ÍNDICE

Histórico das Revisões:

Rev. Nr.	Data	Descrição
00	18/12/2024	Emissão inicial

Elaboração	Aprovação
Área: Gerência de Privacidade e Proteção da Informação (GEP)	Área: Diretoria Jurídica, de Governança e Gestão (DJG)

1. OBJETIVO

1.1. Este documento tem por objetivo estabelecer as diretrizes para a classificação, manuseio e atribuição de sigilo das informações sob a responsabilidade da empresa PRODESP, garantindo a proteção, integridade e confidencialidade de dados e informações, conforme as normativas legais e regulamentares aplicáveis.

2. ABRANGÊNCIA

2.1. Esta norma deve ser observada por todos os administradores, empregados, colaboradores, fornecedores e parceiros da PRODESP.

2.2. A aplicação direta das diretrizes dispostas neste Regulamento, abrangerá:

2.2.1. Autoridade Classificadora;

2.2.2. CADA – Comissão de Avaliação de Documentos e Acesso;

2.2.3. Custodiante;

2.2.4. Usuário

3. DOCUMENTOS REFERENCIADOS

3.1. Lei federal n° 6.404/1976 – Lei das Sociedades Anônimas;

3.2. Lei federal n° 9.279/1996 – Lei da Propriedade Industrial;

3.3. Lei federal n° 12.527/2011 – Lei de Acesso à Informação;

3.4. Lei federal n° 13.303/2016 – Estatuto das Estatais;

3.5. Lei federal nº 13.460/2017 – Lei de Proteção do Usuário do Serviço Público;

3.6. Lei federal n° 13.709/2018 – Lei Geral de Proteção de Dados;

3.7. Lei federal nº 14.129/2021;

3.8. Decreto estadual nº 48.897/2004;

3.9. Decreto estadual nº 68.155/2023;

3.10. Decreto estadual nº 63.382, de 09/05/2018;

3.11. Decreto estadual nº 64.790, de 13/02/2020 – Institui a Central de Dados do Estado de São Paulo - CDESP, a Plataforma Única de Acesso - PUA e o Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo;

3.12. Decreto estadual n° 65.347/2020;

3.13. Deliberação Normativa CGGDIESP-1, de 30/12/2021 - Política de Governança de Dados e Informações – PGDI.

3.14. Deliberação Normativa CGGDIESP-2, de 30/12/2021 - Política de Proteção de Dados Pessoais;

3.15. Decreto estadual nº 68.769/2024 – Política de Dados Abertos;

3.16. Política de Segurança da Informação e Privacidade.

3.17. Política de Governança em Privacidade e Proteção de Dados Pessoais;

3.18. NP-025 – Norma de Acesso e Disponibilidade de Dados.

4. DEFINIÇÕES

4.1. Acesso: Possibilidade e ou oportunidade de obter conhecimento de assunto sigiloso.

4.2. Assunto sigiloso: é aquele que, por sua natureza, é de conhecimento restrito e, portanto, requer medidas especiais para sua segurança.

4.3. Autoridade Classificadora: autoridade máxima que tenha a competência para classificar informações, ou coordenador ou empregado de hierarquia equivalente ou superior que., por delegação, lhe tenha sido atribuída essa competência.

4.4. CADA: Comissão de Avaliação de Documentos e Acesso: comissão designada para, no âmbito desta norma, realizar estudos e orientar sobre a gestão, acesso e divulgação de documentos, dados e informações a fim de direcionar à correta aplicação dos critérios de restrição de acesso e seus prazos, constantes da Tabela Indicativa de Documentos, Dados e Informações Sigilosas e Pessoais, a fim de instruir o trabalho decisório da Autoridade Classificadora, além de outras atribuições legalmente pertinentes.

4.5. Confidencialidade: qualidade imputada a uma informação a fim de garantir que esta seja protegida contra acessos não autorizados, de forma a permitir a disponibilidade apenas àqueles autorizados de acordo com as suas funções laborais.

4.6. Controlador de dados: pessoa natural ou jurídica de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais.

4.7. Custódia: responsabilidade pela segurança de assunto sigiloso, decorrente da posse de material ou documento sigiloso.

4.8. Custodiante: Unidade Organizacional e seus responsáveis incumbidos da proteção e vigilância da informação, ainda que transitoriamente, abrangendo os processos de seu armazenamento, processamento, manutenção, recuperação, disponibilização, guarda, transporte e eventual descarte, conforme Tabela de Temporalidade dos Documentos das Atividades Meio e Fim da PRODESP.

4.9. Dados: são quaisquer registros sem tratamento e contexto e que dão origem a uma informação. Podem ser aleatórios, sem qualquer análise prévia ou estruturação.

4.10. Dado Pessoal: Informação relacionada à pessoa física identificada ou identificável.

4.11. 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 física.

4.12. Documento: unidade de registro de informações, qualquer que seja o seu suporte ou formato.

4.13. Gestor da Informação: gestor da Unidade Organizacional que dá origem ou adquire a informação, tornando-se responsável pela segurança adequada de seu acesso, além da comunicação de riscos corporativos a ela relacionadas.

4.14. Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

4.15. Informação pública: Compreende todas as informações produzidas e recebidas pelos órgãos públicos, instituições de caráter público e entidades privadas encarregadas da gestão de serviços públicos. Incluem-se ainda todas as informações conexas com verbas públicas utilizadas por empresas privadas ou pessoas físicas por meio de contratos, convênios ou congêneres.

4.16. Informação reservada: Informações cuja divulgação não autorizada possa comprometer a segurança da empresa ou do Estado, sendo acessíveis, em regra, a servidores ou colaboradores autorizados, dentro dos limites legais.

4.17. Informação secreta: Informações cuja divulgação não autorizada possa colocar em risco a segurança do Estado ou da empresa, devendo ser acessíveis apenas a pessoas previamente autorizadas, conforme sua função ou necessidade de conhecimento.

4.18. Operador de dados: pessoa natural ou jurídica de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador seguindo as orientações deliberadas por este.

4.19. Sigilo comercial: proteção de informações sobre operações, serviços, bem como as constantes nos livros, papéis e sistemas de escrituração, cuja divulgação possa prejudicar a competitividade, interesses de negócios, iniciativas de governo, políticas públicas ou expor a PRODESP à concorrência desleal.

4.20. Sigilo estratégico: proteção de informações relacionadas a planos estratégicos, projetos ou iniciativas, não revelados a conhecimento público e ao mercado, cuja divulgação do teor possa prejudicar a governança corporativa, a competitividade, interesses de negócios, iniciativas de governo, políticas públicas ou expor a PRODESP à concorrência desleal.

4.21. Sigilo industrial: proteção das informações relacionadas a novas tecnologias, melhorias de sistemas, pesquisas ou soluções técnicas desenvolvidas na PRODESP, cuja divulgação do conteúdo possa prejudicar a competitividade, interesses de negócios, iniciativas de governo, políticas públicas, expor a PRODESP à concorrência desleal ou lesão a direitos de terceiros vinculados contratualmente à PRODESP.

4.22. Termo de Classificação de Informação – TCI: documento no qual deverão constar as informações referentes ao grau de sigilo, categoria na qual se enquadra a informação, indicação de dispositivo legal que fundamenta a classificação, suas razões, indicação do prazo de sigilo, data e identificação da autoridade que classificou a informação.

4.23. Tabela de documentos, dados e informações sigilosas e pessoais: relação exaustiva de documentos, dados e informações com qualquer restrição de acesso, com a indicação do grau

de sigilo, decorrente de estudos e pesquisas promovidos pelas Comissões de Avaliação de Documentos e Acesso - CADAs, e publicada pelas autoridades máximas dos órgãos e entidades.

4.24. Termo de Reavaliação da Informação – TRI: documento no qual deverá ser apontada a reavaliação das informações, a fim de reclassificá-las no caso de redução de prazo ou desclassificá-las no que se refere ao sigilo.

4.25. Usuário: empregado ou colaborador autorizado a utilizar informações ou recursos de informação da PRODESP.

4.26. Uso compartilhado: forma de tratamento de dados que compreende a sua comunicação, difusão, transferência, interconexão de dados ou tratamento compartilhado de bancos de dados entre entes públicos e/ou privados, reciprocamente, para uma ou mais modalidades de tratamento permitidas.

5. DIRETRIZES GERAIS

5.1. A classificação da informação consiste na atribuição de um nível de sigilo e na indicação do respectivo rótulo pela Autoridade Classificadora, com o objetivo de determinar os controles necessários para preservar a informação de acordo com seu grau de confidencialidade.

5.2. A classificação da informação na PRODESP deve ser realizada considerando as diretrizes da Lei de Acesso à Informação (LAI) e os seguintes critérios:

5.2.1. A importância, a criticidade, a sensibilidade e a relevância da informação para as atividades da instituição;

5.2.2. Os requisitos legais, bem como as políticas e normas vigentes da PRODESP;

5.2.3. A necessidade de sigilo para garantir a agilidade dos processos e otimizar os investimentos em controles de proteção;

5.2.4. A análise de riscos e os impactos potenciais para a PRODESP caso a informação seja acessada, divulgada, modificada ou excluída indevidamente.

5.3. Para evitar a aplicação de controles de segurança desnecessários e despesas adicionais, a classificação não deve ser mais restritiva do que o necessário. A informação deve ser classificada de acordo com o mínimo necessário para garantir a segurança e a integridade das atividades da PRODESP.

5.4. As informações de propriedade ou sob responsabilidade da PRODESP devem ser imediatamente classificadas pela Autoridade Classificadora assim que forem geradas, adquiridas, processadas ou armazenadas, garantindo o tratamento e a proteção adequados durante todo o seu ciclo de vida.

5.5. O acesso às informações da PRODESP deve ser restrito àqueles empregados que necessitem delas para o desempenho de suas atividades profissionais.

5.6. A classificação e o tratamento da informação de terceiros, fornecedores e parceiros comerciais devem seguir as disposições dos contratos, termos de confidencialidade ou acordos firmados com a PRODESP.

5.6.1. A classificação em grau de sigilo deverá ser realizada mediante análise do caso concreto, observar o interesse público da informação e utilizar o critério menos restritivo possível, considerando a gravidade de risco claro e específico de dano ao bem jurídico tutelado e as alternativas disponíveis para eventual acesso a parte da informação.

5.6.2. A Autoridade Classificadora deve elaborar o Termo de Classificação de Informação (TCI) que incluirá:

a. o assunto sobre o qual versa a informação;

b. os fundamentos da decisão, observados os critérios estabelecidos no artigo 29 do Decreto 68.155/2023;

c. a indicação do prazo de sigilo, contado em anos, meses ou dias, ou, alternativamente, do evento cuja materialização configurará seu termo final, nos termos do § 2° do artigo 29 deste decreto;

d. a identificação do agente público que proferiu a decisão;

e. as datas da decisão de classificação, reclassificação ou desclassificação e do respectivo termo de registro;

f. indicação do grau de sigilo;

g. indicação do dispositivo legal que fundamentou a decisão.

5.6.3. A classificação das informações poderá ser reavaliada pela Autoridade Classificadora, podendo ser desclassificada ou ter seu prazo de sigilo reduzido, conforme necessário. A reavaliação será formalizada através de Termo de Reavaliação de Informação considerando:

a. Prazo máximo de restrição de acesso à informação;

b. Manutenção das razões para a classificação;

c. Possíveis danos ou riscos decorrentes da divulgação irrestrita da informação.

5.6.4. A PRODESP deverá publicar anualmente, em seu sítio eletrônico, o rol de documentos:

a. Desclassificados nos últimos 12 (doze) meses;

b. Classificados e respectivos graus de sigilo, com identificação para referência futura.

6. CRITÉRIOS DE CLASSIFICAÇÃO DA INFORMAÇÃO

6.1. As áreas da PRODESP devem classificar as informações geradas, adquiridas, processadas ou armazenadas no desenvolvimento de suas atividades, por meio da Autoridade Classificadora.

6.2. A classificação das informações com base nos níveis de sigilo, deve considerar a natureza e o impacto da divulgação das informações, visando proteger os interesses da empresa e garantir a conformidade com as normas legais vigentes.

6.3. Deve ser aplicada a publicidade como preceito geral e o sigilo como exceção, devendo ser observado na atribuição de sigilo o interesse público da informação, utilizando o critério menos restritivo possível.

6.4. É vedada a fixação prévia de sigilo, sendo obrigatória a análise específica e motivada dos documentos, dados e informações.

6.5. Considerando a competência para a definição de informações cabe à PRODESP, a atribuição de classificação das informações nos seguintes níveis de sigilo, conforme as definições e prazos estabelecidos pela legislação vigente:

6.5.1. Reservada: Informações cuja divulgação não autorizada possa comprometer a segurança da empresa ou do Estado, sendo acessíveis, em regra, a servidores ou colaboradores autorizados, dentro dos limites legais.

6.5.2. Secreta: Informações cuja divulgação não autorizada possa colocar em risco a segurança do Estado ou da empresa, devendo ser acessíveis apenas a pessoas previamente autorizadas, conforme sua função ou necessidade de conhecimento.

6.6. É vedado à PRODESP classificar qualquer documento, dado e/ou informação como ultrassecreto nos termos dos incisos I e II, artigo 31 do Decreto Estadual nº 68.155/2023.

6.7. Os documentos, dados e informações sigilosas poderão tornar-se públicos por meio da reclassificação, porém documentos, dados e informações, que em algum momento já foram públicos não poderão tornar-se sigilosos, exceto por determinação legal.

6.8. Os prazos máximos de restrição de acesso à informação, conforme a classificação, vigoram a partir da data de sua produção: reservado: 5 (cinco) anos e secreto: 15 (quinze) anos.

6.9. Transcorrido o prazo de classificação ou consumado o evento que defina o seu termo final, o documento, dado ou informação tornar-se-á, automaticamente, de acesso público.

6.10. Os prazos mencionados podem ser antecipados por evento terminativo que indique perda de razão do sigilo.

6.11. Todo documento classificado deve apresentar, de forma visível e clara, qual o nível de classificação da informação contida no documento.

6.12. Quando a aplicação de rótulos físicos ou eletrônicos não for possível, outras formas para rotular a classificação da informação devem ser usadas. Em caso de dúvidas, o Gestor da Informação pode contatar a Área de Tecnologia da Informação.

6.13. As áreas da PRODESP que identificarem uma informação que ainda não está classificada, deve informar imediatamente à Autoridade Classificadora e tratá-la como reservada

6.14. A classificação de um grupo de informações deve ser a mesma atribuída à informação classificada com o nível mais alto de sigilo.

6.15. Quando a informação pertencer a terceiros e a PRODESP desempenhar o papel de custodiante, a classificação da informação e os requisitos e controles que serão aplicados para proteção devem ser informados pelo terceiro e formalizados em instrumento específico.

6.16. A classificação do grau de sigilo dependerá de prévio estudo pela CADA nos termos legais, devendo obedecer ao rito determinado pela legislação pertinente, bem como das autoridades competentes, podendo ser classificadas como: secreta e reservada, pelos prazos definidos na legislação.

6.17. Nos estudos realizados pela CADA para a classificação do documento, dado ou informação em determinado grau de sigilo, deverá ser observado o interesse público da informação, e utilizado o critério menos restritivo possível, considerando a gravidade do risco ou dano à segurança da sociedade e do Estado e o prazo máximo de restrição de acesso ou o evento que defina seu termo final.

7. CLASSIFICAÇÃO DE INFORMAÇÃO COM SIGILO DETERMINADO POR LEGISLAÇÃO ESPECÍFICA

7.1. As informações protegidas por legislações específicas, tais como sigilos bancário, fiscal, comercial, profissional e segredo de justiça, da mesma forma que ocorre em relação aos dados pessoais devem ser tratadas conforme disciplinado na respectiva legislação.

7.2. Os dados e informações cujos sigilos são determinados por legislação específica, deverão ser protegidos visando atender a devida restrição de acesso de forma automática, sendo de responsabilidade da instância responsável por sua produção e guarda, observar obrigatoriamente o disposto nesta Norma quanto à adequada proteção.

7.2.1. Os documentos, dados e informações protegidas por dispositivo legal específico deverão ser denominados como informação secreta.

7.2.2. Tais restrições não são oponíveis nas hipóteses legais, como em razão de autorização judicial, fiscalizações por órgãos de controle externo, na forma da lei, observada a transferência de sigilo.

7.2.3. Essas informações não deverão ser classificadas pela Autoridade Classificadora.

8. MANUSEIO DA INFORMAÇÃO – DIRETRIZES ESPECÍFICAS

8.1. As informações pessoais relativas à intimidade, vida privada, honra e imagem detidas pela Prodesp:

8.1.1. terão acesso restrito a agentes públicos, empregados e prestadores de serviços legalmente autorizados e à pessoa a que se referirem, independentemente de classificação de sigilo;

8.1.2. poderão ter sua divulgação ou acesso por terceiros autorizados por previsão legal, ou consentimento expresso do titular de dados a que se referirem ou com justificativa em uma das hipóteses autorizadoras apresentadas no artigo 7º da Lei Geral de Proteção de Dados (LGPD), desde que necessário para o atingimento da finalidade comunicada ao titular.

8.1.3. As orientações relativas ao compartilhamento e liberação de acesso aos dados pessoais armazenados no Data Center da PRODESP para uso do próprio controlador, colaboradores e empresas terceirizadas que prestam serviços para a Companhia ou

ainda, em atendimento às solicitações judiciais ou de órgãos de controle externo em situações predeterminadas, estão dispostas na Norma NP-025, ensejando a obtenção da devida autorização conforme o Termo de Autorização de Acesso e Disponibilidade de Dados (TRM-013).

8.2. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

9. TRANSMISSÃO DE INFORMAÇÕES CLASSIFICADAS

9.1. Quando não for autorizado acesso integral à informação, por esta ser parcialmente sigilosa, é assegurado o acesso à parte não sigilosa por meio de certidão, extrato ou cópia com ocultação da parte sob sigilo.

9.2. O acesso a documento preparatório ou informação nele contida, utilizado como fundamento de tomada de decisão ou de ato administrativo, será assegurado a partir da edição do ato ou decisão.

9.3. No caso de existência, no documento preparatório, de informações protegidas por alguma categoria de sigilo, somente poderão ser divulgadas as partes não sigilosas.

9.4. Os rascunhos não serão divulgados por não constituírem informações oficiais da PRODESP, contudo devem ser observadas a diretrizes deste regulamento quanto ao tratamento adequado dessas informações.

9.5. O compartilhamento de documentos que contenham informações confidenciais ou classificadas como sigilosas somente poderá ocorrer mediante solicitação formal e preenchimento de Termo de Confidencialidade, individualizado, anexo de procedimento próprio. O acesso à informação protegida cria a obrigação para aquele que a obteve de resguardar o sigilo.

9.6. A PRODESP identificará a categoria de sigilo nos documentos e informações solicitadas por órgãos de controle, que se tornará corresponsável pela manutenção do sigilo das informações com eles compartilhadas.

9.7. O acesso a documentos e informações classificadas como sigilosas cria a obrigação para aquele que a obteve de resguardar o sigilo.

9.8. A pessoa física ou jurídica contratada, terceiros envolvidos que, em razão de qualquer vínculo com a PRODESP, executar atividades de tratamento de documentos, dados e informações confidenciais ou classificadas como sigilosas, adotará as providências necessárias para que seus empregados, prepostos ou representantes observem as medidas e procedimentos de segurança das informações resultantes da aplicação desta norma e da legislação pertinente.

9.9. O acesso a documentos, dados e informações confidenciais, originários de outros órgãos ou instituições privadas, custodiados para fins de instrução de procedimento, processo administrativo ou judicial, somente poderá ser realizado para outra finalidade se autorizado pelo agente credenciado do respectivo órgão, entidade ou instituição de origem.

9.10. Informações classificadas como RESERVADA ou SECRETA (INTERNA ou EXTERNA) não devem ser publicadas na Internet e nas mídias sociais, exceto quando o compartilhamento for autorizado Gerência de Privacidade e Proteção da Informação (GPA) e Gerência Jurídica (GJU) e juntamente com sua Diretoria Jurídica, de Gestão e Governança (DJG).

10. GESTÃO DE RISCOS

10.1. Deve ser implementado um processo contínuo de gestão de riscos de segurança que inclui, mas não se limita a:

10.1.1. Identificação de ativos de informação e seus riscos associados;

10.1.2. Avaliação dos riscos considerando a confidencialidade, integridade e disponibilidade;

10.1.3. Tratamento dos riscos identificados;

10.1.4. Monitoramento e revisão periódica dos riscos e controles implementados.

10.2. Deve-se estabelecer procedimento formal para resposta a incidentes com a informação classificada, levando em consideração o disposto no item anterior que incluirá:

10.2.1. Identificação e classificação quanto ao tipo de incidente;

10.2.2. Notificações interna e externa (quando se fizer necessária);

10.2.3. Contenção e mitigação do incidente;

10.2.4. Apuração/Investigação e coleta de evidências;

10.2.5. Recuperação e retorno a normalidade;

10.2.6. Lições aprendidas e melhorias no processo de segurança da informação classificada.

10.3. Deve-se estipular em norma ou procedimento próprio meios de avaliação e implementação de controles de segurança específicos para uso de tecnologias emergentes, incluindo, mas não se limitando a:

10.3.1. Inteligência artificial e aprendizado de máquina;

10.3.2. Internet das coisas (IoT);

10.3.3. Computação em nuvem;

10.3.4. Blockchain;

10.3.5. Demais tecnologias de comunicação avançadas, homologadas ou não por instituições oficiais.

11. DA SEGURANÇA PARA INFORMAÇÃO CLASSIFICADA COMO SECRETA:

11.1. Deve ser implementada política/norma de uso de encriptação avançada (criptografia) para informações classificadas como SECRETA e esta deverá conter:

11.1.1. Uso de algoritmos e protocolos criptográficos robustos e atualizados;

11.1.2. Gerenciamento seguro de chaves criptográficas;

11.1.3. Criptografia de dados em repouso e em trânsito;

11.1.4. Revisão mínima de forma a garantir sua eficácia contínua.

12. SEGURANÇA NO CICLO DE VIDA DA INFORMAÇÃO CLASSIFICADA

12.1. Os Colaboradores têm o dever de assegurar a proteção das informações que tiverem contato contra perda, acesso, alteração ou divulgação não autorizada, de acordo com a sua classificação, além de não as utilizar para obtenção de vantagens para si ou outrem.

12.2. Controle de segurança devem ser implementados em todas as fases do ciclo de vida da informação, dentre eles:

12.2.1. Criação e Coleta: Classificação inicial e aplicação de controles de acesso;

12.2.2. Armazenamento: Criptografia e backup;

12.2.3. Uso: Monitoramento de acesso e prevenção de vazamentos;

12.2.4. Compartilhamento: Controles de transferência segura;

12.2.5. Arquivamento: Retenção segura conforme requisitos legais e tabelas de temporalidade;

12.2.6. Descarte: Destruição segura e evidenciada de dados e mídias.

13. RECLASSIFICAÇÃO

13.1. Informações que tiveram sua relevância ou potencial de impacto alteradas devem ser reclassificadas pela respectiva Autoridade Classificadora.

13.1.1. Todos os colaboradores devem comunicar imediatamente à Autoridade Classificadora da inexistência ou inconsistência na classificação de uma informação.

13.2. Compete à Autoridade Classificadora ou colaborador por ele designado formalmente, alterar ou cancelar a classificação atribuída às informações respeitando os interesses da PRODESP quando julgar necessário.

14. RESPONSABILIDADES

14.1. CADA

a) Identificar e elaborar a Tabela Indicativa de Documentos, Dados e Informações Sigilosas e Pessoais, contendo sua manifestação acerca dos prazos mínimos de restrição de acesso e encaminhá-la para manifestação da Assessoria Jurídica e posterior publicação;

b) Propor à Autoridade Classificadora, e na sua ausência, ao Diretor Competente, a renovação, alteração de prazos, reclassificação ou desclassificação de documentos, dados e informações sigilosas;

c) Atuar como instância consultiva da autoridade competente, sempre que provocada, sobre os recursos interpostos relativos às solicitações de acesso a documentos, dados e informações não atendidas ou indeferidas.

14.2. AUTORIDADE CLASSIFICADORA

a) Determinar os graus de sigilo quando aplicáveis, após a manifestação da CADA e deliberar a publicação da tabela correspondente;

b) Alterar ou cancelar a classificação atribuída às informações respeitando os interesses da PRODESP quando julgar necessário.

14.3. SUPERINTENDÊNCIAS, GERÊNCIAS, COORDENADORIAS E ASSESSORIAS

a) Garantir e gerenciar o cumprimento desta Norma e demais documentos complementares pelos seus colaboradores;

b) Identificar violações ou eventual ação em desconformidade às regras de retenção e de descarte de informações praticada por pessoa no uso da informação ou sistemas e comunicar à Área de Segurança da Informação.

14.4. EMPREGADOS, FUNCIONÁRIOS E TERCEIROS PRESTADORES DE SERVIÇOS

a) Cumprir, estar ciente e manter-se atualizado com essa Norma e documentos complementares;

15. DISPOSIÇÕES FINAIS

15.1. O não cumprimento desta norma e demais instrumentos normativos aplicáveis, acarretará ao usuário, penalidades administrativas conforme Código de Conduta e Integridade para empregado/funcionário e cláusulas contratuais em caso de funcionários de empresas terceirizadas.

15.2. Esta norma deve ser revisada a cada dois anos ou sempre que existir a necessidade de alterações, conforme os critérios definidos nas demais normas e políticas específicas da PRODESP.

15.3. O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com as normas e procedimentos aplicáveis na PRODESP.

15.4. Este documento, bem como os demais documentos que a complementam, encontram-se disponíveis na Central de Documentos PRODESP.