UNIVERSIDADE FEDERAL DE MINAS GERAIS
FACULDADE DE DIREITO
Bacharelado em Ciências do Estado

Pedro Henrique do Carmo Pires

O planejamento e o uso de *compliance* na aplicação da Lei Geral de Proteção de Dados na Diretoria Central de Administração de Pessoal da prefeitura de Belo Horizonte

Belo Horizonte
2024

Pedro Henrique do Carmo Pires

O planejamento e o uso de *compliance* na aplicação da Lei Geral de Proteção de Dados na Diretoria Central de Administração de Pessoal da prefeitura de Belo Horizonte

Trabalho de conclusão de curso apresentado ao curso de Ciências do Estado da Universidade Federal de Minas Gerais, orientado pelo professor Rodrigo Almeida Magalhães como requisito parcial para obtenção do título de bacharel em Ciências do Estado.

Orientador: Rodrigo Almeida Magalhães

Belo Horizonte

2024

AGRADECIMENTOS

Gostaria de agradecer primeiramente a Deus, a todas as entidades e aos meus guias que me protegem e me acompanharam durante minha jornada acadêmica. Este grande ciclo da minha vida não teria sido o mesmo sem esse apoio espiritual que me socorreu e confortou nos momentos de aflição, trazendo paz e me ajudando a superar os desafios encontrados para continuar firme.

Aos meus pais, Lícia Silva do Carmo Pires e Rodrigo Alves Pires, que me possibilitaram realizar meus sonhos e me guiaram durante esses anos longe de casa, trazendo conforto e conselhos nos momentos de dificuldade e incerteza, relembrando-me dos objetivos que me trouxeram até este momento.

Aos meus amigos de longa data: Ana Carolina Vasque, Arthur Moreira, Bruno Luiz Moraes, Erika Coelho, Felipe Silva, Fernando Caetano, Gustavo Gonzaga, Kaio Macedo, Leonardo Henrique, Livian Amaral, Marcelo Caetano e Rodrigo Luiz Moraes. Vocês me acompanharam durante a adolescência e me acolheram e alegraram todas as vezes que regressei à casa dos meus pais. Sem vocês, não teria sido possível me reconectar com minhas origens e lembrar de onde vim; sem vocês, eu jamais teria chegado à Universidade Federal de Minas Gerais.

Agradeço a todas as pessoas que conheci na universidade, especialmente àquelas com quem tive contato durante meus anos no Centro Acadêmico de Ciências do Estado e nos momentos de desafogo no Território Livre José Carlos Mata Machado, da Faculdade de Direito e Ciências do Estado. Vocês marcaram positivamente minha curta passagem por este espaço, que me ensinou muito sobre a vida e contribuíram para minha transformação e evolução como pessoa, mesmo que por um curto período de tempo.

Agradeço a todos os meus amigos mais próximos que fiz nestes últimos anos, graças à universidade, e que estiveram ao meu lado trilhando seus caminhos durante essa trajetória de curso: Ana Luiza Reis, Davi Santos, Larissa Castro, Laura Brandão, Lucas Chelala e Paula Aguiar. Sem vocês, eu não teria conseguido suportar esses quase cinco anos longe de casa e das minhas origens. Com vocês, eu me sinto em casa e em família. Obrigado por todos esses anos de amizade e reciprocidade.

Agradeço também a todas as pessoas que conheci em Belo Horizonte, seja nas repúblicas em que morei, nos empregos em que trabalhei ou por pura coincidência da vida e do universo. Cada um de vocês me ofereceu um sorriso ou me desafiou a experienciar a vida adulta da melhor maneira.

Agradeço a Lara Domingos Narde por todas as vezes que me acolheu, me escutou e me proporcionou momentos incríveis nesta cidade. Acho surreal ter encontrado alguém tão parecido comigo a quilômetros de casa; nunca esperaria que aquela nossa primeira conversa no dia 3 de março de 2020, durante o acolhimento de calouros, pudesse se transformar em uma amizade tão sólida, saudável e verdadeira. Você foi minha parceira em todas as ocasiões, nos momentos de felicidade e tristeza, de euforia e ansiedade. Você sempre esteve ao meu lado, compartilhando cada momento e cada sentimento. Foram muitas as discussões que tivemos que enfrentar para fortalecer nossa amizade, transparência e sinceridade. Confio em você mais do que confio em mim mesmo e agradeço por ser tão verdadeira comigo e por me apoiar nos meus planos mais malucos. Te amo, amiga. Espero ter você sempre ao meu lado.

E, por fim, agradeço a Marcos Vinícius Fernandes da Costa. Nunca imaginei que poderia ter feito uma amizade tão forte e profunda em tão pouco tempo. Sou muito agradecido por ter te conhecido e quero poder levar você comigo até o fim da minha vida. Em você, encontrei muito mais que um amigo, encontrei um irmão, que sempre esteve ao meu lado, me arrancando sorrisos nos momentos mais difíceis e que nunca me abandonou ou duvidou de mim. Espero poder retribuir em dobro, ainda nesta vida, tudo o que você me proporcionou nesses anos de parceria e amizade. Te amo, amigo. Deixo aqui minha eterna gratidão e admiração.

RESUMO

Este estudo investiga a implementação de práticas de Governança, Riscos e *Compliance* (GRC) na Diretoria Central de Administração de Pessoal (DCAP) da Prefeitura de Belo Horizonte, com um foco especial na adaptação às exigências da Lei Geral de Proteção de Dados (LGPD). A pesquisa enfatiza a importância do *compliance*, entendido como um conjunto de processos e práticas destinados a assegurar que uma organização esteja em conformidade com leis, regulamentos e normas aplicáveis. O estudo trata também da evolução do conceito de GRC no Brasil e o papel da LGPD nesse contexto, destacando a crescente necessidade de proteção de dados pessoais em um ambiente altamente digitalizado. A metodologia do estudo inclui entrevistas estruturadas, visando avaliar a maturidade das práticas de GRC na DCAP e compreender como essas práticas são integradas ao planejamento estratégico e às operações cotidianas da prefeitura. Os resultados indicam que a implementação do *compliance* digital é fundamental para a administração pública, não apenas para proteger os dados dos cidadãos, mas também para promover maior transparência e responsabilidade no setor público.

Palavras-chave: privacidade, *compliance*, LGPD, administração pública.

ABSTRACT

This study investigates the implementation of Governance, Risk, and Compliance (GRC) practices in the Central Directorate of Personnel Administration (DCAP) of the Belo Horizonte City Hall, with a particular focus on adapting to the requirements of the General Data Protection Law (LGPD). The research emphasizes the importance of compliance, understood as a set of processes and practices designed to ensure that an organization adheres to applicable laws, regulations, and standards. The study also addresses the evolution of the GRC concept in Brazil and the role of the LGPD within this context, highlighting the growing need for personal data protection in an increasingly digitalized environment. The study's methodology includes structured interviews aimed at assessing the maturity of GRC practices within the DCAP and understanding how these practices are integrated into the strategic planning and daily operations of the city administration. The findings indicate that the implementation of digital compliance is crucial for public administration, not only to protect citizens' data but also to promote greater transparency and accountability in the public sector.

Keywords: privacy, compliance, LGPD, public administration.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados.
AS	*Australian Standard.*
ASPE	Assessoria de Projetos Especiais
BBC	*British Broadcasting Corporation*.
CADE	Conselho Administrativo de Defesa Econômica.
CE	Conselho Europeu.
CGU	Controladoria-Geral da União.
DCAP	Diretoria Central de Administração de Pessoal.
FCPA	*Foreign Corrupt Practices Act.*
GECEA	Gerência Central de Atendimento.
GESFO	Gerência de Gestão da Folha de Pagamento.
GETED	Gerência de Gestão de Direitos e Benefícios.
GEVIF	Gerência de Gestão de Ingresso e da Vida Funcional.
GRC	Governança, Risco e *Compliance.*
GT	Grupo de Trabalho
IBGC	Instituto Brasileiro de Governança Corporativa.
ISO	*International Organization for Standardization.*
LGPD	Lei Geral de Proteção de Dados.
MCI	Marco Civil da Internet.
MIT	Instituto de Tecnologia de Massachusetts.
MJ	Ministério da Justiça.
OEA	Organização dos Estados Americanos.
OCDE	Organização para a Cooperação Econômica e Desenvolvimento.
ONU	Organização das Nações Unidas.
PDCA	*Plan, Do, Check, Act.*
PBH	Prefeitura de Belo Horizonte.
RGPD	Regulamento Geral sobre a Proteção de Dados.
SGRC	Solução de Governança, Riscos e *Compliance.*
SMPOG	Secretaria Municipal de Planejamento, Orçamento e Gestão.
SUGESP	Subsecretaria de Gestão de Pessoas.
UE	União Europeia.

SUMÁRIO

1 INTRODUÇÃO

A crescente complexidade dos ambientes organizacionais, aliada à intensificação das regulamentações legais, tem demandado das instituições públicas e privadas a adoção de práticas robustas de Governança, Risco e *Compliance* (GRC). Nesse contexto, a Lei Geral de Proteção de Dados (LGPD) emergiu como uma regulamentação essencial para a proteção dos dados pessoais no Brasil, impondo novos desafios e exigências às organizações. A aplicação eficaz da LGPD é particularmente crítica na administração pública, onde a gestão de dados pessoais se torna um aspecto central para garantir a transparência, a integridade e a confiança dos cidadãos.

Este trabalho investiga o planejamento e o uso de *compliance* na Diretoria Central de Administração de Pessoal (DCAP) da Prefeitura de Belo Horizonte (PBH), com foco na implementação das diretrizes da LGPD. A DCAP, uma das principais unidades administrativas da PBH, lida diariamente com um grande volume de dados pessoais dos servidores públicos, o que torna essencial a adoção de práticas de *compliance* alinhadas às exigências legais. A pesquisa parte do pressuposto de que a integração de modelos de GRC e a conformidade com a LGPD não apenas garantem a proteção dos dados pessoais, mas também promovem uma cultura organizacional de responsabilidade e transparência. Assim, este estudo busca avaliar como a DCAP tem estruturado suas políticas de *compliance* e se estas estão alinhadas às melhores práticas recomendadas pela LGPD, bem como identificar os principais desafios e oportunidades enfrentados na implementação dessas políticas. A metodologia adotada inclui a realização de entrevistas e a análise documental, permitindo uma compreensão aprofundada das práticas de GRC na DCAP e suas implicações para a administração pública.

O trabalho está estruturado em cinco capítulos. O capítulo dois apresenta os fundamentos teóricos das práticas de GRC, estabelecendo a base conceitual necessária para a compreensão dos temas abordados. No capítulo três, é discutida a evolução da proteção de dados, tanto no Brasil quanto no contexto global, incluindo um resumo detalhado da LGPD e sua relação com as práticas de GRC. No capítulo quatro, estão as entrevistas e é analisada a aplicação das práticas de *compliance* digital na DCAP. E o capítulo cinco apresenta as conclusões do estudo, revisitando os principais temas discutidos ao longo do trabalho e avaliando o planejamento da DCAP em relação à conformidade com a LGPD, oferecendo uma reflexão crítica sobre os resultados obtidos.

2 CONCEITO DE GOVERNANÇA, RISCOS E *COMPLIANCE* (GRC)

Com a crescente complexidade do mundo, diversos temas relacionados à noção de Governança, Risco e *Compliance* (GRC) surgiram durante o século XX. Os primeiros conselhos e comissões que iniciaram a discussão e começaram a conceituar o modelo atual do que conhecemos surgiram no início dos anos 2000, quando os primeiros códigos e práticas começaram a se disseminar pelo mundo. Devido a gama de profissionais que discorrem sobre os temas que competem o GRC, desde o jurídico ao administrativo-econômico, muitas definições e práticas se expandem e se tornam cada vez mais completas e diversas, convertendo-se em conceitos multidisciplinares que abrangem diversas áreas e amadurecem as práticas, permitindo sua usabilidade dentro e fora do mundo corporativo.

2.1 Fundamentos de GRC

O GRC entrepassa principalmente entre a governança corporativa, a gestão de riscos e o *compliance*, desenvolvendo esses três pilares a fim de garantir a eficácia e as boas práticas administrativas.

A governança corporativa segundo o Instituto Brasileiro de Governança Corporativa (2023, p. 17) "[...] é um sistema formado por princípios, regras, estruturas e processos pelo qual as organizações são dirigidas e monitoradas, com vistas à geração de valor sustentável para a organização, para seus sócios e para a sociedade em geral". Em essência, é um conjunto administrativo de práticas e processos que diversos agentes assumem com o objetivo de otimizar resultados, definir estratégias e orientar operações por meio de tomadas de decisões e definição de regras que satisfaçam os interesses dos *stakeholders*, garantindo responsabilidade e transparência na organização.

Inicialmente, os *stakeholders* eram entendidos apenas como os investidores e acionistas das empresas, entretanto, com a crescente responsabilização social e com a amplitude dos conceitos de governança corporativa, além do terceiro setor e do setor público também começaram a utilizar das práticas e códigos, houve a compreensão de que os *stakeholders* são também toda a sociedade impactada pelas atividades e aos possíveis impactos ambientais que podem ser gerados pelas atividades da organização. Sendo assim:

> "As boas práticas de governança corporativa convertem princípios básicos em recomendações objetivas, alinhando os interesses com a finalidade de preservar e otimizar o valor econômico de longo prazo da organização, facilitando seu acesso a

> recursos e contribuindo para a qualidade da gestão da organização, sua longevidade e o bem comum." (IBGC, 2015 *apud* ALMEIDA, 2024, p. 8)

. Um avanço significativo destacado pelo Instituto Brasileiro de Governança Corporativa (IBGC) no tema nos últimos anos é a evolução da governança corporativa para um enfoque mais abrangente, que não visa apenas à otimização do valor econômico exclusivamente para os sócios, mas à geração de valor compartilhado entre os sócios e as demais partes interessadas. Essa nova perspectiva reconhece a interdependência entre as organizações e as realidades econômica, social e ambiental em que elas estão inseridas, demonstrando a evolução da governança para um modelo mais sustentável.

Segundo o IBGC, a governança corporativa é fundamentada em cinco princípios essenciais que orientam a gestão das organizações, promovendo a responsabilidade, a transparência e a sustentabilidade.

A integridade é o primeiro princípio, ele envolve a prática e a promoção contínua de uma cultura ética dentro da organização. Inclui evitar decisões influenciadas por conflitos de interesses, manter a coerência entre o discurso e a ação, e preservar a lealdade à organização e o cuidado com todas as partes interessadas, a sociedade em geral e o meio ambiente.

A transparência consiste em disponibilizar informações verdadeiras, tempestivas, coerentes, claras e relevantes para as partes interessadas, sejam elas positivas ou negativas, e não apenas aquelas exigidas por leis ou regulamentos. A transparência deve abranger não apenas o desempenho econômico-financeiro, mas também os fatores ambientais, sociais e de governança, promovendo um ambiente de confiança e desenvolvimento dos negócios.

A equidade implica tratar todos os sócios e demais partes interessadas de maneira justa, levando em consideração seus direitos, deveres, necessidades, interesses e expectativas, tanto individualmente quanto coletivamente. A equidade pressupõe uma abordagem diferenciada conforme as relações e demandas de cada parte interessada com a organização, motivada pelo senso de justiça, respeito, diversidade, inclusão, pluralismo e igualdade de direitos e oportunidades.

A responsabilização (*accountability*) envolve desempenhar funções com diligência, independência e visando à geração de valor sustentável no longo prazo, assumindo a responsabilidade pelas consequências dos atos e omissões. Isso inclui prestar contas de maneira clara, concisa, compreensível e tempestiva, cientes de que suas decisões podem impactar tanto a organização quanto as partes interessadas e o meio ambiente.

E por fim, a sustentabilidade refere-se a zelar pela viabilidade econômico-financeira da organização, reduzindo as externalidades negativas e aumentando as positivas,

considerando os diversos capitais (financeiro, manufaturado, intelectual, humano, social, natural e reputacional) no curto, médio e longo prazo. Compreende que as organizações atuam em uma relação de interdependência com os ecossistemas social, econômico e ambiental, fortalecendo seu protagonismo e suas responsabilidades perante a sociedade.

A aplicação destes princípios não só contribui para a longevidade e sucesso das organizações, mas também para o bem-estar das partes interessadas e da sociedade em geral. A noção de valor compartilhado em conjunto com os princípios, sugere que as empresas não devem focar apenas em maximizar lucros, mas também em contribuir para o bem-estar das comunidades e do ambiente em que operam. Ao integrar objetivos sociais e econômicos, as empresas podem criar um ciclo virtuoso onde o sucesso empresarial impulsiona melhorias sociais e estas, por sua vez, reforçam a competitividade da empresa. Essa abordagem destaca a importância da sustentabilidade e da responsabilidade social corporativa, reconhecendo que o progresso econômico e social são interdependentes e que um desenvolvimento sustentável só é possível quando ambos são promovidos simultaneamente.

Além de estabelecer práticas transparentes, responsáveis e sustentáveis, a governança corporativa serve como alicerce para a gestão de riscos, que por sua vez, serve para identificar, avaliar e mitigar potenciais ameaças aos objetivos estratégicos traçados pela organização. Segundo Neves et al. (2024), os riscos são variáveis capazes de serem identificados, permitindo calcular a ocorrência. Essa afirmação é importante para saber fazer a diferenciação de um risco e de uma incerteza, visto que estas palavras são comumente tratadas como sinônimos.

A gestão de riscos então se entrelaça com a governança corporativa ao assegurar que os riscos sejam identificados nas etapas de planejamento dos projetos e gerenciados de acordo com as diretrizes e políticas estabelecidas, contribuindo para a sustentabilidade e resiliência da empresa. Dentre os riscos que uma empresa pode sofrer, existem alguns casos em que decisões do macroambiente político-legal, ou seja decisões legislativas e governamentais, afetam diretamente a forma que os projetos e processos da empresa devem ser geridos, estas normas podem trazer um impacto significativo para o mercado, sendo necessária uma preocupação ainda maior após a promulgação da lei por parte da governança corporativa.

Diante disto, a multidisciplinaridade entre a ciência administrativa e o direito se instaurou para formalizar os processos da gestão de riscos, criando as normas de *compliance*. Esta expressão corporativa pode ser entendida como:

> "[...] um sistema complexo e organizado de procedimentos de controle de riscos e preservação de valores intangíveis [...].
>
> Esse sistema interno também pode ser chamado de programa de integridade ou programa de *compliance*, com a finalidade de prevenir, detectar e corrigir atos não condizentes com os princípios e valores da empresa, assim como perante o ordenamento jurídico vigente. " (BERTOCCELLI, 2024, p. 38 e 39)

O sistema de *compliance* assim surge, diferentemente de código e práticas, como um programa específico e exclusivo que elabora regras e realiza treinamentos de forma constante, se desenvolvendo continuamente conforme os processos internos são otimizados. Conforme diz Bertoccelli (2024), este programa é realizado principalmente em três fases que funcionam de forma circular, sendo estas fases o estabelecimento, a incorporação à cultura organizacional e a aplicação. A partir disto podemos entender que um programa de *compliance* não pode apenas ser comprado, sendo necessária a incorporação nos valores da organização a partir de uma equipe/pessoa específica para a gestão do processo dependendo das necessidades e complexidades que a instituição entende ser de alto grau de risco.

2.2 O surgimento do *compliance* no Brasil

Até pouco tempo atrás, o termo *"compliance"* era pouco utilizado em terras tupiniquins, sendo estritamente restrito apenas aos ambientes de grandes corporações de setores altamente regulados, como os financeiros, e em multinacionais, que são em sua maioria, de origem estadunidense. Isso se deve ao fato que os primeiros registros da utilização do termo surgiram após a legislação estadunidense de anticorrupção internacional, a *Foreign Corrupt Practices Act* (FCPA), de 1977, que tinha como propósito combater o oferecimento de propinas a funcionários públicos estrangeiros. Esta legislação cumpria o objetivo de punir as empresas corruptas que praticavam este ato para receber vantagens em mercados de outros países. A partir do fim do século XX e início do século XXI, houve uma grande pressão de órgãos internacionais para tratar sobre o tema de corrupção, incluindo a Convenção Interamericana contra a Corrupção, aprovada no âmbito da Organização dos Estados Americanos (OEA) em 1996, a Convenção sobre o Combate da Corrupção de Funcionários Públicos Estrangeiros em Transações Comerciais Internacionais, aprovada no âmbito da Organização para a Cooperação Econômica e Desenvolvimento (OCDE) em 1997, a Convenção das Nações Unidas contra a Corrupção, aprovada no âmbito da Organização das Nações Unidas (ONU) em 2003, dentre outras. As convenções citadas foram ratificadas no

Brasil durante os primeiros anos do século XXI e começaram a gerar esforços jurídicos para a criação e implementação de leis de anticorrupção no Brasil e no mundo.

Então, em 2013, o Brasil aprovou a Lei nº12.846/2013, conhecida como "Lei da Empresa Limpa", que atendia aos compromissos assumidos nas convenções internacionais, e a partir deste momento, deu ao programa de *compliance* destaque, sendo sua existência dentro das organizações essencial para amenizar sanções em caso de infração da legislação, conforme diz o Art. 7º, inciso VII:

> "Serão levados em consideração na aplicação das sanções: a existência de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e a aplicação efetiva de códigos de ética e de conduta no âmbito da pessoa jurídica;" (BRASIL, 2013)

A aprovação da Lei da Empresa Limpa impulsionou as organizações brasileiras a implementarem programas de *compliance* robustos, visando não apenas o cumprimento das normativas legais, mas também a criação de uma cultura ética dentro das empresas. O programa de *compliance*, portanto, passou a ser visto não somente como uma obrigação legal, mas como uma ferramenta estratégica para a sustentabilidade e reputação das empresas no mercado.

Além disso, a disseminação da cultura de *compliance* no Brasil foi acompanhada pelo fortalecimento das atividades de fiscalização e aplicação das leis por parte dos órgãos reguladores, como o Ministério da Transparência e Controladoria-Geral da União (CGU) e o Conselho Administrativo de Defesa Econômica (CADE). Esses órgãos têm atuado de forma rigorosa para assegurar que as empresas cumpram as regulamentações e adotem práticas de integridade.

2.3 Princípios e normas gerais do *compliance*

Em 2006, a *Australian Standard*, um órgão não governamental de desenvolvimento de padrões na Austrália, foi pioneira no mundo em determinar os princípios de um programa de *compliance*. A AS 3806:2006, em seu manual, dispõe de quatro fases: comprometimento; implementação; monitoramento e medição; melhoria contínua. Estas quatro fases juntas se transformam doze princípios, ligados pela seguinte ordem: (I) Existe comprometimento por parte do corpo diretivo e da alta direção com o *compliance* eficaz, que permeia toda a organização; (II) A política de *compliance* está alinhada à estratégia e aos objetivos de negócio da organização e recebe o endosso do corpo diretivo; (III) São alocados os recursos

apropriados para desenvolver, implementar, manter e melhorar o programa de *compliance*; (IV) Os objetivos e a estratégia do programa de c*ompliance* são endossados pelo corpo diretivo e pela alta direção; (V) As obrigações de *compliance* são identificadas e avaliadas; (VI) A responsabilidade por resultados conformes é articulada e atribuída claramente; (VII) As competências e as necessidades de treinamento são identificadas e levadas em consideração, a fim de permitir que os funcionários cumpram com suas obrigações de *compliance*; (VIII) Comportamentos que criam e sustentam o *compliance* são estimulados, e comportamentos que comprometem o *compliance* não são tolerados; (IX) Existem controles para gerenciar as obrigações de *compliance* identificadas e para alcançar os comportamentos desejados; (X) O desempenho do programa de *compliance* é monitorado, mensurado e relatado; (XI) A organização é capaz de demonstrar seu programa de *compliance*, tanto através de documentação quanto da prática; (XII) O programa de *compliance* é analisado criticamente com regularidade e melhorado continuamente.

A partir disto quatro anos depois, em 2010, quando a lei *Bribery Act* do Reino Unido foi aprovada, a legislação de anticorrupção do país conseguiu construir "[...] um novo paradigma, não apenas no âmbito dos países que o compõem (Inglaterra, País de Gales, Escócia e Irlanda do Norte), mas mundial, no tratamento da corrupção" (BERTOCCELLI, 2024, p. 43). Essa lei, em seu teor, mesmo que se trate de um programa *compliance* de anticorrupção, conseguiu sintetizar a norma australiana e formar seis princípios fundamentais, que são utilizados nos programas de *compliance* mais modernos em todo o mundo e se tornou referência para a implantação dos diversos tipos de *compliance* entendidos até hoje. Seus princípios são: (I) Proporcionalidade dos procedimentos de acordo com os riscos, as circunstâncias e a complexidade dos negócios, devendo os mesmos serem claros e acessíveis a todos os colaboradores e fornecedores da empresa; (II) Comprometimento concreto da alta administração da empresa; (III) Avaliação de riscos de forma periódica e documentada; (IV) Procedimentos constantes de *due diligence* com a finalidade de mitigar riscos relacionados à corrupção; (V) Comunicação interna e externa, incluindo treinamentos, a fim de orientar colaboradores e fornecedores sobre riscos e *compliance*; (VI) Monitoramento e revisão periódica do programa de *compliance*.

Com a adaptação britânica da norma australiana para a lei de anticorrupção, que veio a se tornar referência no padrão dos programas de *compliance*, em 2014, a Organização Internacional para Padronização cria a ISO 19600:2014, que estabelece e sintetiza em nove princípios: (I) Suporte da alta administração; (II) Avaliação de riscos, necessidades e expectativas dos *stakeholders*; (III) Determinação do código de conduta e da política de

compliance; (IV) Papéis, responsabilidades e autoridades na organização do programa; (V) Treinamentos e comunicação; (VI) Canais de denúncias; (VII) Investigações internas; (VIII) *Due diligence*; (IX) Monitoramento, auditoria e revisão do programa de *compliance*.

Diante disto, com a simplificação e destrinchamento do modelo de uma forma mais geral, a ISO 19600:2014 começou a servir como base para outros modelos mais específicos de *compliance*.

2.4 A usabilidade do GRC

Com normas cada vez mais detalhadas e complexas, o mercado de gestão e administração começou a se especializar e desenvolver modelos e métodos para ajudar gestores a implementar e garantir melhores resultados em seus negócios, além de cumprir os regulamentos governamentais que impactam diretamente suas operações. Os princípios do GRC se conectam a modelos já conhecidos, como o PDCA (*Plan, Do, Check, Act*), e integram várias normas específicas em um modelo de solução abrangente. As normas de *compliance*, já mencionadas anteriormente, assumem um novo papel dentro do sofisticado modelo de solução GRC, desempenhando uma função mais processual e servindo como base para o modelo.

O modelo de solução GRC, que chamaremos a partir de agora de SGRC (Solução de Governança, Riscos e *Compliance*), contém diversos esquemas, a depender da empresa que aplica o modelo, mudando apenas o nome dado a cada etapa do processo do seu modelo de SGRC. A fim de facilitar o entendimento, utilizaremos o modelo da empresa Interact Solutions, do Rio Grande do Sul, para exemplificar a utilização das normas dentro do SGRC.

Todo modelo de SGRC, tem como base uma abordagem circular, onde os elementos se retroalimentam, fazendo com que cada etapa influencie a próxima e permita uma constante revisão e refinamento do processo como um todo, garantindo melhorias constantes com base nos resultados obtidos. Este tipo de metodologia tem como base o método PDCA, que surgiu em 1939 como o Ciclo de Shewhart, foi refinado em 1950 para se tornar o Ciclo de Deming e aperfeiçoado através dos trabalhos de Armand Feigenbaum, Kaoru Ishikawa e Yoji Akao no Ciclo Japonês, conhecido como o método *Plan-Do-Check-Act*. A SGRC adota o seguinte modelo (Figura 1).

Figura 1 - Esquema de solução em GRC

Fonte: Interact Solutions (2024)

2.4.1 A relação entre o modelo de SGRC e o PDCA

O modelo apresentado contém duas características principais, a primeira é a adaptação do método PDCA no método que consiste nas seguintes abordagens circulares: (I) Gestão do Planejamento; (II) Gestão dos Documentos; (III) Gestão das Auditorias; (IV) Gestão das Ocorrências. E (I) Mapeamento de Processos; (II) Identificação de Riscos; (III) Prática de Controle; (IV) Ações de Melhoria.

Essas duas abordagens circulares utilizam das premissas básicas do PDCA, sendo as todas as fases, releituras das fases de planejamento, execução, controle e atuação do PDCA:

As fases I de gestão do planejamento e mapeamento de processos, ambas referenciam a etapa de planejamento, que consiste em definir claramente os objetivos e os processos necessários para alcançar esses objetivos.

As fases II de gestão dos documentos e identificação dos riscos, estão diretamente ligadas à etapa de execução, que consiste na execução do plano de ação desenvolvido na fase de planejamento. Essa etapa consiste principalmente na documentação e registro de todas as atividades e quaisquer problemas ou desvios encontrados durante a execução.

As fases III de gestão das auditorias e prática de controle, estão diretamente ligadas à etapa de controle, que envolve a avaliação e o monitoramento dos resultados obtidos na etapa de execução.

E por fim, as fases IV de gestão de ocorrências e ações de melhoria, estão diretamente ligadas à fase de atuação, que consiste em tomar ações baseadas nas conclusões da fase de controle para garantir a melhoria contínua.

2.4.2 A relação entre o modelo SGRC e a ISO 19600:2014

A segunda parte do modelo SGRC sintetiza os nove princípios da ISO 19600, mantendo a estrutura original e apenas reformulando a redação dos pontos, sem alterar a ordem ou introduzir novos conceitos. Quando lido de forma completa, o esquema nos revela claramente três chaves para entender como funciona um processo de SGRC e, consequentemente, de *compliance*: Conformidade, Sistema de Gestão de *Compliance*, e Riscos de *Compliance*.

Essas chaves estão diretamente ligadas ao cumprimento de leis, regulamentos, normas, códigos de prática e padrões internos e externos aplicáveis à organização. Elas destacam a importância de compreender o contexto da organização e as necessidades das partes interessadas, bem como o comprometimento da alta liderança na formalização e cumprimento de um conjunto estruturado de políticas, procedimentos, processos e controles.

O modelo inclui planejamento, definição de objetivos, conscientização, comunicação, monitoramento, medição, análise e avaliação para verificar a conformidade com a norma e a eficácia do sistema. Ele também estabelece processos para tratar não conformidades e implementar ações corretivas, buscando continuamente maneiras de melhorar a gestão e o sistema de *compliance*.

3 LEGISLAÇÕES DE PROTEÇÃO DE DADOS E *COMPLIANCE DIGITAL*

Em tempos de mídias digitais, *fake news*, inteligência artificial, invasão de dispositivos informáticos e super coleta dos dados pessoais, o direito viu a necessidade de adequação ao "mundo" digital que estava cada vez mais presente na vida cotidiana. A lei 12.965/14, amplamente conhecida como o Marco Civil da Internet (MCI), surge assim como o primeiro esforço regulatório para garantir que a internet seja um ambiente seguro, plural, democrático e diverso, além de garantir os direitos e deveres fundamentais da população brasileira neste novo "mundo".

3.1 A importância do Marco Civil da Internet

Em outubro de 2009, o Ministério da Justiça (MJ) em parceria com a Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, iniciou a construção do que seria o MCI, através de consulta pública online. Segundo Papp (2014), durante a Campus Party de 2010, Ricardo Poppi, após utilizar a base de dados da consulta pública realizada pelo MJ, conseguiu sintetizar em visuais em *flash*, gráficos, árvores de palavras, dentre outros, os principais tópicos comentados na consulta. Esse trabalho foi essencial para a criação dos princípios básicos do MCI, sendo eles a fiscalização, neutralidade e questões relacionadas à privacidade.

A construção da legislação do MCI durou até 2011, quando o projeto de lei 2.126/2011 da presidenta Dilma Rousseff foi enviado à câmara dos deputados e em 2014 se tornou lei. Pioneiro no mundo e amplamente elogiado durante o NETmundial, o Marco Civil da Internet serviu como pontapé inicial em enfatizar a importância da privacidade e da fiscalização de dados coletados na internet. Durante o NETmundial, Tim Berners-Lee, professor do MIT (Instituto de Tecnologia de Massachusetts) e criador da *World Wide Web*, elogiou o Brasil por sua abordagem exemplar na promoção dos direitos na internet por meio de políticas governamentais. Ele enfatizou que o Brasil servia como um modelo positivo de como os governos podem desempenhar um papel construtivo na regulamentação da internet, além de estimular outros países a seguirem o exemplo brasileiro e adotarem legislações semelhantes para fortalecer os direitos online.

É importante ressaltar que o NETmundial, que ocorreu nos dias 23 e 24 de abril, no dia em que o MCI foi aprovado na câmara dos deputados, teve como estopim o discurso da presidenta Dilma Rousseff durante a abertura da Assembleia Geral da ONU em 2013,

motivado pelas denúncias de espionagem em massa conduzidas pelos Estados Unidos, um caso claro de violação de privacidade.

A lei introduzida ressalta e estabelece a garantia da proteção e anonimização dos dados dos usuários, exigindo a inviolabilidade dos dados coletados pelas empresas. Além disso, exige que os termos de uso incluam claramente informações sobre a coleta, uso, armazenamento e tratamento dos dados, determinando que sejam utilizados exclusivamente para os propósitos estabelecidos durante sua captura a partir da licitação do propósito. No artigo 7º, inciso VII, é interessante reparar que a lei ressalta o: "não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei" (BRASIL, 2014).

Apesar da ampla e clara proteção dos dados pessoais prevista na lei, não há detalhamento de normas e padrões a serem seguidos, deixando esta responsabilidade para o Comitê Gestor da Internet. Fato que precede e legitima a criação da Lei Geral de Proteção de Dados (LGPD).

3.2 O Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia

Estimulados pelas discussões relacionadas à construção do MCI, em 2012, a Comissão Europeia se reuniu para discutir a política de proteção de dados da União Europeia (UE): "Em 2012, a Comissão Europeia ('comissão') propôs uma reforma abrangente das regras de proteção de dados da UE 'para fortalecer os direitos de privacidade on-line e impulsionar a economia digital da Europa'" (FREED e CARVALHO, 2024, p. 394). Na Europa, o assunto de proteção de dados já era um tema relevante antes da comissão de 2012. Em sua legislação, a UE possuía a Directiva 95/46/CE, também conhecida como a Diretiva de Proteção de Dados, cujo principal objetivo era proteger os direitos e liberdades fundamentais das pessoas singulares, em particular o direito à privacidade no tratamento de dados pessoais. Adotada em 1995, essa diretiva abrangia, em seus 34 artigos, diversos aspectos relacionados à proteção de dados. Entre os temas abordados, destacam-se a "licitação do propósito" da coleta de dados, conforme estipulado no artigo 6º, os princípios de igualdade no tratamento de dados discutidos na seção III, nos artigos 8º e 9º, e os direitos de acesso, retificação, apagamento ou bloqueio de dados, conforme descrito no artigo 12º. A diretiva também trazia definições importantes, como o que constitui um dado pessoal, o que é considerado "tratamento de dados", e os nomes técnicos dos responsáveis pelas etapas de tratamento de dados.

É importante ressaltar que a Directiva 95/46/CE representou um avanço significativo para a União Europeia na proteção de dados. No entanto, conforme observam Freed e Carvalho (2024), no ano de sua promulgação, em 1995, o Google ainda não havia sido fundado, fato que ocorreu somente três anos depois. Este detalhe evidencia como a lei rapidamente se tornou desatualizada, não abrangendo os temas mais modernos relacionados à coleta e ao tratamento de dados.

Com essa perspectiva em mente, em 2014, o Parlamento Europeu, após os devidos processos legislativos, votou com 621 votos a favor da reforma conhecida como "*General Data Protection Regulation*", ou em português "Regulamento Geral sobre a Proteção de Dados" (RGPD). Um ano depois, em 2015, após o posicionamento do Conselho Europeu, as alterações do Parlamento, a apresentação da nova proposta para a Comissão e um comitê de conciliação entre o Parlamento, o Conselho e a Comissão, o RGPD foi aprovado e adotado pela UE em 2016 sob o Regulamento 2016/679 do Parlamento Europeu e do Conselho, sendo totalmente implementado na UE a partir de 25 de maio de 2018.

Conforme comentam Freed e Carvalho (2024), o RGPD representou um grande avanço para a UE, uma vez que a legislação anterior, a Directiva, exigia que os Estados-Membros a implementassem em suas próprias legislações. Em contraste, o RGPD é um regulamento, e os regulamentos da UE são diretamente aplicáveis nos Estados-Membros a partir da data de sua entrada em vigor.

Em seu escopo, a RGPD tem um enfoque principalmente na proteção da privacidade e na proteção dos dados pessoais. O panorama geral do regulamento tem com objetivo proteger as pessoas, os cidadãos da UE, a partir dos direitos fundamentais estabelecidos na Convenção Europeia dos Direitos Humanos de 1950, onde em seu artigo 8º, cita:

> " Artigo 8º. Direito ao respeito pela vida privada e familiar.
> 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.
> 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem - estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros." (UNIÃO EUROPEIA, 1950).

Portanto, o RGPD surge como "um regulamento da UE desenvolvido para *controlar* o uso de dados pessoais de indivíduos, a fim de proteger sua privacidade e *assegurar* a conformidade (*compliance*) com regras de proteção de dados." (FREED e CARVALHO, 2024, p. 396).

O regulamento representa assim um marco na evolução das políticas de proteção de dados, destacando-se por sua abrangência e rigor. Ele não apenas fortalece os direitos dos indivíduos, mas também impõe responsabilidades significativas às organizações, promovendo um ambiente de maior transparência e segurança no tratamento de dados pessoais. Com sua implementação, a UE reafirmou seu compromisso com a privacidade e a proteção dos dados, aspectos essenciais para a construção de uma economia digital sólida e confiável.

3.2.1 Princípios, direitos e obrigações do RGPD

O RGPD é uma legislação extremamente abrangente, composta por 99 artigos divididos em 11 capítulos. Esses capítulos abordam a aplicação da lei, os princípios, os direitos dos titulares dos dados coletados, e as obrigações dos controladores e operadores dos dados. A norma deixa em evidência sua aplicação extraterritorial, proibindo a transferência dos dados dos cidadãos para terceiros fora do território da UE, existem três exceções que permitem a transferência: a transferência será feita para um dos países em que houve o reconhecimento por parte da Comissão Europeia como localidades que contém legislações que proporcionem proteção parecida ou superior a proteção da UE; a transferência está coberta por "garantias adequadas" conforme indica o 46º artigo da lei; ou a transferência de dados é coberta por uma derrogação, amplamente indicadas no 49º artigo da lei.

De maneira geral, em seus princípios, a RGPD dispõe no capítulo II, artigo 5º, 6 princípios relativos ao tratamento dos dados pessoais, sendo eles:

> "A) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados (licitude, lealdade e transparência);
> B) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.o, n.o 1 (limitação das finalidades);
> C) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados (minimização dos dados);
> D) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora (exatidão);
> E) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.o, n.o 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados (limitação da conservação);
> F) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou

> danificação acidental, adotando as medidas técnicas ou organizativas adequadas (integridade e confidencialidade);" (UNIÃO EUROPEIA, 2016).

Esses princípios são fundamentais porque estabelecem noções mais completas sobre a licitação do propósito, detalhando quando os dados podem ser legalmente tratados, quando o tratamento é necessário e limitando o uso dos dados conforme a finalidade estabelecida. Além disso, o regulamento aborda questões de segurança, integridade, confidencialidade, responsabilidade e a restrição do uso de "dados sensíveis". Os dados sensíveis são especificamente tratados nos 6º e 9º artigos, que listam quais são esses dados e proíbem seu tratamento conforme a redação do 9º artigo:

> "É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa." (UNIÃO EUROPEIA, 2016).

Esta foi a primeira vez que uma legislação abordou, no quesito de proteção de dados, questões relacionadas a dados sensíveis, além de listar e proibir o tratamento deste tipo de dado, salvo as condições dispostas posteriormente no 9º artigo. A partir disso, o RGPD prossegue no capítulo III abordando os direitos dos titulares dos dados, enfatizando o direito à transparência, o direito de ser informado, o direito de acesso, o direito de retificação e atualização, e o direito de eliminação dos dados. Além desses direitos, o RGPD garante aos titulares o direito de exigir a limitação do tratamento dos dados, o direito à portabilidade dos dados para outro serviço e o direito de oposição ao tratamento dos dados.

O capítulo IV do RGPD aborda as obrigações dos controladores e operadores de dados. Este capítulo é crucial para estabelecer uma relação com as normas de *compliance*, pois explicita de maneira clara as responsabilidades e obrigações daqueles que realizam a coleta e o tratamento dos dados. No 24º artigo, a lei define quem são os responsáveis pelo tratamento dos dados, detalhando o papel e como identificar quem são os controladores.

> "[...] eles [os controladores] decidem quais dados coletar e determinam o motivo pelo qual os dados serão tratados, exercendo controle geral sobre essas atividades. Os controladores devem demonstrar responsabilidade e conformidade com os requisitos previstos no GDPR [RGPD]". (FREED e CARVALHO, 2024, p. 403).

Quando a lei aborda o papel dos operadores e como identificá-los, no artigo 28º, ela define que:

> "eles [os operadores] tratam os dados pessoais 'por conta do responsável pelo tratamento' por meio de um contrato ou 'outro dado normativo'[...]. Esse serviço pode incluir a coleta e o tratamento de dados, mas o operador não determina quais dados coletar, para que são usados, o fundamento legal para o tratamento, e não está interessado no resultado do tratamento." (FREED e CARVALHO, 2024, p. 403 e 404).

É interessante notar que o RGPD faz uma distinção clara entre o papel da alta administração e o da operação, deixando claro que a responsabilidade pela estruturação da coleta e do tratamento de dados recai sobre a administração. Os funcionários devem seguir diretrizes estabelecidas e não criar suas próprias metodologias, ressaltando mais uma vez a importância de programas de *compliance* na estruturação de projetos que envolvam a coleta de dados.

Por fim, ainda no capítulo IV, a partir do 25º artigo, são detalhadas as obrigações dos controladores e operadores. Essas obrigações se baseiam no princípio da *accountability* (responsabilidade), que exige não apenas o cumprimento do RGPD, mas também a implementação de métodos eficazes para garantir a conformidade com a lei durante o planejamento e a execução, além de melhorias contínuas para corrigir possíveis falhas identificadas. Este artigo assim, estabelece a proteção de dados *by design* e *by default*, conceito que segundo Freed e Carvalho (2024), os controladores e operadores incluem diversas medidas e elementos nas atividades capazes de mitigar e proteger os dados durante seu tratamento.

> "a) *by design*
> [...] Ele [o controlador] deve integrar medidas desenhadas para proteger os direitos dos titulares de dados no próprio tratamento e que sejam efetivas desde a sua concepção.
> b) *by default*
> [...] o controlador deve usar 'as medidas técnicas e organizativas adequadas' para garantir que, por padrão, apenas os dados pessoais estritamente necessários para o tratamento legítimo sejam coletados. Além disso, inclui a garantia de restringir o acesso de pessoas físicas aos dados pessoais dos titulares dos dados." (FREED e CARVALHO, 2024, p. 404).

A lei ressalta novamente a necessidade de construir um programa de *compliance* na estruturação do projeto, mencionando pela segunda vez, de forma clara, que as empresas que coletam dados são obrigadas a formalizar esse método. O capítulo continua detalhando as obrigações dos controladores, incluindo determinações técnicas de segurança, como pseudonimização, criptografia e a nomeação de encarregados da proteção de dados (Data Protection Officers), dependendo dos custos, natureza, escopo e riscos associados ao tratamento dos dados. Além disso, estabelece o código de conduta da empresa em caso de violação, conforme o artigo 33º do RGPD.

O RGPD é uma legislação extensa e técnica que teve grande influência em outras leis ao redor do mundo, como a LGPD. É importante ressaltar que entre 2016 e 2018, o RGPD enfrentou muita resistência, tanto dentro quanto fora da Europa, devido ao seu caráter específico e extraterritorial. No entanto, após o escândalo da Cambridge Analytica em 2018, a sua implementação foi acelerada e a legislação passou a influenciar diversos países.

3.3 Caso da Cambridge Analytica

A empresa de consultoria política Cambridge Analytica em 2018 se envolveu em um grande escândalo político envolvendo o uso indevido de dados de milhões de usuários do Facebook. O caso foi amplamente divulgado pela mídia e essas revelações geraram grande controvérsia e preocupações sobre privacidade de dados, manipulação eleitoral e o papel das redes sociais na política.

No caso, segundo matéria da BBC News, departamento de notícias da *British Broadcasting Corporation* (BBC), a emissora pública nacional do Reino Unido, a empresa: "[...] usou um algoritmo capaz de elaborar perfis psicológicos de usuários por meio de suas interações no Facebook." (BBC NEWS BRASIL, 2018). Esse algoritmo é extremamente preciso e, segundo a matéria, o algoritmo conseguia traçar com precisão, a partir de 300 curtidas, o perfil de personalidade de um usuário da rede. Somado aos 1.71 bilhão de usuários mensais ativos que o Facebook alcançou em junho de 2016, segundo dados reportados pela própria empresa em seus relatórios financeiros trimestrais, a Cambridge Analytica tinha em suas mãos uma ferramenta poderosa de análise de dados.

O escândalo surgiu devido à maneira como a consultoria política Cambridge Analytica coletava dados. Na época, a Meta (então chamada Facebook) não especificava em seus termos de uso que os dados coletados poderiam ser utilizados para fins políticos. A Cambridge Analytica utilizou as plataformas de desenvolvedor do próprio Facebook para obter os dados necessários para traçar perfis de milhões de usuários nos Estados Unidos e no Reino Unido. Esses perfis foram usados para realizar campanhas políticas a favor de Donald Trump nas eleições de 2016 e a favor do *Brexit* no referendo de 2016, que decidiu pela saída do Reino Unido da União Europeia.

Este caso foi crucial para a criação de leis mais específicas de proteção de dados e para uma fiscalização mais rigorosa das leis existentes. Mesmo com a existência de leis como o MCI de 2014 no Brasil, as pessoas não se sentiam seguras, elas consideravam que as leis eram incompletas, acelerando o processo do RGPD a entrar em vigor e a criação da LGPD brasileira.

3.4 A Lei Geral de Proteção de Dados (LGPD)

Publicada em 15 de agosto de 2018, a Lei nº 13.709, mais conhecida como Lei Geral de Proteção de Dados Pessoais brasileira (LGPD), foi um importante passo para modernizar a

legislação brasileira em relação à privacidade e proteção de dados. A LGPD estabelece um conjunto de regras e princípios para o tratamento de dados pessoais, tanto no setor público quanto no privado, assegurando maior controle e proteção aos indivíduos. Complementando o MCI, que desde 2014 regula os direitos e deveres na utilização da internet no Brasil, a LGPD reflete um avanço significativo, colocando o país em sintonia com as melhores práticas globais de governança de dados e fomentando um ambiente de confiança e segurança digital.

Inspirada pelo RGPD, a LGPD foi promulgada logo após os escândalos da Cambridge Analytica como a solução brasileira para a regulamentação da proteção de dados. Seguindo o modelo do RGPD, a LGPD visa regular o tratamento de dados coletados ou tratados no Brasil, independentemente do país onde estejam sediados ou armazenados, com o objetivo de proteger a liberdade e a privacidade das pessoas naturais.

A lei define claramente o que são dados pessoais, dados sensíveis e quem são os agentes de tratamento de dados. A LGPD utiliza os mesmos termos e significados que o RGPD: dados pessoais são todas as informações que identificam uma pessoa natural, como nome, endereço, e-mail, etc. Dados sensíveis são informações sobre origem racial, religião, opiniões e filiações políticas, dados relacionados à saúde, etc. Os agentes de tratamento também mantêm os mesmos termos e funções do RGPD, utilizando as denominações de controlador e operador para os dois principais papéis no tratamento de dados.

Além disso, a LGPD dedica atenção especial ao tratamento de dados pessoais de crianças e adolescentes. Conforme disposto no art. 14°, parágrafo 1º, da lei, "o tratamento de dados pessoais de crianças deve ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal." (BRASIL, 2018). A coleta de dados pessoais de crianças sem o consentimento é permitida apenas uma única vez, e os dados não podem ser armazenados ou repassados a terceiros após o uso inicial. Isso garante que o tratamento seja realizado com o máximo de cuidado e respeito à privacidade das crianças.

Ademais, a LGPD estabelece que a participação de crianças e adolescentes em jogos, aplicativos ou outras atividades de internet não pode ser condicionada à entrega de informações pessoais além daquelas estritamente necessárias para a realização da atividade. Essa medida visa proteger os jovens usuários de práticas abusivas e garantir que seus dados pessoais sejam tratados de maneira ética e segura.

Sendo assim, a implementação da LGPD representa um marco crucial para a proteção da privacidade e segurança dos dados no Brasil. Ao alinhar-se com as melhores práticas globais, como aquelas estabelecidas pelo RGPD da UE, a LGPD reforça o compromisso do Brasil com a governança de dados e a construção de um ambiente digital confiável. O

destaque dado ao tratamento de dados de crianças, com requisitos rigorosos de consentimento parental, exemplifica a importância de proteger os grupos mais vulneráveis na era digital.

A LGPD não apenas fortalece a proteção dos dados pessoais, mas também incentiva as empresas a adotarem práticas de *compliance* digital robustas. Este movimento é essencial para garantir que as organizações não apenas cumpram as normas legais, mas também promovam uma cultura de responsabilidade e transparência no tratamento de dados. A conformidade com a LGPD, portanto, não é apenas uma obrigação legal, mas um diferencial competitivo que pode aumentar a confiança dos consumidores e *stakeholders.*

3.4.1 Tratamento, responsabilidades e penalidades da LGPD

A LGPD, em seus termos, estabelece diretrizes claras e específicas sobre como os dados pessoais devem ser tratados, quais são as responsabilidades que das empresas e dos agentes de tratamento e as penalidades aplicáveis em caso de descumprimento. O tratamento de dados pessoais, conforme definido pela LGPD, abrange uma ampla gama de operações realizadas com dados pessoais, desde a coleta e armazenamento até a eliminação dos dados. A lei define princípios fundamentais que devem ser seguidos durante o tratamento, incluindo a finalidade, necessidade, transparência, segurança, e prevenção. Esses princípios garantem que os dados pessoais sejam tratados de maneira ética e segura, minimizando riscos e protegendo os direitos dos titulares dos dados. A lei ainda define que os agentes de dados poderão tratar os dados pessoais a partir de dez fatores, sendo eles:

> "(I) com o consentimento do titular; (II) para cumprir obrigação legal do controlador do tratamento; (III) para o tratamento e uso compartilhado para execução de políticas públicas, nos casos de Administração Pública; (IV) para a realização de estudos por órgão de pesquisa, desde que anonimizados; (V) para a proteção da vida ou da incolumidade física do titular ou de terceiro; (VI) para a tutela da saúde, desde que realizada por profissionais do setor; (VII) para a execução ou pré-execução de um contrato com o titular; (VIII) para pleitos em processos judicial, administrativo ou arbitral; (IX) interesses legítimos do controlador, desde que não afetem direitos e liberdades fundamentais; ou (X) para a proteção do crédito." (BLUM e MORAES, 2024).

É importante mencionar que a legislação estabelece também sete condições nas quais as entidades podem legalmente tratar dados sensíveis, visto que o tratamento desse tipo de dados é proibido, salvo mediante consentimento específico e destacado do titular, para finalidades determinadas ou, sem o consentimento, quando for indispensável para:

> "(I) o controlador cumprir uma obrigação legal; (II) a administração pública executar políticas públicas; (III) órgão de pesquisa realizar estudos, mediante anonimização; (IV) exercício regular de direitos como em contratos, processos judiciais, administrativos ou arbitrais; (V) proteção da vida ou da incolumidade física do titular ou de terceiro; (VI) tutela da saúde, desde que realizado por profissionais da área; ou (VII) garantia de prevenção à fraude e à segurança do titular." (BLUM e MORAES, 2024).

Essas disposições da LGPD são essenciais para garantir que o tratamento de dados pessoais seja realizado de maneira ética e em conformidade com os princípios de transparência e segurança. A lei também atribui responsabilidades específicas ao controlador e ao operador em casos de descumprimento. O controlador, sendo o principal responsável, deve reparar danos patrimoniais, morais, individuais ou coletivos causados durante o tratamento de dados, estando sujeito à inversão do ônus da prova a critério do juiz. O operador, por sua vez, será responsabilizado somente se descumprir a legislação ou se não seguir as instruções lícitas do controlador.

O descumprimento da LGPD prevê uma série de penalidades para as organizações que violarem suas disposições. Essas penalidades podem variar desde advertências e multas diárias até a publicização da infração e a suspensão das atividades de tratamento de dados. As multas podem alcançar até 2% do faturamento da empresa, limitadas a R$50 milhões por infração. A imposição dessas penalidades visa incentivar a conformidade com a lei e assegurar que as organizações tratem os dados pessoais com o devido respeito e cuidado. A aplicação dessas penalidades entrou em vigor a partir de 1º de agosto de 2021, conforme estipulado pela Lei nº 14.010, de 10 de junho de 2020, que acabou estabelecendo um período de adaptação de 1082 dias até a efetiva implementação da LGPD.

A partir dessa data, as organizações passaram a ser responsabilizadas pelos danos que poderiam causar. No entanto, o Artigo 43 da LGPD estabelece três situações em que os agentes de tratamento não serão responsabilizados pelo descumprimento da lei:

> "Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro." (BRASIL, 2018).

Caso a organização adote políticas rigorosas de *compliance* digital, conhecidas na lei como "Programa de Governança em Privacidade", implementando controles internos e processos contínuos de auditoria para garantir a conformidade, esse programa pode auxiliar na redução das penalidades impostas pela Autoridade Nacional de Proteção de Dados (ANPD) em casos de incidentes.

3.4.2 Autoridade Nacional de Proteção de Dados e o *Compliance* Digital

A Autoridade Nacional de Proteção de Dados (ANPD) é um órgão central na estrutura de proteção de dados no Brasil. Criada pela LGPD, a ANPD foi formalmente instituída pela Medida Provisória nº 869 de 2018, que posteriormente se converteu na Lei nº 13.853 de 2019. A ANPD possui natureza jurídica de órgão da administração pública federal, sendo vinculada à Presidência da República.

A principal função da ANPD é garantir a aplicação da LGPD, regulamentando e fiscalizando as atividades de tratamento de dados pessoais realizadas pelas organizações. Esse órgão tem o poder de aplicar sanções administrativas em casos de descumprimento da LGPD, bem como orientar e educar tanto o público quanto as organizações sobre a importância da proteção de dados. A ANPD atua em diversas frentes, sendo a fiscalização uma de suas atribuições mais importantes. Ela tem a responsabilidade de monitorar e assegurar que as práticas de tratamento de dados pessoais nas organizações estejam em conformidade com a legislação vigente. Além disso, a ANPD é responsável por emitir normas e diretrizes que interpretam a LGPD e guiam as organizações na implementação de práticas adequadas de proteção de dados. Outro aspecto crucial da ANPD é sua função orientadora, desempenhando um papel educativo, disseminando informações sobre boas práticas de proteção de dados e segurança da informação, e incentivando uma cultura de privacidade tanto nas empresas quanto na sociedade em geral.

A LGPD recomenda que as organizações implementem programas de governança em privacidade, consistindo em medidas técnicas e administrativas destinadas a proteger os dados pessoais. A ANPD fornece diretrizes para a criação e manutenção desses programas, monitorando sua aplicação e promovendo uma cultura de conformidade com as normas de proteção de dados. A ANPD, assim, promove a atuação do *compliance* digital nas empresas, incentivando práticas que asseguram a conformidade com a legislação vigente e a proteção dos direitos dos titulares de dados pessoais:

> "Em primeiro lugar, cabe destacar a importância de se implementar um Programa de Governança em Privacidade (PGP) (art. 50, § 2º, I). Embora a lei indique ao controlador a possibilidade de elaborar esse programa, o operador, enquanto agente de tratamento, também pode produzir o seu próprio programa. [...]" (ANPD, 2022).

O Programa de Governança em Privacidade, como cita as bibliografias desenvolvidas pela ANPD, envolve a implementação de conjuntos de medidas técnicas e administrativas destinadas a proteger os dados pessoais e garantir a conformidade com a legislação vigente. Esses programas de governança em privacidade não apenas asseguram que as empresas cumpram as disposições da LGPD, mas também promovem uma cultura organizacional focada na proteção dos dados pessoais. A ANPD tem desempenhado um papel crucial nesse contexto, fornecendo orientações detalhadas sobre como criar e realizar a manutenção desses programas. Através de suas diretrizes, a agência ajuda as organizações a entenderem as melhores práticas de segurança da informação e a importância da privacidade de dados, facilitando a implementação de políticas e procedimentos eficazes.

Além das diretrizes práticas, a ANPD tem contribuído significativamente para a literatura sobre o assunto. A agência publicou diversos livros que enfatizam as práticas de GRC no contexto do *compliance* digital. Essas publicações são recursos valiosos para profissionais e organizações que buscam aprofundar seus conhecimentos e aprimorar suas práticas de proteção de dados.

Os livros publicados pela ANPD abordam uma ampla gama de temas, incluindo a identificação e a mitigação de riscos relacionados ao tratamento de dados pessoais, a implementação de políticas de privacidade, e a importância de uma abordagem integrada para a governança em privacidade. Essas obras oferecem uma visão abrangente sobre como desenvolver e manter um programa de governança em privacidade eficaz, destacando as responsabilidades das organizações e os benefícios de uma cultura de conformidade.

Em suma, a atuação da ANPD no campo do *Compliance* Digital é essencial para o fortalecimento da proteção de dados no Brasil. Ao regulamentar, fiscalizar e orientar as organizações, a agência não apenas assegura o cumprimento da LGPD, mas também promove uma cultura de privacidade e segurança da informação. Através de suas publicações e diretrizes, a ANPD continua a ser uma fonte de conhecimento e orientação para todos que buscam estar em conformidade com a legislação e proteger os direitos dos titulares de dados pessoais.

3.5 O Uso de *Compliance* na Administração Pública Direta

Como observado, existe uma ampla discussão sobre as práticas de GRC no contexto das organizações privadas, mas muitas vezes a incorporação das noções de integridade e conformidade nas instituições que fazem parte da Administração Pública Direta não recebe a devida atenção. No contexto legislativo, não existe uma lei específica que obrigue a adoção das práticas de GRC, sendo os valores divididos entre diversas leis, como:

> "(I) Lei 8.429/1992 – Lei de Improbidade Administrativa; (II) Decreto federal 1.171/1994, que estabelece o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal; (III) Decreto 5.480/2005, que dispõe sobre o Sistema de Correição do Poder Executivo Federal; (IV) Lei Complementar 101/2000 (Lei de Responsabilidade Fiscal), tendo por objeto aspectos éticos e morais e o comportamento da liderança; (V) Lei 12.527/2011 – Lei de Acesso à Informação; e (VI) Lei 12.813/2013, que dispõe sobre o conflito de interesses no exercício de cargo ou emprego do Poder Executivo Federal." (OLIVEIRA e ACOCELLA, 2019)

Embora as leis mencionadas anteriormente forneçam um arcabouço regulatório essencial, observa-se que a administração pública federal não discute abertamente a aplicação de modelos de *compliance* ou métodos de GRC de forma explícita para seu funcionamento interno. A implementação dessas práticas, muitas vezes cruciais para a integridade e eficiência administrativa, acaba sendo relegada, caso haja interesse, aos níveis estadual e municipal. Isso cria uma disparidade na adoção de boas práticas de governança, uma vez que a responsabilidade pela implantação e operacionalização de tais modelos pode variar significativamente entre diferentes jurisdições subnacionais.

Em referência a essa falta de legislação, em 28 de março de 2019, foi promulgado o Decreto nº 39.736, que aborda a Política de Governança Pública e *Compliance* na Administração Direta, Autárquica e Fundacional do Poder Executivo do Distrito Federal. Este decreto estabeleceu a necessidade de implementar políticas de governança e programas de integridade nos órgãos da Administração Pública do Distrito Federal, sendo esse o primeiro passo nítido da administração direta brasileira na adoção de práticas de GRC. A governança pública, como chamado no decreto, é o sistema GRC aplicado à administração pública e nele são abordados cinco eixos principais: (I) Comprometimento e apoio da alta direção; (II) Instância responsável pelo plano de integridade; (III) Análise de risco; (IV) Monitoramento Contínuo; (V) Disseminação da cultura de integridade. Estes cinco eixos, conforme estabelecido no decreto, adaptam e simplificam os princípios da ISO 19600:2014, utilizando

terminologias específicas do método SGRC para facilitar a implementação e compreensão das práticas de governança e *compliance*.

A implementação do *compliance* na Administração Pública Direta é de suma importância, pois promove um ambiente de transparência e responsabilidade, sendo essencial para assegurar que todos os processos administrativos sejam claros e compreensíveis, permitindo que a população e os órgãos fiscalizadores acompanhem as ações governamentais de forma precisa além de garantir que cada ator dentro da administração pública conheça e assuma suas funções e obrigações, o que facilita a identificação de falhas e a atribuição de consequências adequadas quando necessário. Esse programa também estabelece controles internos rigorosos e promove uma cultura de integridade, tornando mais difícil a ocorrência de irregularidades. Outro aspecto fundamental é a melhoria na gestão dos recursos públicos. A implementação de *compliance* não apenas aumenta a eficiência, mas também a eficácia das operações governamentais. Com processos mais claros e responsabilidades bem definidas, a administração pública pode operar de maneira mais organizada e produtiva. Resultando em uma melhor alocação de recursos, redução de desperdícios e uma maior capacidade de alcançar os objetivos governamentais de forma mais eficaz. Em suma, o *compliance* contribui significativamente para a criação de uma administração pública mais transparente, responsável, íntegra e eficiente, beneficiando diretamente toda a sociedade.

3.5.1 LGPD na Administração Pública Direta

Com o advento da LGPD em 2018, os órgãos públicos foram compelidos a se organizar para cumprir as exigências da lei. No capítulo IV, a LGPD discorre sobre as regras que a administração pública deve seguir em casos de infração da lei, mencionando, ainda que de forma superficial, a adoção de *compliance*. Este capítulo estabelece diretrizes fundamentais para a administração pública, mas não detalha explicitamente como um sistema de *compliance* deve ser implementado para mitigar sanções, cabendo à ANPD sugerir como deve ser estruturado o sistema, conforme estabelecido nos artigos 31 e 32 da lei:

> *"Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.*
>
> *Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público." (BRASIL, 2018).*

Esta transição para da administração pública para *compliance* digital é um passo fundamental para a modernização, garantindo que todas as práticas e atividades digitais estejam em conformidade com as leis e regulamentos vigentes. Na era da informação, os dados emergem como um dos ativos mais valiosos para organizações, incluindo a administração pública. A conformidade com essas regulamentações não só protege os dados dos cidadãos, mas também fortalece a confiança pública nas instituições governamentais, promovendo uma cultura de transparência e responsabilidade.

A implementação do *compliance* digital, principalmente na administração pública direta, apresenta tanto desafios quanto benefícios significativos, entre estes desafios, destaca-se a necessidade constante de atualizações tecnológicas para acompanhar a evolução de ameaças e das normas regulatórias, isso exige investimentos contínuos em infraestrutura tecnológica e treinamentos específicos para os funcionários públicos, para que eles estejam preparados para operar e gerenciar as novas ferramentas de *compliance* digital. No entanto, os benefícios dessa transição são substanciais, já que a proteção de dados é um dos principais ganhos, evitando vazamentos e outros incidentes que podem comprometer a privacidade e a segurança das informações. Além disso, o *compliance* digital melhora a confiança pública, pois os cidadãos se sentem mais seguros ao saber que suas informações estão sendo tratadas de acordo com os mais altos padrões de segurança e conformidade. Em suma, a transição para o *compliance* digital é essencial para a administração pública moderna, trazendo avanços significativos em termos de segurança, eficiência e transparência. A administração pública deve então adotar medidas 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.

4. O USO DO *COMPLIANCE* DIGITAL PELA DIRETORIA CENTRAL DE ADMINISTRAÇÃO DE PESSOAL DA PREFEITURA DE BELO HORIZONTE

A Prefeitura de Belo Horizonte (PBH) está situada na capital do estado de Minas Gerais, uma das cidades mais importantes e influentes do Brasil. Fundada em 1897, Belo Horizonte se destaca como um centro econômico, político e cultural crucial para a região sudeste do país. Com uma população superior a 2,5 milhões de habitantes, a cidade é reconhecida por sua infraestrutura robusta, parques urbanos e um planejamento urbano inovador, especialmente para a época de sua fundação. A PBH desempenha um papel essencial na administração e no desenvolvimento da cidade, sendo responsável pela implementação de políticas públicas que influenciam diretamente a qualidade de vida de seus cidadãos.

Dentro da estrutura organizacional da PBH, existem 18 secretarias municipais e correlatas da administração direta e indireta, cada uma desempenhando um papel crucial na governança e operação da cidade. Neste trabalho, vamos focar em uma das secretarias mais significativas para o funcionamento administrativo interno da prefeitura: a Secretaria Municipal de Planejamento, Orçamento e Gestão (SMPOG). Essa secretaria é fundamental para o desenvolvimento estratégico de Belo Horizonte, pois é responsável pela elaboração e monitoramento do orçamento municipal, planejamento do uso eficiente dos recursos e gestão dos processos administrativos que garantem a execução eficaz da PBH.

A SMPOG é composta por quatro subsecretarias, entre as quais a Subsecretaria de Gestão de Pessoas (SUGESP) se destaca por seu papel crucial na administração de pessoal da prefeitura. No âmbito da SUGESP, encontra-se a Diretoria Central de Administração de Pessoal (DCAP), onde tive a oportunidade de trabalhar, passando por duas das suas quatro gerências. A diretoria é vital para o funcionamento eficiente da administração pública, garantindo que todas as questões relacionadas aos servidores sejam tratadas de maneira adequada e eficaz. As quatro gerências que compõem a DCAP são: a Gerência Central de Atendimento (GECEA), responsável pelo recebimento de demandas dos servidores relacionadas à sua vida profissional, fornecendo suporte e esclarecendo dúvidas, a GECEA é o primeiro setor a se comunicar com os futuros servidores e a cadastrar novos servidores, desempenhando um papel crucial no acolhimento dos colaboradores. A Gerência de Gestão da Folha de Pagamento (GESFO) atua diretamente na administração da folha de pagamento, assegurando que todos os servidores recebam seus vencimentos corretamente e dentro do prazo. Além disso, a GESFO é responsável pela gestão dos desligamentos, garantindo que

todo o processo seja realizado de forma transparente e eficiente. A Gerência de Gestão de Direitos e Benefícios (GETED) encabeça a administração dos direitos dos servidores e celetistas da prefeitura, incluindo frequência, ponto, férias, vale-transporte, vale-alimentação/refeição, tempo de serviço, progressão de carreira, entre outros, a GETED assegura que todos os benefícios e direitos sejam geridos conforme as normativas vigentes, promovendo a satisfação e o bem-estar dos servidores. E por fim, a Gerência de Gestão de Ingresso e da Vida Funcional (GEVIF) trata de assuntos relacionados a concursos, ingresso, cessão, informações da vida funcional, arquivamento dos documentos dos servidores e questões de estágio, desempenhando um papel central na gestão de todo o ciclo de vida dos servidores, desde a admissão até a aposentadoria ou desligamento. Além das gerências, há a Assessoria de Projetos Especiais (ASPE) que tem como função a gestão e orientação na elaboração de novas propostas, projetos, atividades, programas e ações, visando a garantir a melhoria dos processos dentro da DCAP.

A PBH, através de suas diversas secretarias e gerências, demonstra um compromisso contínuo com a melhoria da qualidade de vida de seus cidadãos e a eficiência administrativa. A DCAP, em especial, é de suma importância devido à quantidade de dados pessoais que guarda, sendo essa atenção necessária para reforçar a segurança e privacidade das informações dos servidores, garantindo um ambiente de trabalho confiável e protegido.

4.1 Modelo e Propósito da Entrevista

Inicialmente, o presente trabalho foi concebido para ser realizado através de entrevistas com a equipe de liderança da DCAP, utilizando o modelo de entrevista não-estruturado, esse método foi escolhido devido à sua capacidade de oferecer uma abordagem flexível e adaptável, onde os entrevistados teriam a oportunidade de compartilhar suas percepções e experiências de maneira livre e espontânea. A metodologia não-estruturada seria particularmente eficaz para captar nuances e percepções detalhadas sobre a gestão de pessoal e a implementação de políticas de *compliance* dentro da administração pública.

No entanto, devido ao calendário eleitoral do ano de 2024, a viabilidade das entrevistas foi comprometida e após uma avaliação criteriosa, concluiu-se que as entrevistas não poderiam ser realizadas conforme planejado, dado o impacto das restrições impostas pelo período eleitoral. Essas restrições, geralmente associadas à necessidade de neutralidade e à intensificação das atividades administrativas durante o período eleitoral, tornaram inviável a coleta de dados por meio de entrevistas diretas com os líderes da DCAP e para contornar essa

limitação, o trabalho foi reformulado para que as entrevistas fossem realizadas através da Lei de Acesso à Informação, Lei n° 12.527/2011. As solicitações foram protocoladas por meio do sistema Tag/BH Digital em 02 de agosto de 2024, permitindo que a coleta de dados continuasse de forma legal e adequada às restrições impostas pelo período eleitoral. Essa adaptação metodológica garantiu a continuidade da pesquisa, preservando a integridade e a qualidade do estudo, ao mesmo tempo em que se alinhou às exigências legais e administrativas vigentes.

O propósito desta entrevista é analisar e compreender a maturidade da DCAP em relação às práticas de GRC adotadas por esta diretoria, além disso, busca-se avaliar a eficácia da comunicação interna, tanto entre a diretoria e suas respectivas gerências, que lidam com as operações diárias, quanto entre a diretoria e a subsecretaria, no que tange à implementação e monitoramento dessas práticas. Para alcançar esses objetivos, a entrevista foi estruturada para abordar diferentes níveis hierárquicos dentro da DCAP, assegurando uma visão abrangente e detalhada das práticas de GRC. Foram realizadas perguntas direcionadas às gerências, que são responsáveis pelo aspecto operacional e execução das políticas da diretoria, para entender como as práticas de GRC são aplicadas no cotidiano e quais desafios operacionais podem surgir. A diretoria, que supervisiona e gerencia essas operações, foi questionada sobre sua visão estratégica em relação ao GRC e adicionalmente, a entrevista incluiu a assessoria de projetos especiais, uma área diretamente envolvida com as questões de *compliance* dentro da diretoria, sendo eles responsáveis por garantir que as políticas e práticas de GRC estejam alinhadas com os padrões estabelecidos, além de monitorar sua efetividade. Esse enfoque multifacetado permite uma análise mais rica e detalhada da maturidade da DCAP em GRC, fornecendo percepções valiosas sobre as práticas atuais e identificando possíveis áreas de melhoria, buscando mapear a situação atual das práticas de governança, riscos e *compliance* dentro da diretoria.

4.2 Resultados da Entrevista

Das seis solicitações protocoladas no sistema Tag/BH Digital, todas solicitações foram respondidas dentro do prazo estabelecido, tornando-se viável a análise no presente trabalho. Na pesquisa realizada com a DCAP, foram abordados diversos aspectos relacionados à conformidade com a LGPD, práticas de GRC, bem como as metodologias de planejamento e gestão adotadas pela diretoria, sendo estas questões fundamentais para compreender a maturidade e a eficácia da DCAP no gerenciamento de suas atividades e na adaptação às

exigências legais. Na pesquisa realizada com a ASPE, foram abordados os métodos, a estrutura e o funcionamento do programa de *compliance* digital, abordando as características e os indicadores do programa, para medir o nível de maturidade e o planejamento da diretoria desde a publicação da lei. E por fim, as pesquisas realizadas com as gerências, foram abordados os conhecimentos e a familiaridade com as técnicas de *compliance*, questionando a relação entre os servidores e os padrões estabelecidos pelo programa. Todas as informações foram revisadas e enviadas pela Subcontroladoria de Transparência e Prevenção Da Corrupção da Controladoria-Geral do Município de Belo Horizonte.

Para entender o contexto da organização, a adaptação da DCAP com a LGPD teve início em 2019, antes mesmo da lei entrar em vigor em setembro de 2020, a diretoria implementou ações como o mapeamento de processos e a identificação de riscos, com o objetivo de preparar a organização para as novas exigências legais. As capacitações para os agentes públicos da DCAP começaram em 2023, indicando um esforço para manter os servidores atualizados, em conformidade e preparados para lidar com as implicações da LGPD.

4.2.1 Resultado da DCAP

A DCAP adotou uma série de procedimentos internos para garantir o cumprimento dessa legislação, reconhecendo a importância da proteção de dados no setor público. Entre as medidas implementadas, destacam-se a capacitação contínua dos agentes públicos, a disponibilização de material de consulta específico e a criação de um fluxo interno de comunicação que envolve Grupos de Trabalho (GTs) dedicados à LGPD. Esses GTs têm a função de esclarecer dúvidas e orientar a execução das práticas exigidas pela lei, contribuindo para que os servidores estejam bem informados e preparados para lidar com as demandas relacionadas à proteção de dados. A escolha por esse modelo de capacitação e suporte contínuo demonstra o comprometimento da diretoria em promover uma cultura de conformidade e integridade.

Além disso, foi identificado que a DCAP possui conhecimento das práticas de GRC e as aplica conforme as exigências legais e regulamentares específicas do setor público. As práticas de GRC adotadas pela diretoria estão alinhadas com normas estabelecidas por órgãos de controle, como o Tribunal de Contas do Estado e a Lei de Responsabilidade Fiscal. Além disso, a diretoria realiza auditorias internas em conjunto com a Controladoria Geral do Município, e utiliza o e-Social como uma ferramenta essencial para assegurar o cumprimento

das obrigações fiscais, previdenciárias e trabalhistas. Essas iniciativas reforçam o compromisso da DCAP em manter a conformidade regulatória e promover a boa governança. No entanto, a implementação de uma frente mais robusta de Gestão de Riscos ainda está em fase de planejamento pois este novo projeto, que será coordenado pelos Grupos de Trabalho da LGPD, incluirá o mapeamento de processos, a identificação e classificação de riscos utilizando a ferramenta GUT, e a elaboração de planos de ação com base no método 5W2H. A expectativa é que essa nova frente de trabalho venha a fortalecer ainda mais a capacidade da diretoria de gerenciar riscos de maneira proativa.

No que diz respeito às metodologias de planejamento e gestão, embora a DCAP esteja familiarizada com a metodologia PDCA, ela não é utilizada diretamente no acompanhamento dos processos. Em vez disso, a diretoria desenvolveu uma abordagem própria para gerenciar projetos e atividades, incluindo a definição clara do escopo dos projetos, o planejamento estratégico para a execução das atividades e a elaboração de cronogramas detalhados. Além disso, a DCAP implementa planos de ação específicos para cada projeto, monitora as pendências e gerencia cenários para controle de riscos, a integração de *feedbacks* contínuos e o registro sistemático de todo o processo garantem que as lições aprendidas sejam documentadas e possam ser utilizadas para futuras melhorias. Esse modelo de gestão, embora personalizado, reflete o modelo de SGRC apresentado neste trabalho, demonstrando que mesmo não tendo conhecimento do modelo, a DCAP ajustou suas práticas de acordo com as necessidades específicas da administração pública, montando um modelo de eficiência e eficácia nas suas operações.

Em relação à comunicação interna, a DCAP realiza reuniões semanais entre a diretoria e as gerências para tratar de temas estratégicos e operacionais, as questões relacionadas à LGPD são frequentemente abordadas, evidenciando a relevância do tema para a diretoria. No entanto, foi observado que as reuniões com a liderança da SUGESP não seguem uma estrutura formalizada em termos de alinhamento sobre práticas de GRC e essa ausência de um alinhamento formalizado pode indicar uma oportunidade para melhorar a integração das práticas de *compliance* entre as diferentes camadas da administração pública, principalmente pelo fato que a DCAP acaba sobrecarregando seu papel de gerenciamento, tendo que fazer o trabalho de direção, estabelecendo as metas e o plano estratégico. Outro ponto relevante foi a ausência de documentação formal que descreva as políticas, normas e instrumentos de governança e *compliance* que devem ser adotados pelas gerências da DCAP. Embora tenha-se dito que existe a disponibilização de material de consulta específico e relatórios de auditoria ou monitoramento da conformidade digital, eles foram elaborados pela Controladoria Geral

do Município e não são adaptados para a rotina regular da diretoria, cabendo a interpretação dos agentes na aplicação das normas. Esses relatórios também são voltados para processos específicos considerados críticos, o que pode sugerir que a DCAP ainda não integrou plenamente essas práticas em sua operação diária.

Podemos concluir que, a entrevista com a DCAP revelou um comprometimento significativo da diretoria com a conformidade legal e a adoção de boas práticas de governança. Contudo, também destacou áreas onde há espaço para melhorias, especialmente no que diz respeito à formalização de práticas de GRC e à integração dessas práticas em todos os níveis da administração.

4.2.2 Resultado da ASPE

Durante a entrevista com a ASPE, foram abordados diversos tópicos relacionados à métodos, estrutura e funcionamento do *compliance* digital na diretoria. A ASPE indicou que, embora não exista um programa formal de *compliance* digital na DCAP, a diretoria adota diversas ações isoladas que abordam aspectos críticos como proteção de dados, privacidade, e governança de TI, sendo essas ações o treinamento e conscientização sobre a LGPD, revisões periódicas dos acessos aos sistemas para assegurar a conformidade com normas de proteção de dados, e a virtualização de serviços de RH, visando maior eficiência e ética. Um exemplo significativo dessas iniciativas é o Projeto LGPD, conduzido pela ASPE desde 2020, com foco na implementação de medidas de instrução, orientação e monitoramento para garantir o cumprimento integral da LGPD. Atualmente, segundo a assessoria, a capacitação dos agentes públicos da DCAP em relação à LGPD está em andamento, com 58% dos servidores já capacitados.

Apesar dessas iniciativas, a entrevista revelou a ausência de indicadores quantitativos de desempenho formais para avaliar a eficácia das ações de *compliance* digital, havendo um único indicador qualitativo relacionado ao treinamento e conscientização da LGPD, que inclui estudos de caso adaptados às áreas específicas sendo capacitadas, garantindo a compreensão e aplicabilidade dos conteúdos nas rotinas diárias. Essa abordagem, embora qualitativa, proporciona uma visão prática da eficácia do treinamento, essencial para a internalização das práticas de *compliance*.

A ASPE confirmou que a DCAP possui conhecimento das práticas de GRC e as aplica em consonância com as exigências legais e regulatórias do setor público através das normas do Tribunal de Contas do Estado, a Lei de Responsabilidade Fiscal, e o e-Social, conforme já

dito também pela DCAP. No que tange à estrutura organizacional, a ASPE destacou que, embora não haja um programa de *compliance* digital formal, existem equipes responsáveis por diferentes aspectos dessas ações. A equipe da ASPE lidera o Projeto LGPD, enquanto outras equipes, como a da Assessoria de Tecnologia da Informação e a Subsecretaria de Modernização da SMPOG, são responsáveis por aspectos técnicos e de virtualização dos serviços. Essa estrutura descentralizada reflete uma abordagem fragmentada, que busca integrar diferentes especialidades na promoção da conformidade e eficiência administrativa.

Quanto à capacitação contínua, a ASPE afirmou que, atualmente, as capacitações internas estão focadas principalmente na LGPD, com sessões de treinamento ocorrendo a cada quinze dias em rodízio entre as gerências e assessorias da DCAP. Essas capacitações são cruciais para manter o pessoal atualizado e preparado para lidar com as complexidades da conformidade digital. No que diz respeito a canais de denúncia, a ASPE informou que não existe um canal exclusivo da DCAP, podendo as denúncias serem encaminhadas através do sistema TAG, da Ouvidoria, por e-mail ou ofício. Além disso, há um fluxo específico para dúvidas ou denúncias relacionadas à LGPD, que envolve várias instâncias, desde o agente público até o Comitê Municipal de Proteção de Dados Pessoais. Foi mencionado também a existência das auditorias internas conduzidas em parceria com a Controladoria Geral do Município, entretanto, a implementação de uma frente de gestão de riscos, especificamente via GT da LGPD, ainda está em fase de planejamento, o que evidencia a necessidade de uma abordagem mais sistemática e integrada para a gestão de riscos. A produção de relatórios de auditoria ou monitoramento da conformidade digital, conforme relatado, é responsabilidade da Controladoria Geral do Município e não faz parte da rotina da DCAP, sendo esses relatórios elaborados apenas para processos considerados críticos, o que entra em conformidade com o relato da DCAP.

Finalmente, no que concerne à melhoria contínua, embora a DCAP não tenha um programa estruturado de *compliance* digital, a ASPE mencionou a utilização de metodologias como *benchmarking* e revisões de processos para promover melhorias. A capacitação sobre a LGPD também é continuamente atualizada, refletindo o compromisso da diretoria com a evolução constante das práticas de *compliance*. Esses pontos destacados pela ASPE fornecem uma visão abrangente da situação atual na DCAP, revelando tanto os progressos quanto às áreas que necessitam de aprimoramento na implementação de práticas de GRC e *compliance* digital.

4.2.3 Resultado das Gerências

Em relação à conformidade com a LGPD, todas as gerências relataram a implementação de procedimentos internos para garantir o cumprimento da legislação. Um ponto comum foi a realização de um mapeamento dos processos de trabalho em 2021, que incluiu a identificação de riscos e a adoção de medidas para mitigar possíveis problemas relacionados à proteção de dados, esse mapeamento foi acompanhado por capacitações e revisões dos processos, especialmente nas gerências GETED, GEVIF e GESFO, que relataram um esforço contínuo para alinhar suas operações às exigências da LGPD. Por outro lado, a GECEA, embora tenha mencionado a realização de treinamentos e orientações internas, não detalhou com a mesma profundidade as ações de mitigação de riscos, sugerindo que sua abordagem pode ter sido menos estruturada em comparação às outras gerências.

No que tange às metodologias de gestão, todas as gerências relataram conhecimento da metodologia PDCA, mas nenhuma a utiliza de forma estruturada para o acompanhamento de processos, em vez disso, adotam outras formas de monitoramento, principalmente através de indicadores de desempenho, como volume de demandas, prazos de execução e taxa de retrabalho. A GECEA e a GESFO, por exemplo, fazem uso de indicadores para acompanhar o andamento dos processos, enquanto a GETED e a GEVIF adotam uma abordagem de melhoria contínua baseada na análise de problemas e implementação de ações corretivas. Embora essas práticas não sigam formalmente o modelo PDCA, elas refletem uma gestão adaptativa e orientada por resultados, o que pode ser visto como uma aplicação prática dos princípios do PDCA, mesmo que não de forma explícita e metódica.

Entretanto, houveram algumas divergências significativas observadas nas entrevistas no que diz respeito ao conhecimento e aplicação das práticas de GRC. A GEVIF demonstrou um entendimento mais avançado dessas práticas, buscando garantir a uniformidade nos processos e implementando controles rigorosos para a gestão de riscos. Em contrapartida, as gerências GECEA, GETED e GESFO indicaram que não há um programa formal de *compliance* digital e que a terminologia GRC não é comumente utilizada. Apesar disso, essas gerências reconhecem que existem ações isoladas voltadas para a proteção de dados e a segurança digital, o que indica uma compreensão parcial e não sistematizada das práticas. Essa disparidade sugere que, enquanto algumas áreas da DCAP estão mais avançadas na implementação dessas práticas, outras ainda operam de maneira fragmentada e necessitam de maior integração e formalização. A gestão e atualização de riscos digitais é outro aspecto em

que as gerências mostraram variações já que a GECEA destacou que o mapeamento de riscos não foi atualizado para incluir novos processos, o que pode representar uma vulnerabilidade na gestão contínua de riscos da gerência, o que, em contrapartida, as gerências GETED, GEVIF e GESFO mencionaram que a gestão de riscos é uma prática discutida e atualizada regularmente, especialmente em reuniões de equipe, o que demonstra um compromisso mais ativo com a identificação e mitigação de riscos relacionados à LGPD. No que diz respeito a treinamentos específicos sobre GRC e *Compliance* Digital, as entrevistas revelaram uma lacuna significativa, pois, nenhuma das gerências relatou a realização de treinamentos focados nessas áreas, concentrando suas capacitações principalmente no entendimento da LGPD.

Por fim, todas as gerências confirmaram que não existe um relatório ou documento formal que descreva as políticas de governança adotadas, sendo essa ausência de documentação formalizada por toda DCAP uma oportunidade para padronizar e consolidar as práticas de governança dentro da diretoria. A padronização não só facilitaria o alinhamento entre as diferentes áreas, como também melhoraria a transparência e a responsabilidade nos processos, contribuindo para uma administração pública mais eficiente e conforme com as exigências legais.

Podemos concluir então que as entrevistas revelam que, enquanto há um esforço comum entre as gerências da DCAP para implementar práticas básicas de conformidade com a LGPD, as abordagens em relação ao GRC e à gestão de riscos digitais variam significativamente. A ausência de programas formais e a falta de atualização contínua em algumas áreas indicam a necessidade de uma abordagem mais integrada e sistemática para garantir a eficácia das práticas de governança e *compliance* dentro da DCAP em nível operacional. Esses achados sugerem que, embora a DCAP tenha feito progressos importantes, há um espaço considerável para melhorias, especialmente no que diz respeito à formalização e integração das práticas de GRC na diretoria.

5. CONCLUSÃO

A implementação do *compliance*, especialmente no contexto digital, é fundamental na administração pública direta, com destaque para a atuação da DCAP. O *compliance*, entendido como um conjunto de processos e práticas destinados a assegurar a conformidade com a legislação, desempenha um papel crucial na promoção da transparência e segurança na gestão de dados pessoais dos servidores públicos e a conformidade com a LGPD é particularmente importante nesse contexto, pois não só protege a privacidade dos indivíduos, mas também fortalece a confiança pública, um elemento essencial para a eficácia e responsabilidade da administração pública. Embora a DCAP tenha demonstrado avanços significativos na implementação do *compliance* digital, as entrevistas realizadas durante a pesquisa apontaram para a necessidade de melhorias tanto legislativas quanto estruturais para garantir a plena eficácia dessas práticas. A ausência de um programa formal de *compliance* digital e a falta de indicadores quantitativos de desempenho são evidências claras da necessidade de aprimoramentos contínuos e de uma maior formalização, a integração das práticas de *compliance* deve ser estendida a todos os níveis da administração pública, mostrando nesse sentido, a urgência o desenvolvimento de um marco regulatório municipal que exija a formalização dessas práticas em todos os órgãos públicos, promovendo uma abordagem mais sistemática e abrangente para a governança e o *compliance*.

Os resultados das entrevistas ainda revelam um comprometimento dos diferentes setores da DCAP com a conformidade legal, especialmente em relação à LGPD, e um esforço contínuo para a implementação de práticas de GRC. No entanto, também foram identificadas disparidades na aplicação, com algumas áreas mais avançadas do que outras, reforçando que a falta de formalização e a implementação fragmentada indicam a necessidade de uma abordagem mais integrada para garantir a eficácia das práticas de *compliance* em toda a diretoria. Em particular, a ausência de programas formais e de treinamentos específicos para GRC e *compliance* digital são lacunas que precisam ser abordadas para fortalecer a governança e mitigar os riscos no ambiente digital. Portanto, a consolidação de práticas robustas de *compliance* digital na administração pública não apenas promoverá a proteção dos dados pessoais, mas também contribuirá para o fortalecimento da cultura organizacional voltada para a responsabilidade e a transparência.

Sem a formalização de um programa de *compliance* digital e a ausência de relatórios ou documentos que detalham as políticas de governança adotadas, a gestão de riscos digitais na DCAP ainda está longe de atingir um nível de maturidade estruturado, devido às ações da

ASPE terem sido predominantemente reativas e dispersas, focadas em resolver problemas à medida que surgem, em vez de seguir um planejamento. O modelo ideal para uma solução de *compliance* digital que deveria incluir etapas como planejamento estratégico, definição clara de metas e objetivos, conscientização e treinamento dos envolvidos para o programa, comunicação efetiva, monitoramento constante, análise e avaliação da conformidade e da eficácia do sistema e finalizando com a implementação de ações corretivas. Mesmo após seis anos da publicação da LGPD e quatro anos desde sua entrada em vigor, a falta de planejamento adequado persiste, em grande parte devido à ausência de direcionamento claro da subsecretaria que supervisiona a DCAP, bem como à escassez de tempo e pessoal necessários para desenvolver e executar um planejamento eficaz.

Apesar dessas limitações, o programa improvisado apresenta algum grau de funcionalidade, evidenciando que, mesmo diante da escassez de recursos, a DCAP demonstra um compromisso com a conformidade e se esforça para treinar os servidores, tratar anomalias e garantir a adesão à LGPD. Para alcançar um nível adequado de governança e gestão de riscos digitais, é imprescindível que se estabeleçam um planejamento, recebam um maior investimento e seja concretizado um marco regulatório que defina claramente as diretrizes a serem seguidas. Essa formalização é crucial para a consolidação de práticas de *compliance* que não apenas protejam os dados pessoais, mas também fortaleçam uma cultura organizacional pautada pela responsabilidade, transparência e eficácia na administração pública.

BIBLIOGRAFIA

ALMEIDA, Luiz Eduardo. Governança Corporativa. In: CARVALHO, André Castro et al (coord.). **Manual de Compliance.** 4. ed. rev. atual. e aum. Rio de Janeiro: Editora Forense Ltda., 2024. cap. 1, p. 3-15. ISBN 978-65-5964-901-3.

ASSOCIAÇÃO BRASILEIRAS DE NORMAS TÉCNICAS. ISO 19600: **Sistema de gestão de compliance - Diretrizes.** Rio de janeiro, 2014.

AUSTRALIAN STANDARD. AS 3806: **Compliance programs**. Sydney, 2006. Disponível em: https://www.saiglobal.com/PDFTemp/Previews/OSH/as/as3000/3800/3806-2006.pdf. Acesso em: 9 abr. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia de Boas Práticas para Implementação da LGPD.** Brasília, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_lgpd_final.pdf. Acesso em: 19 jun. 2024.

ALVES, Gustavo Henrique Tardelli. **A Lei Anticorrupção e os parâmetros de avaliação dos programas de integridade no Brasil [Apresentação]**. 20 mar. 2019. Apresentação em PowerPoint. Disponível em: https://repositorio.cgu.gov.br/handle/1/32965. Acesso em: 9 abr. 2024.

BABESCO, Lucas. **O que é Marco Civil?** [S.l.]: Starti, 2021. 1 vídeo (6 min). Disponível em: https://www.youtube.com/watch?v=LrVoOdgr3S0. Acesso em: 22 mai. 2024.

BBC NEWS BRASIL. **Como a Cambridge Analytica analisou a personalidade de milhões de usuários no Facebook.** [S.l.]: BBC News Brasil, 2018. 1 vídeo (4 min). Disponível em: https://www.youtube.com/watch?v=x1SnHHby0wA. Acesso em: 22 mai. 2024.

BERTOCCELLI, Rodrigo de Pinho. Compliance. In: CARVALHO, André Castro et al (coord.). **Manual de Compliance.** 4. ed. rev. atual. e aum. Rio de Janeiro: Editora Forense Ltda., 2024. cap. 3, p. 37-47. ISBN 978-65-5964-901-3.

BLUM, Rita Peixoto Ferreira; MORAES, Hélio Ferreira. Lei Geral de Proteção de Dados - LGPD. In: CARVALHO, André Castro et al, (coord.). **Manual de Compliance.** 4. ed. rev.

atual. e aum. Rio de Janeiro: Editora Forense Ltda., 2024. cap. 26, p. 407-415. ISBN 978-65-5964-901-3.

BRASIL. **Lei nº 12.846, de 1º de agosto de 2013**. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. DOU, 2 ago. 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm. Acesso em: 9 abr. 2024.

BRASIL. **Lei nº 12.965, de 23º de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. DOU, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 22 mai. 2024.

BRASIL. **Lei nº13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). DOU, 15 ago 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 12 jun. 2024.

BRASIL. **Lei nº14.010, de 10 de junho de 2020**. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19). DOU, 12 jun. 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14010.htm. Acesso em: 18 jun. 2024.

CARARETTO, Vitor. **A Importância do Compliance nas Instituições Públicas.** Tribunal de Contas dos Municípios do Estado de Goiás, Goiânia, 06 out. 2021. Disponível em: https://www.tcm.go.gov.br/escolatcm/wp-content/uploads/2021/10/Artigo-A-importancia-do-compliance-nas-instituicoes-publicas.pdf. Acesso em: 18 jul. 2024.

CARVALHO, André Castro et al, (coord.). **Manual de Compliance**. 4. ed. rev. atual. e aum. Rio de Janeiro: Editora Forense Ltda., 2024. 656 p. ISBN 978-65-5964-901-3.

CONFESSORE, Nicholas. ***Cambridge Analytica and Facebook:*** *The Scandal and the Fallout So Far*. The New York Times, Nova Iorque, 4 abr. 2018. Disponível em: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. Acesso em: 23 mai. 2024.

EJCHEL, Maurício. Compliance & Política Interna de Empresa. **Jusbrasil**, São Paulo, 2015. Disponível em: https://www.jusbrasil.com.br/artigos/compliance-politica-interna-de-empresa/189818691. Acesso em: 9 abr. 2024.

FREED, Elizabeth Anne; CARVALHO, André Castro. General Data Protection Regulation - GDPR. In: CARVALHO, André Castro et al, (coord.). **Manual de Compliance.** 4. ed. rev. atual. e aum. Rio de Janeiro: Editora Forense Ltda., 2024. cap. 25, p. 393-405. ISBN 978-65-5964-901-3.

GODOY, Raimundo; BESSAS, Cláudia. **Formação de gestores**: Criando as bases da gestão. 2. ed. Belo Horizonte: Aquila, 2021. 208 p. ISBN 978-65-990007-7-5.

GRC: Governança, Riscos e Compliance. **Interact Solutions**. Lajeado, 2024. Disponível em: https://www.interactsolutions.com/solucao/grc-governanca-riscos-e-compliance/. Acesso em: 23 mai. 2024

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das Melhores Práticas de Governança Corporativa**. 6. ed. São Paulo: IBGC, 2023.

INSTITUTO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO NACIONAL. **História de Belo Horizonte (MG)**. Brasília, [2014]. Disponível em: http://portal.iphan.gov.br/pagina/detalhes/1832/. Acesso em: 18 jul. 2024.

PREFEITURA DE PENÁPOLIS. **O que é compliance no setor público e sua importância**. Penápolis, 24 set. 2021. Disponível em: https://www.penapolis.sp.gov.br/portal/0/galeria-de-fotos/230/o-que-e-compliance-no-setor-publico-e-sua-importancia/. Acesso em:18 jul. 2024.

META. ***Facebook Reports Second Quarter 2016 Results***, Menlo Park, 2016. Disponível em: https://investor.fb.com/investor-news/press-release-details/2016/Facebook-Reports-Second-Quarter-2016-Results/default.aspx. Acesso em: 23 mai. 2024.

NBR ISO 19600: Sistema de Gestão de Compliance. **I9 Consultoria, Auditoria e Treinamentos**, Santa Catarina, [201-]. Disponível em: https://www.i9ce.com.br/iso-19600-2/. Acesso em: 9 abr. 2024.

NEVES, Edmo Colnaghi; FIGUEIROA, Caio Cesar; FERNANDES, Nelson Ricardo. Gestão de Riscos. In: CARVALHO, André Castro et al (coord.). **Manual de Compliance**. 4. ed. rev. atual. e aum. Rio de Janeiro: Editora Forense Ltda., 2024. cap. 2, p. 17-35. ISBN 978-65-5964-901-3.

NEWTON, Casey. ***Facebook's Cambridge Analytica data scandal, explained***. [S.l]: The Verge, 2018. 1 vídeo (6 min). Disponível em: https://www.youtube.com/watch?v=VDR8qGmyEQg. Acesso em 23 mai. 2024.

OLIVEIRA, Rafael Carvalho Rezende; ACOCELLA, Jéssica. **Compliance na Administração Pública.** [s.l.]: Jusbrasil, 2019. Disponível em: https://www.jusbrasil.com.br/artigos/compliance-na-administracao-publica/738820873. Acesso em: 27 jun. 2024.

PAPP, Anna Carolina. **Em nome da internet**: os bastidores da construção coletiva do Marco Civil. São Paulo: Escola de Comunicações e Artes da Universidade de São Paulo, 2014. 147 p.

PROCURADORIA-GERAL DO DISTRITO FEDERAL. ***Governança Pública da PGDF***. Brasília, 2023. Cartilha Digital. Disponível em: https://pg.df.gov.br/wp-conteudo/uploads/2023/05/Nova-Cartilha-Governanca.pdf. Acesso em 27 jun. 2024.

UNIÃO EUROPEIA. **Convenção Europeia dos Direitos do Homem e Liberdades Fundamentais**. Roma: Conselho da Europa, 1950. 32 p. Disponível em: https://gddc.ministeriopublico.pt/sites/default/files/convention_por.pdf. Acesso em 24 mai. 2024.

UNIÃO EUROPEIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995**. Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. JO, 23 nov. 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX%3A31995L0046. Acesso em 24 mai. 2024

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a

Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). JO, 4 mai. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em 24 mai. 2024.

VENTURINI, Otavio. Programa de Compliance Digital. In: CARVALHO, André Castro et al (coord.). **Manual de Compliance.** 4. ed. rev. atual. e aum. Rio de Janeiro: Editora Forense Ltda., 2024. cap. 24, p. 373-391. ISBN 978-65-5964-901-3.

APÊNDICE A - Entrevistas através da LAI

ENTREVISTA I

DCAP - Diretoria Central de Administração de Pessoal

P: Quais são os procedimentos internos adotados para garantir a conformidade com a LGPD?

R: Capacitação, disponibilização de material para consulta e Fluxo interno envolvendo os Grupos de Trabalho da LGPD para saneamento de dúvidas e orientação da execução.

P: Vocês têm conhecimento das práticas de Governança, Riscos e *Compliance* (GRC)? Se sim, quais são aplicadas na diretoria?

R: Sim, temos conhecimento das práticas de GRC. Considerando se tratar de órgão público, as práticas de GRC vigentes estão muito alinhadas com as exigências legais, regulamentares e de boas práticas específicas do setor público.

Dentre os frameworks utilizados há normas do Tribunal de Contas do Estado, Lei de Responsabilidade Fiscal, práticas de auditorias internas e controle interno em conjunto com a Controladoria Geral do Município, o e-Social que é uma ferramenta importante para *compliance* nas prefeituras garantindo que as obrigações fiscais, previdenciárias e trabalhistas sejam cumpridas de acordo com as normas estabelecidas.

Quanto ao treinamento, atualmente, o foco é garantir a capacitação dos agentes públicos da DCAP. Paralelamente, a implementação de uma frente de Gestão de Riscos, via Grupo de Trabalho da LGPD está na fase de planejamento. Esta iniciativa incluirá o mapeamento de processos, a identificação e classificação de riscos (utilizando a ferramenta GUT) e a elaboração de planos de ação (adaptados do método 5W2H) para mitigar riscos classificados como graves.

P: Vocês têm conhecimento da metodologia PDCA (Plan, Do, Check and Action)? Em caso positivo, de que forma ele é implementado na diretoria? Em caso negativo, vocês utilizam alguma metodologia de planejamento? Caso não haja nenhuma metodologia, quais atividades são realizadas para fazer este acompanhamento?

R: Embora tenhamos conhecimento da metodologia PDCA (Plan, Do, Check, Act), não a utilizamos diretamente para o acompanhamento dos processos. Adotamos uma

abordagem própria para gerenciar projetos. Isso inclui a definição do escopo, o planejamento estratégico para execução e a elaboração de cronogramas. Além disso, implementamos planos de ação específicos para cada projeto, monitoramos pendências e gerenciamos cenários para controle de riscos. Nossa abordagem também inclui a integração de feedbacks contínuos e o registro de todo o processo para futuras referências e melhorias.

P: Qual a frequência de reuniões com os gestores da diretoria? Nessas reuniões de alinhamento são tratados questões acerca da LGPD ou de GRC?

R: .Reuniões entre Diretoria e Gerências: semanais. São tratados a Lei Geral de Proteção de Dados (LGPD), devido a relevância do tema.

P: Qual a frequência de reuniões com a liderança da Subsecretaria de Gestão de Pessoas (SUGESP)? Nestas reuniões são estruturados e alinhados os processos de GRC?

R: Não se aplica.

P: Existe algum relatório ou documento que descreva as políticas, normas e instrumentos de governança e *compliance* que devem ser adotadas pelas gerências?

R: Não existe.

P: Existe algum relatório de auditoria ou de monitoramento da conformidade digital? Em caso positivo, este relatório é apresentado para a liderança da SUGESP de quanto em quanto tempo?

R: Os relatórios de auditoria ou de monitoramento da conformidade digital existentes foram elaborados pela Controladoria Geral do Município. Não integram a rotina da diretoria. Foram elaborados visando alguns processos mais críticos.

P: Existe ou existiu alguma dificuldade em adaptar a diretoria para entrar em conformidade com a LGPD? Houve treinamento interno ou externo antes da lei entrar em vigor em setembro de 2020?

R: As ações da LGPD na DCAP iniciaram em 2019, em 2021 tivemos uma ações como mapeamento de processos, identificação de riscos e outras frentes, as capacitações com os agentes públicos da DCAP ocorrem desde 2023.

ENTREVISTA II

ASPE - Assessoria de Projetos Especiais

P: Há ou existe vislumbre de algum programa de *compliance* digital dentro da DCAP? Em caso positivo, quais são as principais fases de implementação e em qual fase a diretoria se encontra?

R: Não há um programa de *compliance* digital formal dentro da DCAP, no entanto a DCAP e suas unidades subordinadas adotam ações isoladas que incluem proteção de dados, privacidade, segurança, governança de TI e outras áreas que envolvem o uso de tecnologia e dados digitais para garantir que suas operações e uso de tecnologia estejam em conformidade com as leis, regulamentos, normas e diretrizes relacionadas ao ambiente digital. Como por exemplo:

- Treinamento e Conscientização relativos à LGPD
- Acessos dos sistema revisados observando às normas de proteção de dados e privacidade;
- Serviços de RH virtualizados e revisados para garantir a automatização, bem como a eficiência e ética na condução.

A Assessoria de Projetos Especiais, área que integra diretamente a DCAP, está conduzindo o Projeto LGPD, iniciado em 2020. Nosso papel é implementar medidas de instrução, orientação e monitoramento para assegurar a efetiva implementação da LGPD no ambiente da DCAP, garantindo o cumprimento integral da norma. Atualmente, a principal ação em andamento é a capacitação de todos os agentes públicos da DCAP em relação à LGPD, seus princípios, fundamentos e bases legais. Até o momento, atingimos a marca de 58% de agentes públicos capacitados.

P: Existem indicadores de desempenho para avaliar a eficácia do programa? Em caso positivo, quais são eles?

R: Não há indicadores para avaliar a eficácia do programa como um todo. No entanto, dentre as ações realizadas, a relativa ao Treinamento e Conscientização da LGPD possui um indicador qualitativo. Durante a capacitação, aplicamos estudos de caso com atividades voltadas para as áreas específicas que estão sendo capacitadas. Isso garante o entendimento do conteúdo apresentado e sua aplicabilidade nas rotinas diárias.

P: Existe alguma estrutura e/ou equipe responsável pelo programa?

R: Não há um programa de *compliance* digital formal dentro da DCAP, no entanto, há equipes responsáveis por conduzir as ações isoladas, conforme sua natureza.

Treinamento e Conscientização relativos à LGPD

A Assessoria de Projetos é a responsável pelo projeto, com uma equipe composta por três membros: uma encarregada da LGPD na SUGESP e duas agentes públicas com conhecimento aprofundado no tema, que conduzem as capacitações.

Acessos dos sistema revisados observando às normas de proteção de dados e privacidade;

Equipe da Assessoria de Tecnologia da Informação - ASTIN-GESP em conjunto com as áreas de negócio da DCAP.

Serviços de RH virtualizados e revisados para garantir a automatização, bem como a eficiência e ética na condução.

Equipe da Subsecretaria de Modernização da SMPOG - Secretaria Municipal de Planejamento, Orçamento e Gestão em conjunto com as áreas de negócio da DCAP.

P: Vocês têm conhecimento das práticas de Governança, Riscos e *Compliance* (GRC)? Se sim, quais são aplicadas nas gerências? Quais frameworks de GRC são utilizados pelo órgão?

R: Sim, temos conhecimento das práticas de GRC. Considerando se tratar de órgão público, as práticas de GRC vigentes estão muito alinhadas com as exigências legais, regulamentares e de boas práticas específicas do setor público. Dentre os frameworks utilizados há normas do Tribunal de Contas do Estado, Lei de Responsabilidade Fiscal, práticas de auditorias internas e controle interno em conjunto com a Controladoria Geral do Município, o e-Social que é uma ferramenta importante para *compliance* nas prefeituras garantindo que as obrigações fiscais, previdenciárias e trabalhistas sejam cumpridas de acordo com as normas estabelecidas. Quanto ao treinamento, atualmente, o foco é garantir a capacitação dos agentes públicos da DCAP. Paralelamente, a implementação de uma frente de Gestão de Riscos, via Grupo de Trabalho da LGPD está na fase de planejamento. Esta iniciativa incluirá o mapeamento de processos, a identificação e classificação de riscos (utilizando a ferramenta GUT) e a elaboração de planos de ação (adaptados do método 5W2H) para mitigar riscos classificados como graves.

P: Existem capacitações internas realizadas pela assessoria em relação às práticas de GRC e *compliance* digital? Em caso positivo, qual a frequência dessas capacitações?

R: As capacitações regulares e atualmente vigentes são as relacionadas à Lei Geral de Proteção de Dados. Elas são realizadas em rodízio entre todas as gerências e assessorias da DCAP, ocorrendo, em média, a cada quinze dias.

P: Existe a produção de relatórios de auditoria ou de monitoramento da conformidade digital?

R: Os relatórios de auditoria ou de monitoramento da conformidade digital existentes foram elaborados pela Controladoria Geral do Município. Não integram a rotina da diretoria. Foram elaborados visando alguns processos mais críticos.

P: Existem canais de denúncia na diretoria?

R: Não existe um canal de denúncia exclusivo da diretoria. As denúncias, se houver, são encaminhadas via TAG, Demanda da Ouvidoria, por e-mail ou ofício. Utilizados independentemente da natureza do questionamento. Quanto à LGPD, existe um fluxo para esclarecimento de dúvidas relacionadas à proteção de dados que eventualmente também pode ser utilizado para denúncia. O fluxo segue as seguintes instâncias, conforme a necessidade:

1º - Agente Público;

2º - Gestor Responsável;

3º - Encarregado Responsável;

4º - Grupo de Trabalho da LGPD da SMPOG (composto por encarregados designados de todas as subsecretarias);

5º - Comitê Municipal de Proteção de Dados Pessoais (CMPDP).

P: Vocês utilizam alguma metodologia para realizar melhorias contínuas no programa de *compliance* digital? Se sim, qual é a metodologia ou quais são os processos utilizados para realizar estas melhorias?

R: No contexto de um programa de *compliance* digital, as metodologias de melhoria contínua são essenciais para garantir que a diretoria esteja sempre em conformidade com as regulamentações, que os riscos sejam adequadamente gerenciados e que as melhores práticas sejam incorporadas no dia a dia da operação. Não há um programa de *compliance* estruturado, mas há metodologias para realizar melhorias contínuas como *benchmarking*, pequenas revisões de processos e treinamento contínuo. Quanto à capacitação da LGPD, a equipe

responsável acompanha continuamente as mudanças e a evolução da LGPD, atualizando as capacitações sempre que necessário.

P: Foi realizado algum mapeamento de processos comuns e identificação de possíveis riscos relacionados a LGPD com as gerências da DCAP?

R: Sim, um levantamento de processos, baseado nas Hipóteses de Tratamento, foi realizado em 2021, incluindo a identificação de riscos. Atualmente, estamos planejando a revisão do levantamento de processos, utilizando uma estratégia diferenciada.

P: Existe alguma auditoria interna em relação aos processos da DCAP? Já foram realizadas auditorias externas independentes?

R: Há auditoria interna em relação aos processos da DCAP conduzida pela Controladoria Geral do Município para alguns processos mais críticos. A DCAP ainda está na fase inicial para implementação de forma autônoma de controles internos de processos críticos da diretoria, como por exemplo: compra e pagamento de benefícios; processos de pagamento da folha.

ENTREVISTA III

GECEA - Gerência de Central de Atendimento

P: Quais são os procedimentos internos adotados para garantir a conformidade com a LGPD?

R: Treinamentos com servidores e orientações internas sobre a aplicação da Lei nas atividades da área, classificação de riscos e possíveis ações de mitigação ou correção.

P: Vocês têm conhecimento das práticas de Governança, Riscos e *Compliance* (GRC)? Se sim, quais são aplicadas no setor?

R: Não temos conhecimento.

P: Vocês têm conhecimento da metodologia PDCA (Plan, Do, Check and Action)? Em caso positivo, de que forma ele é implementado na gerência? Em caso negativo, vocês

utilizam alguma metodologia de acompanhamento de processos? Caso não haja nenhuma metodologia, quais atividades são realizadas para fazer este acompanhamento?

R: Temos conhecimento da metodologia, mas não aplicamos no setor. Não é aplicada nenhuma outra metodologia. Fazemos o acompanhamento através de indicadores (quantitativo de demandas, prazos de execução, percentual de erros). Os problemas identificados são tratados e caso necessário, implantamos novos procedimentos de trabalho.

P: Existe dentro da gerência algum processo de identificação de possíveis riscos relacionados a LGPD? Como é realizada a gestão de riscos digitais?

R: O mapeamento de riscos foi realizado em 2021, porém não foi atualizado para inclusão e atualização de novos processos.

P: Qual a relação entre os servidores e a gerência para identificação e correção dos riscos relacionados a LGPD

R: Os servidores que detectarem riscos podem reportá-los ao gerente ou coordenador.

P: Caso haja, qual a frequência de treinamentos relacionados às práticas de GRC e de *Compliance* Digital com os servidores?

R: Não realizamos, até o momento, treinamento sobre GRC e *Compliance* Digital.

P: Existe algum relatório ou documento que descreva as políticas de governança adotadas pela gerência?

R: Não existe.

ENTREVISTA IV

GETED - Gerência de Gestão de Direitos e Benefícios

P: Quais são os procedimentos internos adotados para garantir a conformidade com a LGPD?

R: Capacitação, disponibilização de material para consulta e Fluxo interno envolvendo os Grupos de Trabalho da LGPD para saneamento de dúvidas e orientação da execução. Após capacitação dos agentes públicos, fizemos a revisão dos nossos processos de trabalho a fim de mitigar os riscos existentes e evitar a ocorrência de riscos futuros.

P: Vocês têm conhecimento das práticas de Governança, Riscos e *Compliance* (GRC)? Se sim, quais são aplicadas no setor?

R: Não há um programa de *compliance* digital formal dentro da DCAP (A terminologia GRC não é comumentemente utilizada), no entanto a DCAP e suas unidades subordinadas adotam ações isoladas que incluem proteção de dados, privacidade, segurança e outras áreas que envolvem o uso de tecnologia e dados digitais para garantir que suas operações e uso de tecnologia estejam em conformidade com as leis, regulamentos, normas e diretrizes relacionadas ao ambiente digital. Não temos conhecimento.

P: Vocês têm conhecimento da metodologia PDCA (Plan, Do, Check and Action)? Em caso positivo, de que forma ele é implementado na gerência? Em caso negativo, vocês utilizam alguma metodologia de acompanhamento de processos? Caso não haja nenhuma metodologia, quais atividades são realizadas para fazer este acompanhamento?

R: Não utilizamos uma ferramenta específica, mas fazemos o acompanhamento de todos os processos com a análise de indicadores como volume de demandas, prazo de atendimento e ocorrência de retrabalho. Diante da identificação de algum problema e após a identificação da causa, implementamos as melhorias possíveis.

P: Existe dentro da gerência algum processo de identificação de possíveis riscos relacionados a LGPD? Como é realizada a gestão de riscos digitais?

R: Sim, fizemos o levantamento dos riscos de todos os processos em 2021.

P: Qual a relação entre os servidores e a gerência para identificação e correção dos riscos relacionados a LGPD

R: Periodicamente tratamos do assunto em reuniões de equipe e quando identificadas dúvidas, encaminhamos para orientação da ASPE (Assessoria de Projetos Especiais).

P: Caso haja, qual a frequência de treinamentos relacionados às práticas de GRC e de *Compliance* Digital com os servidores?

R: .Não se aplica

P: Existe algum relatório ou documento que descreva as políticas de governança adotadas pela gerência?

R: Não existe.

ENTREVISTA V

GEVIF - Gerência de Gestão de Ingresso e da Vida Funcional

P: Quais são os procedimentos internos adotados para garantir a conformidade com a LGPD?

R: Foi realizado um levantamento e uma análise de todos os processos de trabalho da Gerência, avaliando os riscos e ações necessárias para ajustes conforme a LGPD.

P: Vocês têm conhecimento das práticas de Governança, Riscos e *Compliance* (GRC)? Se sim, quais são aplicadas no setor?

R: Sim, estamos buscando garantir a uniformidade dos processos da GEVIF, através de um controle mais de perto. Além disso, buscamos sempre realizar alinhamentos com toda a equipe, de modo a não criar interpretações distintas para a mesma ação. Em relação à gestão de riscos, buscamos sempre avaliar os projetos e criar planos de ação de modo a prevenir incidentes e suavizar os riscos.

P: Vocês têm conhecimento da metodologia PDCA (Plan, Do, Check and Action)? Em caso positivo, de que forma ele é implementado na gerência? Em caso negativo, vocês utilizam alguma metodologia de acompanhamento de processos? Caso não haja nenhuma metodologia, quais atividades são realizadas para fazer este acompanhamento?

R: Não utilizamos necessariamente o PDCA (Plan, Do, Check and Action), entretanto, fazemos um acompanhamento de perto, desde o planejamento, levantamento de riscos, principais problemas, criação de plano de ação, cronogramas, de modo que o projeto seja executado da melhor forma possível até a sua implementação.

P: Existe dentro da gerência algum processo de identificação de possíveis riscos relacionados a LGPD? Como é realizada a gestão de riscos digitais?

R: Sim, fizemos o levantamento dos riscos de todos os processos em 2021.

P: Qual a relação entre os servidores e a gerência para identificação e correção dos riscos relacionados a LGPD

R: As dúvidas e possíveis riscos identificados são levantados nas equipes para busca de orientações junto à ASPE (Assessoria de Projetos Especiais).

P: Caso haja, qual a frequência de treinamentos relacionados às práticas de GRC e de *Compliance* Digital com os servidores?

R: Não se aplica.

P: Existe algum relatório ou documento que descreva as políticas de governança adotadas pela gerência?

R: Não existe.

ENTREVISTA VI

GESFO - Gerência de Gestão da Folha de Pagamento

P: Quais são os procedimentos internos adotados para garantir a conformidade com a LGPD?

R: Capacitação, disponibilização de material para consulta e Fluxo interno envolvendo os Grupos de Trabalho da LGPD para saneamento de dúvidas e orientação da execução.

Em 2021, realizamos o mapeamento dos processos da Gerência relacionados ao tratamento de dados. Desde então, com a disseminação de informações sobre o tema entre as equipes, temos buscado alinhar todos os processos da gerência à Lei Geral de Proteção de Dados (LGPD).

P: Vocês têm conhecimento das práticas de Governança, Riscos e *Compliance* (GRC)? Se sim, quais são aplicadas no setor?

R: Não há um programa de *compliance* digital formal dentro da DCAP (A terminologia GRC não é comumentemente utilizada), no entanto a DCAP e suas unidades subordinadas adotam ações isoladas que incluem proteção de dados, privacidade, segurança e outras áreas que envolvem o uso de tecnologia e dados digitais para garantir que suas operações e uso de tecnologia estejam em conformidade com as leis, regulamentos, normas e diretrizes relacionadas ao ambiente digital. Não temos conhecimento.

P: Vocês têm conhecimento da metodologia PDCA (Plan, Do, Check and Action)? Em caso positivo, de que forma ele é implementado na gerência? Em caso negativo, vocês utilizam alguma metodologia de acompanhamento de processos? Caso não haja nenhuma metodologia, quais atividades são realizadas para fazer este acompanhamento?

R: Embora tenhamos conhecimento da metodologia PDCA, não a utilizamos como ferramenta específica. Nossa gestão de riscos concentra-se principalmente no levantamento e acompanhamento dos principais gaps, buscando mitigar problemas na execução dos processos.

P: Existe dentro da gerência algum processo de identificação de possíveis riscos relacionados a LGPD? Como é realizada a gestão de riscos digitais?

R: Sim, o levantamento dos riscos de todos os processos foi realizado em 2021.

P: Qual a relação entre os servidores e a gerência para identificação e correção dos riscos relacionados a LGPD?

R: Os servidores que identificarem riscos relacionados à LGPD podem remetê-los à chefia imediata, que buscará orientações junto à ASPE.

P: Caso haja, qual a frequência de treinamentos relacionados às práticas de GRC e de *Compliance* Digital com os servidores?

R: Até o momento, não realizamos nenhum treinamento sobre o tema.

P: Existe algum relatório ou documento que descreva as políticas de governança adotadas pela gerência?

R: Não existe.