Diario Oficial - DODP
Publicada 09/10/2024

Rua dos Guajajáras, 1707 - Bairro Barro Preto - CEP 30180-099 - Belo Horizonte - MG - www.defensoria.mg.def.br

RESOLUÇÃO

Nº 2970/2024

Dispõe sobre a Política de Segurança da Informação da Defensoria Pública do Estado de Minas Gerais.

A DEFENSORA PÚBLICA-GERAL DO ESTADO DE MINAS GERAIS, no uso de suas atribuições estabelecidas no art. 9º da Lei Complementar nº 65, de 16 de janeiro de 2003, e tendo em vista o disposto na Lei Federal nº 13.709, de 14 de agosto de 2018, **RESOLVE**:

Art. 1º – Fica aprovada a Política de Segurança da Informação da Defensoria Pública do Estado de Minas Gerais, nos termos do Anexo.

Art. 2º – Esta Resolução entra em vigor na data de sua publicação.

Belo Horizonte, 08 de outubro de 2024.

Raquel Gomes de Sousa da Costa Dias

Defensora Pública-Geral do Estado de Minas Gerais

ANEXO

(a que se refere o art. 1º da Resolução nº 2970/2024)

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA DEFENSORIA PÚBLICA DO ESTADO DE MINAS GERAIS (DPMG)

1. OBJETIVO

1.1 O objetivo da Política de Segurança da Informação é estabelecer diretrizes aos usuários de informações e dados sob cuja responsabilidade a Defensoria Pública do Estado de Minas Gerais (DPMG) detenha e, ainda, determinar padrões de comportamento relacionados à segurança, privacidade e proteção de dados pessoais e estratégicos, bem como às demais informações necessárias ao desempenho de suas atividades.

1.2 Esta política constitui também uma declaração formal da DPMG sobre o seu compromisso com a privacidade e proteção de dados pessoais e estratégicos, bem como de outras informações em sua posse, propriedade ou que estejam sob sua responsabilidade.

2. PRINCÍPIOS

2.1 Dentre os princípios em que se baseiam esta política, destaca-se a garantia da qualidade dos dados e informações da DPMG quanto aos seguintes aspectos:

2.1.1 Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas

autorizadas;

2.1.2 Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;

2.1.3 Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário;

2.1.4 Autenticidade: garantia de que as informações sejam verídicas, pois, por meio da autenticação, é possível confirmar a identidade da pessoa ou entidade que presta a informação;

2.1.5 Não repúdio: garantia de que o autor não irá negar qualquer ação relacionada aos arquivos e/ou documentos, desde sua criação, quanto à alteração, deleção ou assinatura.

3. APLICAÇÃO

3.1 As diretrizes estabelecidas nesta Política deverão ser seguidas por todos os usuários de dados e informações cuja propriedade seja da DPMG, bem como àquelas que estiverem sob sua responsabilidade.

4. REFERÊNCIAS

4.1 ABNT NBR ISO/IEC 27001:2013*;*

4.2 ABNT NBR ISO/IEC 27002:2005;

4.3 LEI Nº 12.965/2014 – Marco Civil da Internet;

4.4 LEI Nº 13.709/18 – LEI GERAL DE PROTEÇÃO DE DADOS(LGPD);

4.5 Condutas, Normas e Procedimentos internos da DPMG, aperfeiçoados constantemente, aprovados e disponibilizados a todos os usuários.

5. DEFINIÇÕES

5.1 Para fins deste documento devem ser consideradas as seguintes definições:

5.1.1 Administradores: Defensor Público-Geral, Subdefensor Público-Geral, Corregedor-Geral, Coordenadores, Superintendentes e Diretores.

5.1.2 Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

5.1.3 Ativos: entende-se como qualquer componente (seja humano, tecnológico, software etc.) que sustente um ou mais processos de uma unidade ou área de negócio;

5.1.4 Autoridade Nacional de Proteção de Dados (ANPD): entidade da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional;

5.1.5 Comitê Gestor de Segurança da Informação (CGSI): comitê multidisciplinar responsável por definir e apoiar estratégias necessárias à implantação e manutenção desta Política de Segurança da Informação e dar outras providências com relação a temática;

5.1.6 Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

5.1.7 Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

5.1.8 Dado pessoal: toda informação relacionada à pessoa natural identificada ou identificável;

5.1.9 Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião

política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

5.1.10 Documento Corporativos: trata-se de registro formal produzido dentro de uma organização, incluindo a administração pública. Esse documento é essencial para o funcionamento eficiente e transparente da instituição;

5.1.11 Encarregado de Dados – *Data Protection Officer* (DPO): trata-se do encarregado pela proteção de dados que deverá ser indicado pelo controlador para atuar como canal de comunicação entre este, os titulares dos dados pessoais e a ANPD, dentre outras atribuições previstas na LGPD;

5.1.12 Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

5.1.13 Incidente de Segurança: quebra de segurança que leva a acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração ou qualquer forma de tratamento inadequado ou ilícito que possa causar risco ou dano relevante aos titulares;

5.1.14 Informação: conjunto organizado de dados que proporciona decisões otimizadas e estratégicas sobre como resolver problemas, tomar decisões e mudar a direção de um negócio ou de uma vida;

5.1.15 Lei nº 13.709/18 - Lei Geral de Proteção de dados (LGPD): criada para regulamentar o tratamento de dados pessoais;

O diploma legal dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, sendo aplicada a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados;

5.1.16 Responsável pela Segurança da Informação – *Information Security Officer*: responsável por organizar regras para salvaguardar a informação gerida e utilizada pela instituição;

5.1.17 Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

5.1.18 Tratamento: toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

5.1.19 Uso compartilhado de dados: tornar dados disponíveis para várias aplicações, usuários ou organizações através de comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

5.1.20 Usuário: qualquer pessoa física ou jurídica, seja servidora, contratada ou cedida, prestadora de serviço ou partícipe, que atue dentro ou fora da DPMG e que trate, colete, processe, armazene ou transmita dados ou informações da Instituição, ou ainda que utilize ou se beneficie dos serviços da DPMG, incluindo assistidos e visitantes.

6. VALORES

6.1 O valor da informação varia conforme o indivíduo interessado, as necessidades e o contexto em que ela é produzida e compartilhada, sendo que uma informação pode ser altamente relevante para um indivíduo e, ao mesmo tempo, não ter significado nenhum para outro.

6.2 A Segurança da Informação está relacionada diretamente com a proteção das informações, no sentido de preservar o valor que elas representam aos indivíduos interessados.

6.3 Os casos omissos ou excepcionais, considerando o contexto desta Política de Segurança da Informação, serão analisados pelo Comitê Gestor da Segurança da Informação, preservada a competência dos órgãos da Administração Superior da DPMG.

7. CLASSIFICAÇÃO DA INFORMAÇÃO

7.1 Toda a informação de propriedade da DPMG, ou sob sua responsabilidade, deve ser classificada para possibilitar o controle adequado, devendo ser utilizados os níveis de classificação adiante discriminados.

7.1.1 Confidencial: são as informações protegidas por lei e por órgãos reguladores, cláusulas de confidencialidade, de caráter pessoal dos titulares, do quadro funcional e as informações estratégicas para os interesses e atuação institucional da DPMG. A divulgação não autorizada dessas informações pode causar impactos de ordem financeira, legal, normativa, contratual, operacional, estratégica, de imagem ou ainda danos à reputação, sanções administrativas, cíveis ou criminais, sendo que essas informações são sempre restritas a um grupo específico de pessoas;

7.1.2 Restrita: informações organizacionais, técnicas, comerciais, cuja utilização é restrita a determinados grupos, áreas, funções ou cargos;

7.1.3 Interna: informações de interesse e uso exclusivamente interno, que não devem ser expostas publicamente;

7.1.4 Pública: informações que podem ser divulgadas para público interno e externo à DPMG, sem restrições, pois não geram impacto negativo.

7.2 Na presente classificação são consideradas as informações pertencentes aos usuários, manipuladas ou armazenadas nos meios pelos quais a DPMG detém controle administrativo, físico, lógico e responsabilidade legal.

7.3 Considera-se propriedade da DPMG todas as criações, códigos ou procedimentos desenvolvidos por qualquer defensor, servidor, colaborador, estagiário, ou prestador de serviço de qualquer natureza durante todo o seu vínculo com a instituição, ou em razão dele.

8. DIRETRIZES DE SEGURANÇA E PROTEÇÃO DE DADOS E INFORMAÇÕES

8.1 A segurança, proteção e privacidade de dados e informações da DPMG, ou sob sua responsabilidade, são consideradas fatores primordiais nas atividades da instituição.

8.2 É responsabilidade dos usuários assegurar a integridade e disponibilidade das informações da DPMG.

8.2.1 A responsabilidade pela segurança e proteção de dados e informações pelos usuários estende-se pelo período mínimo de 24 (vinte e quatro) meses após seu eventual desligamento ou cessação da prestação de serviços;

8.2.2 Os usuários devem assumir uma postura proativa, no que diz respeito à proteção das informações da DPMG e devem estar atentos a ameaças externas, bem como a fraudes e acessos

indevidos a sistemas de informação sob responsabilidade da instituição;

8.2.3 Informações confidenciais e internas não devem e não podem ser expostas publicamente;

8.2.4 As informações recebidas pela DPMG devem ser tratadas e armazenadas de forma segura e íntegra;

8.2.5 Para as informações em meio digital, devem ser feitos *backups* diretamente pelo prestador de serviços contratado pela DPMG, sendo que uma cópia deles deve ser armazenada semanalmente, utilizando mecanismos de segurança tecnológica e administrativa, suficientes para proteger todos os dados e informações armazenadas, nos termos estabelecidos na LGPD e demais leis pertinentes e vigentes;

8.2.6 Todos os dados inseridos nos sistemas informatizados utilizados pela DPMG devem ser protegidos por meio de rotinas sistemáticas, documentadas, com cópia de segurança, devendo ser submetidos a testes periódicos de recuperação, utilizando mecanismos de segurança tecnológica e administrativa suficientes para proteção desses dados e das informações armazenadas, nos termos estabelecidos na LGPD e demais leis pertinentes e vigentes;

8.2.7 Documentos impressos e arquivos contendo dados pessoais e/ou informações confidenciais e internas devem ser armazenados e descartados de forma segura, conforme normas internas da DPMG;

8.2.8 Não é permitido envio de informações ou documento corporativos para e-mails pessoais de usuários nem de terceiros.

8.3 De acordo com as regras de permissão de acesso, para aqueles que não tiverem autorização definida, as cópias de qualquer informação ou documento corporativo em dispositivos removíveis, tais como pen drive, HD externo e itens da mesma categoria, deverão ser previamente autorizadas pelo responsável pela Segurança da Informação.

8.4 Os *softwares* corporativos poderão ser utilizados no ambiente da DPMG, somente após homologação do responsável pela Segurança da Informação, podendo-se consultar o encarregado de dados, caso aplicável.

8.5 Os dados que necessitam de compartilhamento devem ser alocados nos servidores apropriados, com atenção às devidas permissões de acesso.

9. TRATAMENTO DE DADOS PESSOAIS E OBSERVÂNCIA À LGPD

9.1 Todas as atividades da DPMG envolvendo tratamento de dados e informações pessoais devem estar em conformidade com a LGPD, demais leis pertinentes e atos normativos internos que legitimem o tratamento de dados pessoais e garantem direitos aos seus titulares.

9.2 As atividades de tratamento, armazenamento e transferência de dados pessoais e/ou sensíveis, de qualquer natureza, nas operações da DPMG, devem observar os princípios e diretrizes apresentadas a seguir:

9.2.1 Os dados e informações pessoais tratados pela DPMG devem ser coletados de forma ética, com o conhecimento do titular, para propósitos específicos;

9.2.2 Devem ser tomadas medidas razoáveis para garantir que os dados dos titulares sejam tratados dentro da necessidade e apoiados nas bases legais, conforme a LGPD;

9.2.3 Deve-se minimizar os dados, limitados ao que é necessário em relação aos propósitos para os quais são processados, utilizando-se o *Framework "Privacy by Design"*. Caso isso não seja possível, tal impossibilidade deve ser justificada, conforme inciso VIII do art. 52 da LGPD;

9.2.4 Deve-se garantir a segurança dos dados pessoais tratados pela DPMG e a comunicação dos eventuais incidentes de segurança da informação à ANPD, sendo que, dependendo da gravidade do

incidente, o titular dos dados também deverá ser comunicado;

9.2.5 Devem ser mantidos todos os dados coletados (nas formas e canais cabíveis) enquanto o cadastro do titular estiver ativo, e conforme seja necessário para as atividades da DPMG, observando-se o período de retenção estabelecido em contrato e instrumentos congêneres, lei e normativos que suportem a retenção;

9.2.6 O descarte de dados pessoais deve ser feito com segurança, de forma que os dados sejam irrecuperáveis;

9.2.7 O armazenamento deve utilizar bancos de dados da DPMG ou, "nuvem" (*Cloud Computing*).

9.3 A Superintendência de Tecnologia da Informação – STI deve avaliar, monitorar e gerenciar as permissões de usuários, administradores e desenvolvedores, considerando a necessidade de acesso a cada Sistema de Gestão de Banco de Dados, aplicando essas permissões de acesso de maneira adequada aos serviços realizados.

9.4 Os prestadores de serviços deverão estar em conformidade com a legislação de proteção de dados vigente e cumprir as cláusulas contratuais estabelecidas, adotando procedimentos de segurança para proteger a confidencialidade, segurança e integridade dos dados.

9.5 Qualquer informação ou documento corporativo somente poderá ser armazenado em um banco de dados homologado ou ativo da DPMG.

9.6 O compartilhamento de dados pessoais ou sensíveis com órgão ou instituições, públicas ou privadas deve ser avaliado pelo Encarregada de Dados.

10. CONTROLES DE ACESSO (FÍSICO E LÓGICO)

10.1 Os dados e informações devem ser acessados somente por pessoas autorizadas e capacitadas, visando o uso adequado desse acesso. Além disso, o acesso deve ser específico e restrito à necessidade de execução da atividade das pessoas que o executam.

10.2 O acesso lógico aos sistemas computacionais disponibilizados pela DPMG deve ser autorizado e controlado, garantindo sua rastreabilidade e efetividade, salvo quando se tratar de acesso a conteúdo de caráter público.

10.3 O usuário deverá possuir chave e senha previamente cadastrados, sendo esta pessoal e intransferível, e proibida a utilização de códigos de acesso genéricos ou comunitários, exceto quando devidamente autorizado pela STI, por meio de registro de chamado.

10.4 Senhas, chaves e outros recursos de caráter pessoal são considerados intransferíveis e não podem ser compartilhados e divulgados, exceto quando devidamente autorizados pela STI, por meio de registro de chamado.

10.4.1 Nenhum usuário deve ter, por padrão, acesso de "Administrador" em estações de trabalho e/ou notebooks. Caso seja necessário tal acesso, deverá ser feita uma solicitação à área responsável, por meio de abertura de chamado na STI, com a devida finalidade destacada para avaliação, podendo tal acesso ser negado.

10.5 Não é permitido o compartilhamento de dados pessoais e dados pessoais sensíveis com órgão ou instituições, públicas ou privadas, dentro e fora das dependências da DPMG, por qualquer meio de comunicação, exceto para a realização da atividade pública a cargo da Instituição, por meio de termos, contratos ou instrumentos congêneres, devidamente assinados, destacando claramente a finalidade específica na qual se insere a aludida atividade, salvo por determinação legal.

10.6 As informações e dados confidenciais constantes nos cadastros da DPMG podem ser disponibilizados às empresas contratadas para prestação de serviços, sendo exigido de tais organizações o cumprimento desta Política de Segurança da Informação e diretivas de segurança e privacidade de dados.

10.7 Para acesso às dependências da DPMG deve ser realizado controle para identificação e registro de usuários e visitantes, visando a rastreabilidade. E adicionalmente é recomendado, sempre que possível, que a DPMG acompanhe o visitante durante o seu período de permanência nas dependências da instituição.

10.8 O acesso físico aos Servidores e "*Appliances*" deve ser previamente autorizado e monitorado pela STI.

10.8.1 Quando em trabalho de auditoria, os auditores são autorizados a terem acesso, sempre acompanhados pela STI;

10.8.2 Em caso de prestação de serviços de terceiros a serem realizados no ambiente dos Servidores e "*Appliances*", faz-se necessário o acompanhamento e aprovação da STI, sendo qualquer incidente tipo de incidente reportado ao Encarregado de Dados;

10.8.3 Todo acesso ao ambiente dos Servidores e "*Appliances*" deve ser registrado de forma manual ou automatizada, em sistema de controle de acesso;

10.8.4 Os registros de acesso ao ambiente dos Servidores e "*Appliances*" devem ser armazenados em local seguro e mantidos em histórico por, pelo menos, 01 (um) ano.

10.9 É proibida a utilização de câmeras fotográficas ou filmadoras, sejam elas acopladas ao smartphone ou não, para fotografar ou filmar áreas internas, pessoas, dados e informações classificadas como confidenciais, restritas e internas para divulgação ou compartilhamento com terceiros, em qualquer uma das dependências da DPMG, salvo em situações inerentes à rotina de trabalho, confraternizações oficiais, previamente autorizadas, situações de emergência em que o uso se faça necessário ou por disciplina permissiva legal.

11. MONITORAMENTO DE SEGURANÇA

11.1 Visando garantir as regras de segurança, a DPMG deverá monitorar periodicamente seus procedimentos internos e sistemas de informação, com as ações apresentadas a seguir:

11.1.1 Implantação de sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou *wireless* e componentes da rede, desde que preservados o conteúdo das comunicações e o sigilo profissional;

11.1.2 Informações geradas por sistemas de monitoramento e *logs*, poderão ser usadas para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

11.1.3 Realização de inspeções físicas às máquinas da DPMG;

11.1.4 Instalação de sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações, do ambiente de infraestrutura e dos perímetros de acesso;

11.1.5 Execução de testes de vulnerabilidade periódicos, com frequência mínima semestral.

11.2 O armazenamento de informações pessoais e privadas nos equipamentos da DPMG, por meio físicos, em servidor local ou em nuvem, não confere a particularização e segurança individualizada destes dados.

12. COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO – CGSI

12.1 O CGSI, grupo multidisciplinar e com responsabilidade de definir e apoiar estratégias necessárias à implantação e manutenção da Segurança da Informação na DPMG, será instituído por resolução da Defensoria Pública-Geral, conforme preceitua a Deliberação nº 397/2024 do Conselho Superior.

13. AUTORIDADE E RESPONSABILIDADE

1.

RESPONSÁVEIS	DESCRIÇÃO
Superintendência de Tecnologia da Informação - STI	·Fazer parte do CGSI e auxiliar no processo de implementação, revisão e atualização desta Política quando necessário.
Superintendências que cuidam de Gestão de Pessoas, Segurança da Informação e Escola Superior.	·Prover treinamentos a todos os envolvidos nesta Política; ·Gerenciar a divulgação e as diretrizes estabelecidas nesta Política, através dos meios oficiais de comunicação da DPMG.
Defensoria Pública-Geral	·Aprovar as normas, cumprir e disseminar suas regras e diretrizes.
Comitê Gestor de Segurança da Informação - CGSI	·Cumprir suas responsabilidades definidas nesta Política, conforme o que preceitua a Deliberação 397/2024 e a resolução que trata sobre o comitê.
Gestores de pessoas e/ou processos	·Atribuir aos usuários, na fase de contratação e de formalização dos contratos, de prestação de serviço ou individuais de trabalho, a responsabilidade do cumprimento desta Política;
Usuários	·Observar as regras e diretrizes desta Política, zelando continuamente pela proteção de dados e informações contra acesso, modificação, destruição ou divulgação não autorizada; ·Comunicar aos canais oficiais de Privacidade e Proteção de Dados, Ouvidoria e Corregedoria, quaisquer atos ou suspeitas de violação às legislações e normas internas.

14. COMUNICAÇÃO E TREINAMENTOS

14.1 As regras e diretrizes definidas nesta Política serão divulgadas, por meios oficiais de divulgação da DPMG, de maneira que seu conteúdo possa ser consultado a qualquer momento.

14.2 Os treinamentos serão realizados com apoio da Escola Superior, da área de Privacidade e Proteção de Dados Pessoais, da Superintendência de Gestão de Pessoas e Saúde Ocupacional, Coordenadoria de Estágio e Serviço Voluntário, STI e pela área responsável pela Segurança da Informação.

14.3 Cabe a cada usuário manter-se atualizado em relação a esta Política e às normas relacionadas, buscando orientação junto ao Encarregado de Dados e ao responsável pela Segurança da Informação, sempre que não estiver seguro quanto à aquisição, uso ou descarte de informações.

15. VIOLAÇÃO DE SEGURANÇA E PRIVACIDADE

15.1 No caso de uma violação de segurança e/ou privacidade que leve à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a dados pessoais e informações estratégicas, a DPMG deverá prontamente avaliar o risco para os direitos e liberdades das pessoas e, se apropriado, informar essa violação

à autoridade competente e/ou ao titular.

15.2 O incidente deve ser registrado manualmente ou por meio de *software* que possibilite a Gestão e Tratativa de Incidentes (recomendado padrão ITIL) e, de forma devida, ficar disponível para consulta da autoridade.

15.3 Será de inteira responsabilidade de cada usuário todo prejuízo ou dano que vier a sofrer em decorrência da não observância das diretrizes e normas estabelecidas nesta Política.

15.4 Os usuários poderão ser responsabilizados pelos prejuízos ou danos que causarem à DPMG ou a terceiros, em decorrência da não observância das diretrizes e normas estabelecidas nesta Política.

16. DEVERES E RESPONSABILIDADES

16.1 É dever dos usuários da DPMG zelar pelo cumprimento das normas estabelecidas nesta política. Caso identifiquem qualquer desvio de conduta ou infração a qualquer política e/ou norma, isso deve ser comunicado imediatamente pelos canais oficiais de Privacidade e Proteção de Dados, Ouvidoria e Corregedoria.

16.2 As informações que descreverem mentiras, ameaças ou inverdades que possam prejudicar a reputação de outra pessoa interna ou externa estarão sujeitas às medidas disciplinares, administrativas e judiciais cabíveis.

17. DISPOSIÇÕES GERAIS

17.1 É competência de o CGSI aprovar as revisões ou alterações desta Política, anualmente ou sempre que se fizer necessário, resguardadas as competências dos órgãos da Administração Superior.

18. CONTROLE DAS REVISÕES

18.1 A revisão desta Política será realizada anualmente, em conformidade com as melhores práticas globais de segurança da informação e as normas ISO aplicáveis ao nosso negócio.

Documento assinado eletronicamente por **Raquel Gomes de Sousa da Costa Dias**, **Defensora Pública-Geral**, em 09/10/2024, às 10:26, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://defensoria.mg.def.br/portal-sei informando o código verificador **0367244** e o código CRC **85822FC4**.