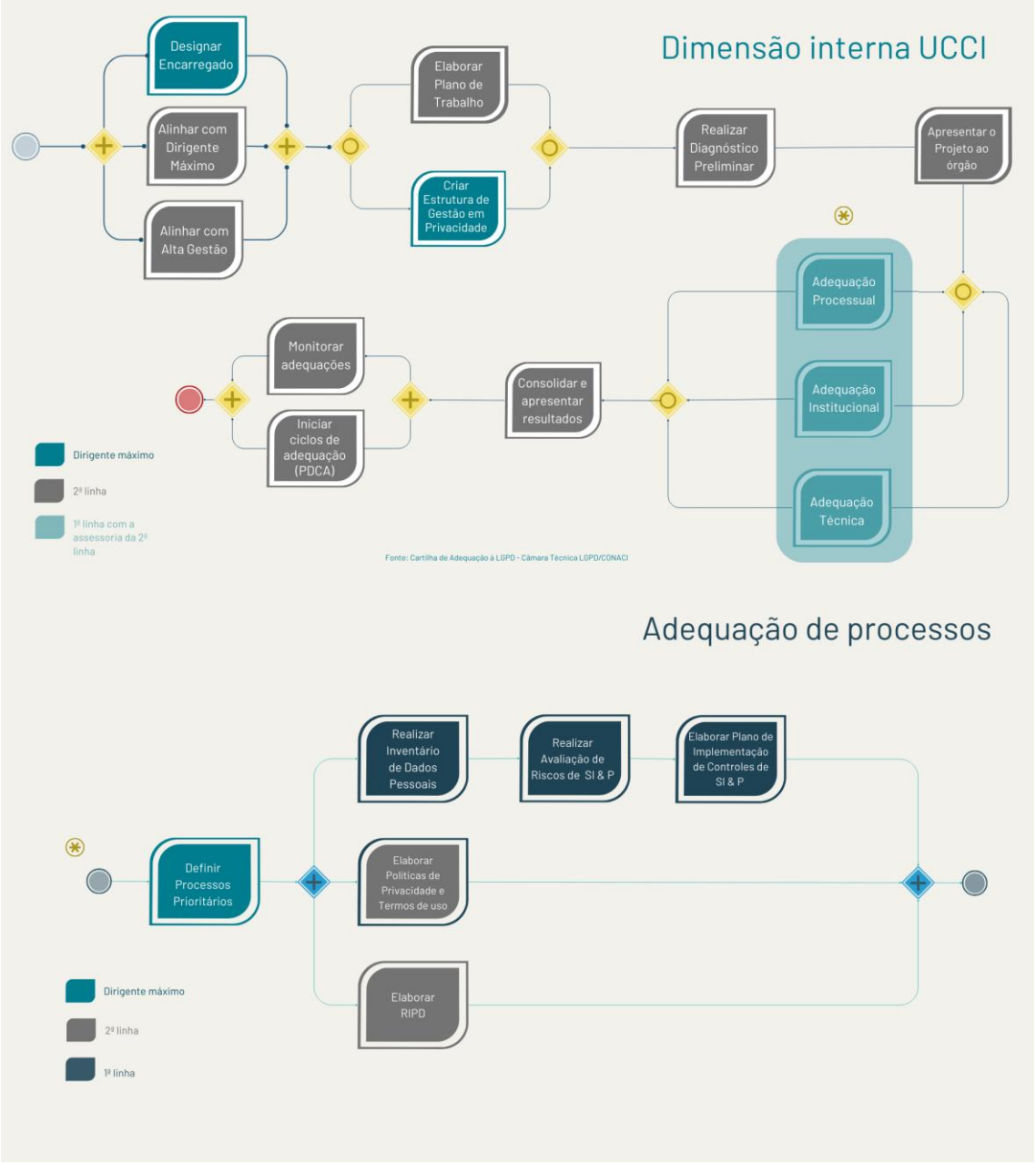
Além de avaliar o processo de implantação da LGPD na Administração Pública, a auditoria tem o potencial de despertar interesse quanto ao tema, produzir conhecimento especificamente voltado à sua implantação no setor público e nortear as atuações dos órgãos para o atingimento da conformidade com a lei.

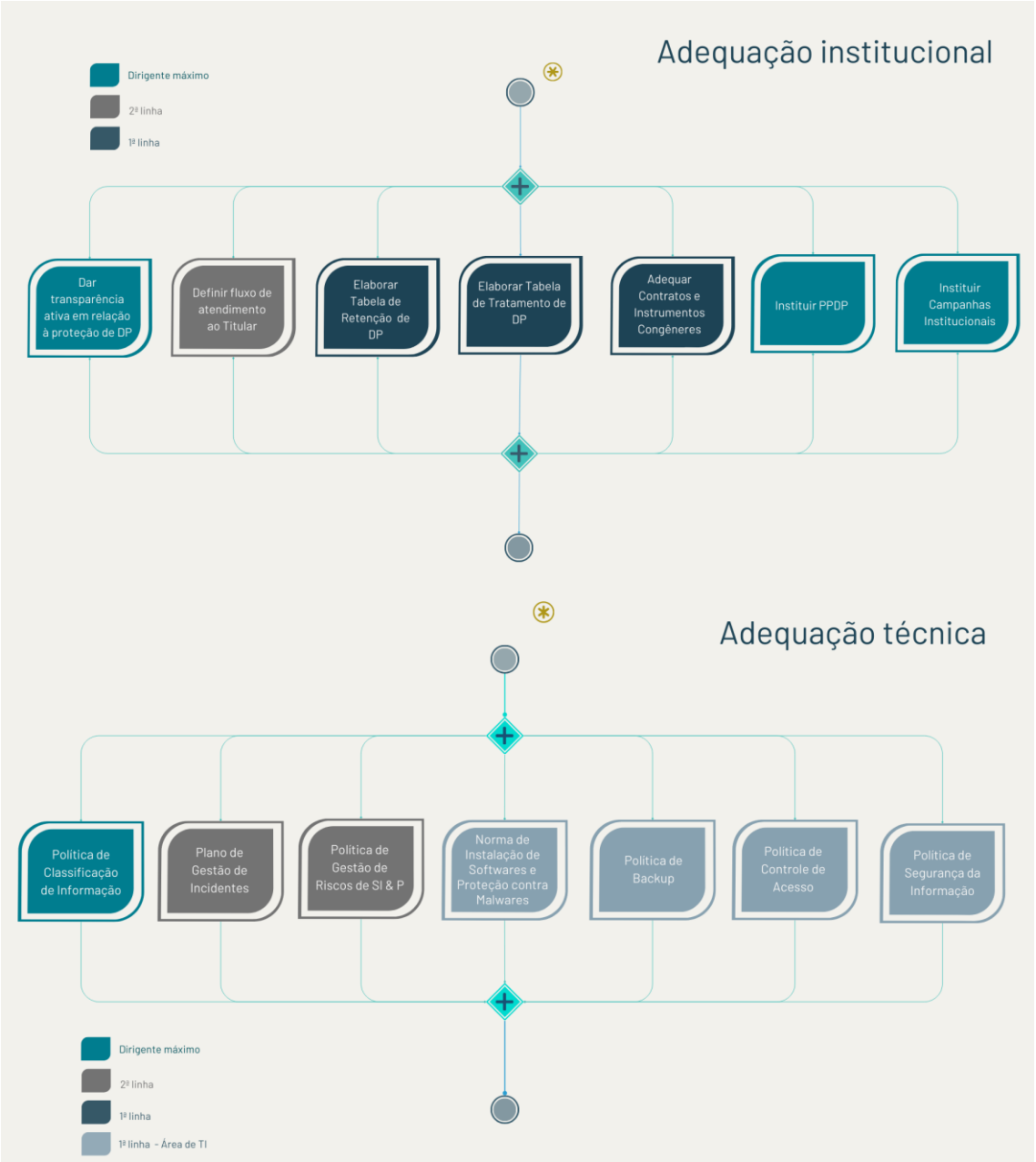


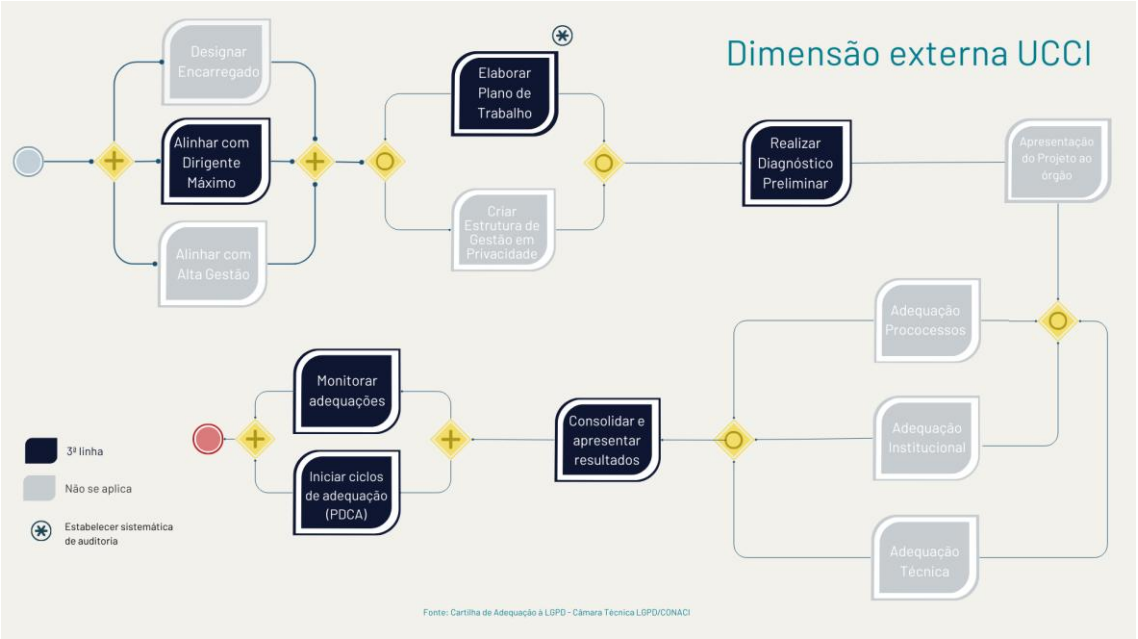
3. CONCLUSÃO

A proposta aqui trazida considera o fluxo de adequação à LGPD, aprovado e divulgado pelo Conaci em junho de 2023, em alinhamento com o recomendado e dirigido aos órgãos e às entidades da Administração Pública Federal.

Deste modo, foi elaborada a seguinte estrutura, buscando ilustrar as etapas de implementação das ações de adequação à LGPD adaptada ao modelo das três linhas:




Adequação institucional
Dirigente máximo
2ª linha
1ª linha
Dar transparência ativa em relação à proteção de DP
Definir fluxo de atendimento ao Titular
Elaborar Tabela de Retenção de DP
Elaborar Tabela de Tratamento de DP
Adequar Contratos e Instrumentos Congêneres
Instituir PPDP
Instituir Campanhas Institucionais
Adequação técnica
Política de Classificação de Informação
Plano de Gestão de Incidentes
Política de Gestão de Riscos de SI & P
Norma de Instalação de Softwares e Proteção contra Malwares
Política de Backup
Política de Controle de Acesso
Política de Segurança da Informação
Dirigente máximo
2ª linha
1ª linha
1ª linha - Área de TI



A seguir, passamos a descrever as atividades atinentes à adequação à LGPD, à luz do modelo das três linhas.

1ª LINHA

UCCI - Dirigente máximo

- Designar o Encarregado de Dados
- Criar Grupo de apoio ao Encarregado
- Definir processos prioritários a serem mapeados
- Dar transparência ativa em relação à proteção de dados pessoais
- Instituir Campanhas institucionais
- Instituir Política Proteção de Dados Pessoais
- Instituir Política de Classificação de Informação

Gestor responsável pelo processo de negócio a ser mapeado:

São responsáveis pelos controles primários, inclusive envolvendo adoção de medidas de privacidade e proteção de dados pessoais, no que se refere à implementação das políticas públicas durante a execução de atividades e tarefas, no âmbito de seus macroprocessos finalísticos e de apoio.

Atividades na implementação da LGPD:

- Realizar Inventário de Dados Pessoais
- Realizar avaliação de riscos à privacidade
- Elaborar Plano de implementação de controles de privacidade
- Elaborar tabela de retenção de dados pessoais
- Elaborar tabela de tratamento de dados pessoais
- Adequar contratos e instrumentos congêneres

Gestor responsável pela área de Tecnologia da Informação

São responsáveis por planejar, implementar, melhorar e otimizar continuamente os processos e procedimentos que envolvem a área de TI e gerenciar as oportunidades de aplicação de tecnologia, interagindo com outras áreas de maneira a assegurar a segurança das informações.

Atividades na implementação da LGPD:

- Elaborar Norma de Instalação de Softwares e Proteção contra Malwares
- Elaborar Política de Backup
- Elaborar Política de Controle de Acesso
- Elaborar Política de Segurança da Informação

2ª LINHA

Estrutura de Gestão em Privacidade

Responsável por estabelecer, manter, monitorar e aprimorar sistemas de gestão de riscos e controles internos com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos que possam impactar a implementação da estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional, quando se tratar de controles de privacidade e segurança da informação.

Composição:

- Encarregado;
- Responsável pelo Controle Interno;
- Responsável pelo Planejamento;
- Gestor de TI.

Atividades na implementação da LGPD:

- Alinhar com Dirigente máximo
- Alinhar com Alta Gestão
- Elaborar Plano de trabalho
- Apresentação do Projeto ao órgão
- Elaborar Relatório de Impacto à Proteção de Dados - RIPD
- Elaborar Políticas de Privacidade e Termos de uso
- Plano de Gestão de Incidentes
- Política de Gestão de Riscos de SI & P
- Consolidar e apresentar resultados
- Iniciar ciclo de adequações (PDCA)
- Monitorar adequações

Encarregado de Dados

Desempenha o papel de fomentar e orientar o planejamento, a implementação e melhoria contínua dos controles de privacidade em serviços ou produtos que realizem o tratamento de dados pessoais.

Atividades na implementação da LGPD:

- Alinhar com Dirigente máximo
- Alinhar com Alta Gestão
- Coordenar a elaboração do Plano de trabalho e conduzir a realização do diagnóstico preliminar
- Definir e implementar o fluxo de atendimento ao Titular
- Monitorar adequações

3ª LINHA

UCCI - Dirigente máximo

Responsável pela atividade de auditoria interna governamental, que presta serviços de avaliação e de consultoria com base nos pressupostos de autonomia técnica e de objetividade.

Atividades na implementação da LGPD:

- Alinhar com Chefe do **Ente/Poder** - consulta à alta administração e/ou a outras partes interessadas
- Apresentar plano de trabalho - estabelecer sistemática de auditoria
- Realizar diagnóstico preliminar
- Consolidar e apresentar resultados
- Implementar ciclo de adequações (PDCA)
- Monitorar adequações
- Compor órgão colegiado do Ente com atribuições sistêmicas, caso exista, a exemplo de:
    - normatização e orientação da rede de encarregados setoriais
    - assessoramento técnico
    - proposição de diretrizes. estratégias políticas, ações e metas
    - apoio técnico na produção de documentos, manuais e capacitações
    - promoção cultural de privacidade e proteção de dados pessoais
    - estabelecimento de padrões para serviços e produtos, inclusive plataformas digitais
    - acompanhamento da implementação da Política Estadual de Proteção de Dados pessoais

REFERÊNCIAS

ANPD. (2022). Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Retrieved 01 20, 2025, from https://www.gov.br/

ATRICON. (n.d.). Diretrizes de Controle Externo ATRICON 3302/2014. https://www.atricon.org.br/wp-content/uploads/2014/08/ANEXOUNICO_RESOLUCAOATRICON_04.pdf

ATRICON. (s.d.). ANEXO ÚNICO DA RESOLUÇÃO ATRICON 05/2014. Fonte: https://www.fapeam.am.gov.br/wp-content/uploads/2023/04/2.-ANEXO-UNICO-RES-N.-05.2014-ATRICON.pdf

ATRICON. (s.d.). Resolução nº04/2014 - Aprova as Diretrizes de Controle Externo Atricon 3302/2014 relacionadas à temática “Controle interno: instrumento de eficiência dos Tribunais de Contas”, integrante do Anexo Único. Fonte: www.atricon.org.br

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Guia de Elaboração de Inventário de Dados Pessoais. Brasília, DF: Ministério da Gestão e da Inovação em Serviços Públicos, 2023. Disponível em: https://www.gov.br/governodigital. Acesso em: 30 jan. 2025.

BRASIL. Ministério da Transparência e Controladoria-Geral da União (CGU). (2017, 06 09). *Instrução Normativa n. 3, de 9 de junho de 2017 [revogada parcialmente]*. Retrieved 02, 2025, from https://repositorio.cgu.gov.br/bitstream/1/33409/19/Instrucao_Normativa_CGU_3_2017.pdf

GUIA DO FRAMEWORK DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO. (2024, dezembro). Retrieved janeiro 23, 2025, from https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf

IIA. (2020). MODELO DAS TRÊS LINHAS DO IIA 2020. Retrieved novembro, 2024, from https://iiabrasil.org.br/korbilload/upl/editorHTML/uploadDireto/20200758glob-th-editorHTML-00000013-20072020131817.pdf

Ministério da Transparência e Controladoria-Geral da União. (2017). Repositório de Conhecimento da CGU. Retrieved January 23, 2025, from https://repositorio.cgu.gov.br/bitstream/1/33409/19/Instrucao_Normativa_CGU_3_2017.pdf