I - Introdução

1.1. A presente Política de Classificação da Informação da Fundação de Apoio Científico e Tecnológico do Tocantins - Fapto dispõe sobre as diretrizes seguidas pela Fundação, em observância às disposições da Lei n° 13.709/2018 - Lei Geral de Proteção de Dados (LGPD), da Lei n° 12.527/2011 - Lei de Acesso à Informação - LAI e demais disposições legais que tratem sobre a matéria.

1.2 Esta Política integra o Programa de Governança em Privacidade e Segurança da Informação da Fapto, sendo de observância obrigatória por todos que tratam informações em nome da Fundação.

II - Objetivo

2.1. Estabelecer diretrizes para a classificação, tratamento e proteção das informações produzidas e tratadas pela Fapto, assegurando sua autenticidade e observância dos princípios da confidencialidade, disponibilidade, integridade e privacidade, em conformidade com a Lei n° 13.709/2018 - LGPD, com a Lei n° 12.527/2011 - LAI e demais normas aplicáveis.

2.2 Reforçar a rastreabilidade e a responsabilização no tratamento da informação, prevenindo riscos de incidentes de segurança, fraudes, perdas financeiras e danos à imagem institucional.

III - Abrangência

3.1. Esta Política de Classificação da Informação aplica-se a todos os colaboradores, estagiários, bolsistas, terceirizados, gestores, consultores, parceiros, coordenadores de projetos e quaisquer pessoas físicas ou jurídicas que atuem em nome da Fapto e tenham acesso a informações institucionais.

IV - Definições

4.1. Para fins do disposto nesta Política devem ser observadas as definições a seguir:

4.1.1. CLASSIFICAÇÃO DA INFORMAÇÃO: identificação do nível de acesso dos documentos e/ou processos;

4.1.2. DADO PESSOAL: informação relacionada a pessoa natural identificada ou identificável;

4.1.3. DADO PESSOAL SENSÍVEL: dado pessoal sobre a 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;

4.1.4. DADOS DE CRIANÇAS E ADOLESCENTES: dados pessoais de titulares menores de 18 (dezoito) anos, submetidos à proteção especial, nos termos do art. 14 da Lei Geral de Proteção de Dados Pessoais (LGPD) e do Estatuto da Criança e do Adolescente (ECA), devendo seu tratamento observar o princípio do melhor interesse do menor;

4.1.5. INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;

4.1.6. INFORMAÇÃO PESSOAL: é a informação relacionada à pessoa física cuja identidade seja determinada ou possa ser determinada;

4.1.7. TRATAMENTO DA INFORMAÇÃO: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

4.1.8. DISPONIBILIDADE: característica da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;

4.1.9. AUTENTICIDADE: característica da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;

4.1.10. INTEGRIDADE: característica da informação não modificada, inclusive quanto à origem, trânsito e destino;

4.1.11. PRIMARIEDADE: característica da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações.

4.1.12. INCIDENTE DE SEGURANÇA: qualquer evento adverso confirmado ou sob suspeita que envolva violação de confidencialidade, integridade, disponibilidade ou privacidade das informações.

V - Classificação da informação

5.1. A classificação dos documentos, dados e processos na Fapto deve ser realizada de forma compatível com o grau de segurança da informação exigido, considerando sua **confidencialidade, integridade e disponibilidade.** Essa prática visa garantir a proteção adequada das informações, otimizar e agilizar os processos de tratamento, além de promover a eficiência no uso dos recursos, reduzindo custos relacionados à segurança da informação e assegurando o cumprimento das normas legais.

5.1.1. Ao classificar as informações institucionais, devem ser consideradas as seguintes características, que orientam a definição do grau de sigilo e do tratamento adequado:

a) **Confidencialidade:** proteção contra o acesso não autorizado, avaliando o grau de impacto caso a informação seja revelada a pessoas, sistemas, órgãos ou entidades não autorizadas.

b) **Integridade:** proteção contra modificações ou destruição não autorizadas ou acidentais, considerando o impacto de eventual alteração indevida da informação.

c) **Disponibilidade:** garantia de que a informação esteja acessível e utilizável, sob demanda, por pessoas ou sistemas devidamente autorizados, avaliando o impacto de sua indisponibilidade.

d) **Autenticidade:** garantia de que a informação é genuína, produzida e mantida por fonte confiável, avaliando o impacto de eventual falsificação ou manipulação indevida.

e) **Privacidade:** proteção dos dados pessoais, em conformidade com a LGPD, considerando o impacto de eventual vazamento ou uso indevido de informações de pessoas naturais.

5.2. Os documentos, quando de sua emissão e/ou recebimento, terão os seus conteúdos visualizados de acordo com os níveis de acesso a eles atribuídos, conforme a seguinte classificação:

5.2.1. **Público:** informações disponíveis ao público em geral, cujo acesso irrestrito não gera risco à Fapto ou aos titulares de dados.

5.2.1.1. Pode ser acessado e divulgado livremente, não exigindo medidas específicas de segurança.

5.2.2. **Restrito:** informações que podem identificar pessoas ou conter dados pessoais comuns, seu acesso deve ser controlado para evitar uso indevido.

5.2.2.1. Acesso limitado a colaboradores autorizados, com medidas básicas de segurança, quais sejam, controle de acesso, autenticação, armazenamento seguro.

5.2.3. **Sigiloso:** informações que envolvem dados pessoais sensíveis, cujo vazamento pode causar dano grave.

5.2.3.1. Acesso estritamente restrito e monitorado, com medidas rigorosas de segurança, quais sejam, criptografia, autenticação multifator, políticas rigorosas de compartilhamento, registro de acesso e treinamentos específicos.

5.3. Para fins desta Política, adota-se a seguinte categorização acerca dos potenciais impactos decorrentes de eventual quebra de confidencialidade:

Grau de Sigilo	Impacto
Sigiloso	Dano grave ou severo, com risco de comprometer a imagem institucional, gerar prejuízos financeiros, impactar operações e inviabilizar objetivos estratégicos.
Restrito	Dano de nível médio, podendo ocasionar consequências colaterais indesejadas.
Público	Sem impactos relevantes em caso de divulgação.

VI - Controle de Prazos de Sigilo

6.1. A classificação de informações como sigilosas deverá observar os prazos máximos de restrição de acesso previstos no art. 24 da Lei nº 12.527/2011 – Lei de Acesso à Informação (LAI), sendo:

a) ultrassecreta: até 25 (vinte e cinco) anos;

b) secreta: até 15 (quinze) anos;

c) reservada: até 5 (cinco) anos.

6.2. As informações classificadas como sigilosas deverão possuir registro formal contendo, no mínimo:

a) fundamento legal da restrição de acesso;

b) autoridade responsável pela classificação;

c) grau de sigilo atribuído;

d) data da classificação;

e) prazo de restrição de acesso;

f) data prevista para revisão ou desclassificação.

6.3. O controle dos prazos de sigilo deverá ser realizado pelo setor responsável pela custódia da informação, com apoio do Encarregado pelo Tratamento de Dados Pessoais (DPO), visando assegurar a revisão periódica das classificações atribuída.

6.4. Encerrado o prazo legal de restrição de acesso, a informação deverá ser automaticamente reavaliada para fins de:

a) desclassificação;

b) redução do grau de sigilo; ou

c) manutenção da restrição, quando houver fundamento legal superveniente que justifique sua continuidade.

6.5. As informações pessoais relativas à intimidade, vida privada, honra e imagem terão acesso restrito pelo prazo máximo de 100 (cem) anos, nos termos da legislação aplicável, restrito aos agentes públicos legalmente autorizados e à própria pessoa a que se referirem.

6.6. O acesso, compartilhamento, armazenamento e descarte de informações classificadas deverão observar controles compatíveis com o respectivo grau de sigilo, garantindo a proteção da confidencialidade, integridade, disponibilidade e privacidade das informações.

6.7. A Fapto deverá manter mecanismos de rastreabilidade e registro das operações realizadas com informações classificadas, possibilitando auditoria, monitoramento e responsabilização em caso de uso indevido ou acesso não autorizado.

VII - Diretrizes Gerais

7.1. Todas as informações devem ser classificadas no momento do recebimento ou criação.

7.2. O tratamento, armazenamento e compartilhamento das informações devem respeitar a classificação definida, garantindo a segurança adequada.

7.3. No âmbito da Fapto, são consideradas de acesso restrito, às informações que:

a) possam afetar a imagem e a credibilidade institucional;

b) revelem estratégias, metodologias ou planos relacionados à gestão de projetos, quando sua divulgação comprometer a execução ou a competitividade;
c) contenham dados sigilosos de parceiros, pesquisadores, empresas ou órgãos públicos vinculados a contratos, convênios ou outros instrumentos;
d) envolvam dados pessoais sensíveis, protegidos nos termos da LGPD (Lei n° 13.709/2018);
e) estejam legalmente classificados como sigilosas por força da lei, regulamento ou instrumento contratual.

7.4. Informações classificadas como “sigiloso” devem receber autorização formal, via e-mail, para acesso.

7.5. O compartilhamento externo de informações classificadas como “restrito” e “sigiloso” depende de análise prévia e autorização específica de quem classificou o documento.

7.6. Toda solicitação de acesso à informação dirigida à Fapto será analisada e respondida no prazo de até 20 (vinte) dias, contado da data de seu protocolo, observando-se o equilíbrio entre transparência e proteção de dados pessoais.

7.6.1. O prazo poderá ser prorrogado uma única vez por mais 10 (dez) dias, mediante justificativa expressa e comunicação prévia ao solicitante.

7.6.2. Caso a informação solicitada não possa ser imediatamente fornecida, a Fapto, por meio do setor responsável, deverá indicar, de forma clara e fundamentada:

a) As razões da negativa de acesso, quando aplicável; ou
b) A data, local e modo em que a informação poderá ser consultada ou obtida.

7.7. Nas transferências eletrônicas de informações realizadas no âmbito da Fapto, devem ser observados controles que assegurem a confidencialidade dos dados, conforme as seguintes diretrizes:

a) adotar mecanismos de detecção e proteção contra *malware*, prevenindo a contaminação dos sistemas;

b) garantir a proteção de informações sensíveis transmitidas em anexos eletrônicos, utilizando-se, quando aplicável, de criptografia ou outros meios seguros;
c) implementar procedimentos para evitar o envio de documentos ou mensagens a destinatários incorretos;
d) exigir aprovação prévia antes da utilização de serviços públicos externos de transferência de arquivos ou dados;
e) assegurar a autenticação adequada quando a transferência ocorrer por meio de redes públicas de acesso;
f) proibição do envio de informações críticas por SMS ou aplicativos de mensagens não corporativos.

7.8. O descarte das informações deve respeitar as normas internas e as disposições legais aplicáveis, assegurando a eliminação segura.

7.9. Todos os colaboradores, estagiários, bolsistas, terceirizados, gestores, consultores, parceiros, coordenadores de projetos e quaisquer pessoas físicas ou jurídicas que atuem em nome da Fapto e tenham acesso a informações institucionais devem ser treinados sobre esta política e sobre boas práticas de proteção da informação.

VIII - Responsabilidades

8.1. Todos os colaboradores, estagiários, bolsistas, terceirizados, gestores, consultores, parceiros, coordenadores de projetos e quaisquer pessoas que atuem em nome da Fapto e tenham acesso a informações institucionais, independente de sua função ou cargo, são responsáveis pela correta classificação, manuseio e proteção das informações e dados pessoais ao quais tenham acesso, observando os critérios e orientações estabelecidos nesta política e na legislação vigente.

8.2. Os gestores devem promover conformidades em suas equipes, reportar incidentes, prezar pelo controle da execução adequada dos normativos, sugerir novos controles e reportar necessidade de novos treinamentos.

8.3. O Encarregado de Tratamento de Dados - DPO é responsável por monitorar o cumprimento desta política, prestar suporte e orientação aos colaboradores sobre a aplicação da LGPD, bem como atuar como canal para tratamento de demandas relacionadas à proteção de dados pessoais e supervisionar auditorias e treinamentos.

8.4. O descumprimento desta Política poderá acarretar sanções administrativas, civis e disciplinares, incluindo advertência, suspensão ou desligamento, conforme a gravidade.

IX - Transparência e Divulgação Pública

9.1. A Fapto mantém o compromisso com a transparência pública, disponibilizando informações institucionais e documentos relevantes por meio do Portal da Transparência, em atendimento às normas legais aplicáveis.

9.2. As informações divulgadas no Portal da Transparência são previamente avaliadas e classificadas para garantir que estejam em conformidade com a legislação de proteção de dados pessoais, especialmente a LGPD, assegurando que dados pessoais sensíveis ou informações que possam comprometer a segurança e a privacidade dos titulares não sejam divulgados.

9.3. A divulgação busca garantir o acesso público às informações de interesse coletivo, promovendo a transparência e o controle social, conforme determina a Lei n° 12.527/2011, sem prejuízo da proteção dos dados pessoais e do sigilo necessário a processos internos e estratégicos da Fundação.

X - Revisão e atualização

10.1. Esta política será revisada anualmente, ou sempre que houver alteração legal ou mudança relevante no tratamento de informações, para garantir conformidade legal e eficiência na proteção das informações, promovendo ainda, análise crítica que deve incluir a avaliação de oportunidade de melhoria.

FAPTO FUNDAÇÃO DE APOIO CIENTÍFICO E TECNOLÓGICO DO TOCANTINS	**POLÍTICA DE CLASSIFICAÇÃO DA INFORMAÇÃO E CONTROLE DE PRAZOS**			**Data da Elaboração:** **24/10/2025**
	Código PL.LGPD.010	**Folha** **1/1**	**Rev.:** 00 **Data:**	**Macroprocesso:** **LGPD**

LEO ARAUJO DA SILVA:91756570159

Assinado digitalmente por LEO ARAUJO DA SILVA:91756570159
ND: C=BR, O=ICP-Brasil, OU=38132981000101, OU=Secretaria da Receita Federal do Brasil - RFB, OU=RFB e-CPF A1, OU=(EM BRANCO), OU=videoconferencia, CN=LEO ARAUJO DA SILVA:91756570159
Razão: Eu sou o autor deste documento
Localização:
Data: 2026.06.23 14:12:01-03'00'
Foxit PDF Reader Versão: 2024.4.0

Léo Araújo da Silva

Diretor-Geral

Fapto