GOVERNO DE PERNAMBUCO
Secretaria de Educação

POLÍTICA

POLÍTICA DE CLASSIFICAÇÃO DA INFORMAÇÃO - PCI

CONTROLE DE VERSÕES

Ao verificar a **necessidade de atualizações neste normativo** entre em contato com "**SGQ – Sistema da Gestão da Qualidade**"

Versão	Data	Autor	Revisor	Aprovador	Descrição
1.0	03/09/2026	Nathália Baltar (GPGT/NSIP)	Rafaella Cintra (GPGT)	Luís Felipe Pereira (GGTIC)	Elaboração do Documento

SUMÁRIO

1. DISPOSIÇÕES GERAIS 4
2. OBJETIVO 6
3. ABRANGÊNCIA 6
4. CONCEITOS E DEFINIÇÕES 6
5. PRINCÍPIOS E DIRETRIZES 7
6. NÍVEIS DE CLASSIFICAÇÃO DA INFORMAÇÃO 7
7. CRITÉRIOS PARA CLASSIFICAÇÃO 8
8. DA PRÉ-CLASSIFICAÇÃO E ROTULAGEM DA INFORMAÇÃO 10
9. PROCEDIMENTOS E RESPONSABILIDADES 10
10. TRATAMENTO DA INFORMAÇÃO CLASSIFICADA 11
11. SANÇÕES 11
12. REFERÊNCIAS 12
13. DISPOSIÇÕES GERAIS 12
ANEXO I – TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO (TCI) 12
ANEXO II – ROL DE INFORMAÇÕES CLASSIFICADAS 13

1. DISPOSIÇÕES GERAIS

A **Secretaria de Educação Pernambuco (SEE/PE)** reconhece a informação como ativo essencial para o cumprimento de sua missão institucional, para a continuidade dos serviços educacionais e administrativos e para a adequada prestação dos serviços públicos à sociedade.

A **Política de Classificação da Informação** estabelece diretrizes, critérios e responsabilidades para a classificação, identificação, tratamento, acesso, armazenamento, compartilhamento, transmissão e descarte das informações produzidas, recebidas, armazenadas ou custodiadas pela SEE/PE, de acordo com seu nível de sensibilidade, criticidade, requisitos legais e necessidade de proteção.

A classificação da informação tem como finalidade assegurar que cada informação receba nível de proteção compatível com seu conteúdo, finalidade, criticidade e possíveis impactos decorrentes de acesso, divulgação, alteração, perda ou uso não autorizado.

Nesse sentido, deverão ser observados os seguintes princípios e diretrizes:

I. **Classificar as informações** de acordo com seu grau de sensibilidade, criticidade, requisitos legais, necessidade de acesso e potenciais impactos decorrentes de sua divulgação, alteração, perda ou indisponibilidade.
II. **Assegurar tratamento adequado às informações durante todo o seu ciclo de vida**, compreendendo sua criação, recebimento, classificação, utilização, armazenamento, compartilhamento, transmissão, arquivamento e descarte.
III. **Restringir o acesso às informações de acordo com a necessidade de conhecimento e de utilização para o desempenho das atribuições institucionais**, observando o princípio do menor privilégio e as autorizações aplicáveis.
IV. **Proteger a confidencialidade, integridade, disponibilidade e autenticidade das informações**, considerando sua classificação, criticidade e os riscos associados ao seu tratamento.
V. **Observar os requisitos legais, regulamentares, contratuais e normativos aplicáveis**, especialmente a **Lei nº 12.527/2011 – Lei de Acesso à Informação (LAI)**, a **Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)** e demais normas relacionadas à Segurança da Informação, proteção de dados pessoais, transparência, gestão documental e Administração Pública.
VI. **Garantir que a classificação da informação não seja utilizada de forma indevida para restringir o acesso a informações que, por sua natureza ou por determinação legal, sejam públicas**, devendo ser observados os princípios da publicidade, transparência e acesso à informação aplicáveis à Administração Pública.

VII. **Adotar medidas de segurança proporcionais ao nível de classificação da informação**, contemplando controles administrativos, físicos e tecnológicos adequados ao risco e à criticidade das informações tratadas.

VIII. **Definir responsabilidades quanto à classificação e ao tratamento das informações**, incluindo a atuação dos responsáveis pela informação, usuários, gestores, áreas técnicas e demais envolvidos em seu ciclo de vida.

IX. **Promover a conscientização e capacitação dos servidores, colaboradores, prestadores de serviços e demais usuários** quanto às regras de classificação, manuseio, compartilhamento, armazenamento e proteção das informações institucionais.

X. **Reavaliar a classificação das informações sempre que houver alteração em seu conteúdo, contexto, finalidade, requisitos legais, nível de sensibilidade ou necessidade de proteção**, bem como quando encerrado o período que justifique determinada restrição de acesso.

XI. **Revisar periodicamente esta Política e seus instrumentos complementares**, de modo a assegurar sua contínua adequação às necessidades institucionais e às mudanças organizacionais, tecnológicas, legais e regulatórias.

A Política de Classificação da Informação aplica-se a todas as informações produzidas, recebidas, armazenadas, processadas, transmitidas ou custodiadas pela SEE/PE, independentemente do meio ou formato em que se encontrem, incluindo documentos físicos e digitais, sistemas de informação, bancos de dados, mensagens eletrônicas, arquivos, mídias, registros, imagens, áudios e demais formas de representação da informação.

Aplica-se a todas as unidades da SEE/PE, incluindo Sede, Gerências Regionais de Educação (GREs), Anexos e unidades escolares, abrangendo servidores, professores, estudantes, prestadores de serviços, terceirizados, estagiários, jovens aprendizes e demais partes que tenham acesso às informações institucionais ou realizem atividades relacionadas ao seu tratamento.

A classificação atribuída à informação deverá orientar os controles de acesso, formas de armazenamento, compartilhamento, transmissão, reprodução, transporte, retenção e descarte, observando-se os requisitos específicos definidos nesta Política e em seus normativos complementares.

2. OBJETIVO

Instituir a Política de Classificação da Informação (PCI) no âmbito da Secretaria Educação de Pernambuco (SEE-PE), com a finalidade de estabelecer diretrizes, critérios e responsabilidades para a classificação, o manuseio, o tratamento e a proteção dos ativos de informação produzidos, recebidos ou custodiados pela Secretaria, em conformidade com a legislação vigente e as melhores práticas de segurança da informação.

3. ABRANGÊNCIA

Esta Política aplica-se a todas as unidades administrativas e pedagógicas da SEE-PE, incluindo a Sede, Gerências Regionais de Educação (GREs), escolas da rede estadual e anexos, bem como a todos os servidores, professores, prestadores de serviço, terceirizados, estagiários e qualquer pessoa que, em virtude de seu relacionamento com a Secretaria, tenha acesso a suas informações, independentemente do meio ou formato em que se encontrem.

4. CONCEITOS E DEFINIÇÕES

TERMO	DEFINIÇÃO
Ativo de Informação	Qualquer recurso da SEE-PE que armazene, processe ou transmita informação.
Classificação da Informação	Atribuição de um nível de proteção à informação (Pública, Restrita, Sigilosa) com base em sua sensibilidade, valor e criticidade.
Custodiante da Informação	Servidor ou unidade organizacional responsável pela guarda e manutenção dos requisitos de segurança de um ativo de informação.
Desclassificação	Cancelamento da classificação de uma informação, tornando-a pública.
Gestor da Informação	Autoridade responsável por um processo de negócio e pelas informações a ele relacionadas, com competência para definir seus requisitos de proteção e autorizar o acesso.
Rotulagem	Ato de registrar e evidenciar o nível de classificação em um documento ou ativo de informação
Termo de Classificação de Informação (TCI)	Documento formal que registra a decisão de atribuir um grau de sigilo a uma informação.
Tratamento da Informação	Conjunto de ações referentes à produção, recepção, classificação, acesso, reprodução, transporte, transmissão, armazenamento e descarte da informação.

Tabela 1: Termos e definições

5. PRINCÍPIOS E DIRETRIZES

A classificação da informação na SEE-PE deve ser orientada pelos seguintes princípios:

I. **Publicidade como Preceito Geral:** O acesso à informação pública é a regra, e o sigilo, a exceção.

II. **Necessidade de Saber:** O acesso a informações restritas e sigilosas deve ser limitado apenas às pessoas que necessitam da informação para o desempenho de suas funções legítimas.

III. **Proporcionalidade:** O nível de proteção aplicado a uma informação deve ser proporcional ao seu valor, criticidade e aos riscos associados à sua divulgação não autorizada.

IV. **Responsabilização e Prestação de Contas:** Todo aquele que manuseia informações classificadas é responsável por sua proteção e deve ser capaz de prestar contas de suas ações.

6. NÍVEIS DE CLASSIFICAÇÃO DA INFORMAÇÃO

Toda informação produzida ou custodiada pela SEE-PE deve ser classificada em um dos seguintes níveis:

I. **PÚBLICA:** Informação cujo acesso é irrestrito, podendo ser divulgada a qualquer cidadão sem necessidade de autorização. Exemplos: atos normativos publicados, notas oficiais, informações institucionais do site da SEE-PE.

II. **RESTRITA:** Informação que, embora não seja sigilosa nos termos da LAI, tem seu acesso limitado a determinados grupos de servidores ou agentes públicos em razão da necessidade de trabalho ou por força de legislação específica (como a LGPD).

III. **SIGILOSA**: Informação submetida temporariamente à restrição de acesso público por ser considerada imprescindível à segurança da sociedade ou do Estado. Esta categoria se subdivide em:

a) Reservada: Prazo de sigilo de até 5 anos.

b) Secreta: Prazo de sigilo de até 15 anos.

c) Ultrassecreta: Prazo de sigilo de até 25 anos (classificação não aplicável no âmbito da SEE-PE, salvo em casos excepcionais definidos por autoridade superior).

7. CRITÉRIOS PARA CLASSIFICAÇÃO

Serão consideradas de acesso **RESTRITO**, no mínimo, as seguintes informações:

I. Informações Pessoais de Alunos, Servidores e Terceiros: Dados cadastrais (CPF, RG, endereço), histórico escolar, notas, frequência, informações de saúde, dados de remuneração, dados bancários e qualquer outra informação protegida pela LGPD.

II. Documentos Preparatórios: Pareceres, notas técnicas, minutas de portarias, relatórios parciais e outros documentos que subsidiem uma tomada de decisão ou ato administrativo ainda não concluído.

III. Processos Administrativos Disciplinares e Sindicâncias em Andamento.

IV. Informações Estratégicas e de Gestão: Planejamentos estratégicos não consolidados, detalhes técnicos de sistemas de informação, arquitetura de rede, senhas de acesso, atas de reuniões deliberativas de caráter não público.

V. Informações Protegidas por Outras Hipóteses Legais: Informações abrangidas por sigilo fiscal, bancário, comercial ou segredo de justiça.

Serão passíveis de classificação como **SIGILOSAS** as informações cuja divulgação ou acesso irrestrito possam, conforme o Art. 23 da LAI:

I. Pôr em risco a vida, a segurança ou a saúde de alunos, servidores ou da comunidade escolar.

II. Comprometer atividades de inteligência ou de fiscalização em andamento.

III. Prejudicar ou causar risco a planos ou operações estratégicas da Secretaria ou do Estado.

IV. Pôr em risco a segurança de instituições ou de altas autoridades.

Classificação de Dados Pessoais e Sensíveis:

As informações que contenham dados pessoais ou dados pessoais sensíveis, conforme definidos nos arts. 5º e 11 da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), deverão possuir classificação e controles de segurança específicos, compatíveis com o seu grau de sensibilidade e risco.

Os dados pessoais (ex.: nome, CPF, e-mail, matrícula, endereço) deverão ser classificados, no mínimo, como **RESTRITOS**, sendo seu acesso limitado às pessoas cuja função exija o

tratamento da informação

Os dados pessoais sensíveis (ex.: informações sobre saúde, deficiência, dados biométricos, origem racial, religião, opinião política) deverão ser classificados, no mínimo, como **SIGILOSOS**, com aplicação de controles técnicos e administrativos reforçados.

O tratamento, armazenamento, compartilhamento e descarte dessas informações deverão observar:

a. Uso exclusivo para finalidades legítimas e previamente definidas;

b. Controle de acesso baseado em perfis e necessidade de conhecimento (need to know);

c. Adoção de criptografia ou anonimização, quando aplicável;

d. Proibição de divulgação pública, reuso indevido ou compartilhamento sem base legal;

e. Registro de acesso e rastreabilidade das operações.

f. O Comitê Gestor de Proteção de Dados (CGPD) poderá estabelecer controles adicionais para assegurar a conformidade com a LGPD e demais normas correlatas.

NÍVEL DE CLASSIFICAÇÃO	DESCRIÇÃO	CONTROLES MÍNIMOS DE SEGURANÇA	EXEMPLOS DE APLICAÇÃO
PÚBLICA	Informação cujo acesso é irrestrito e pode ser amplamente divulgado sem risco à SEE-PE.	• Disponibilização apenas em canais oficiais; • Validação prévia da integridade e veracidade antes da publicação; • Proteção contra alterações não autorizadas (ex.: controle de versão).	Atos normativos, comunicados e informações institucionais do portal da SEE-PE.
RESTRITA	Informação de acesso limitado aos servidores, colaboradores, terceirizados ou unidades organizacionais que necessitem conhecê-la para o desempenho de suas atribuições institucionais. Sua divulgação não autorizada poderá comprometer atividades administrativas, processos decisórios, informações pessoais protegidas por legislação específica ou interesses institucionais da SEE/PE.	• Armazenamento em ambientes institucionais com controle de acesso; • Compartilhamento restrito aos usuários autorizados, observando o princípio da necessidade de conhecimento; • Vedado o envio para contas de e-mail pessoais ou plataformas não autorizadas; • Utilização de credenciais individuais e intransferíveis; • Observância dos níveis de acesso definidos no SEI e demais sistemas corporativos; • Registro e rastreabilidade dos acessos, quando tecnicamente viável.	Comunicados internos, atas de reuniões de equipe, minutas de documentos em elaboração.
SIGILOSA	Informação crítica cuja divulgação pode comprometer a segurança institucional, pública ou estratégica.	• Criptografia forte (AES-256 ou superior); • Armazenamento em ambiente controlado fisicamente (servidores internos, cofres, armários com chave); • Acesso autorizado formalmente por autoridade classificadora; • Proibição de cópia, fotografia ou envio por e-mail comum; • Auditoria e rastreabilidade completa de acessos e transferências; • Descarte seguro por fragmentação ou exclusão definitiva.	Dados sensíveis (saúde, biometria, origem étnica), informações de segurança da rede, planejamento estratégico, investigações administrativas.

Tabela 2 - Controles por nível de classificação da informação

8. DA PRÉ-CLASSIFICAÇÃO E ROTULAGEM DA INFORMAÇÃO

Compete a todo servidor, colaborador ou prestador de serviço que produza ou receba uma informação realizar sua pré-classificação, identificando o grau de sensibilidade do conteúdo e adotando, desde a origem, os cuidados de manuseio e os controles de acesso compatíveis com o nível de classificação atribuído.

I. A pré-classificação tem por objetivo assegurar que somente usuários devidamente autorizados tenham acesso às informações, conforme o princípio do menor privilégio e o critério de necessidade de saber.

II. As informações classificadas como Confidenciais, Restritas ou Sigilosas deverão ser armazenadas e compartilhadas em ambientes institucionais com controle de acesso e, sempre que possível, com autenticação multifator, registro de logs e rastreabilidade das operações.

III. O servidor e terceirizado responsável deverá garantir a rotulagem do documento e a indicação do nível de classificação em local visível, tanto em documentos físicos quanto digitais.

9. PROCEDIMENTOS E RESPONSABILIDADES

Compete a todo servidor ou colaborador que produzir ou receber informação realizar sua pré-classificação, observando, desde a origem, os cuidados de manuseio compatíveis com a natureza e a sensibilidade do conteúdo.

Compete ao Gestor da Informação, a exemplo de Diretor de Escola, Gerente Regional ou Coordenador de Área, a responsabilidade pela classificação das informações sob sua gestão.

A classificação de informação como **SIGILOSA** deverá ser formalizada pela Autoridade Classificadora competente, mediante o preenchimento do Termo de Classificação de Informação (TCI), conforme disposto no **Anexo I** desta Política.

A rotulagem das informações classificadas é obrigatória e deverá observar os padrões definidos pelo Comitê de Segurança da Informação, contemplando, no mínimo:

1. **Documentos físicos:** o nível de classificação deverá ser indicado de forma visível no cabeçalho e no rodapé de todas as páginas.
2. **Documentos digitais:** o nível de classificação deverá ser indicado no documento e, quando tecnicamente aplicável, no nome do arquivo, em suas propriedades ou metadados e no cabeçalho ou rodapé.
3. **E-mails:** o nível de classificação deverá ser indicado no início do campo “Assunto”, mediante identificação correspondente, a exemplo de **[RESTRITO]**.

10. TRATAMENTO DA INFORMAÇÃO CLASSIFICADA

O **armazenamento** de informações classificadas como Restritas ou Sigilosas deverá ocorrer em ambientes seguros, utilizando-se, para documentos físicos, locais com acesso controlado, como armários com chave, e, para documentos digitais, repositórios institucionais com mecanismos de controle de acesso.

O **compartilhamento** de informações classificadas deverá observar as diretrizes de segurança estabelecidas nesta Política, assegurando a confidencialidade, integridade e rastreabilidade das informações.

As informações **Confidenciais, Restritas e Sigilosas** somente poderão ser compartilhadas com pessoas ou entidades devidamente autorizadas e que possuam necessidade de acesso, observadas, quando aplicáveis, as obrigações de confidencialidade previstas em instrumento contratual, termo específico ou outro mecanismo institucional pertinente.

Toda transferência eletrônica de informações classificadas deverá ocorrer por meios seguros e autorizados pela SEE-PE, utilizando, quando aplicável, mecanismos como criptografia, protocolos seguros e autenticados e sistemas institucionais que possibilitem o registro e a rastreabilidade das operações.

É vedado o envio ou compartilhamento de informações classificadas por e-mails pessoais, aplicativos de mensagens ou plataformas não autorizadas pela SEE-PE.

O responsável pelo compartilhamento deverá assegurar que o destinatário tenha ciência das obrigações relacionadas à confidencialidade, à segurança da informação e, quando houver tratamento de dados pessoais, às disposições da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

O **descarte** de informações classificadas deverá ser realizado de modo a impedir sua recuperação indevida, mediante métodos adequados ao tipo de suporte, incluindo fragmentação de documentos físicos e exclusão segura de arquivos digitais, observados os prazos e procedimentos estabelecidos na Tabela de Temporalidade de Documentos e demais normas aplicáveis.

11. SANÇÕES

O uso indevido, o acesso não autorizado, o compartilhamento indevido, a divulgação ou o vazamento de informações classificadas como **RESTRITAS** ou **SIGILOSAS** sujeitará o responsável à apuração de responsabilidade e à aplicação das sanções administrativas, civis e penais cabíveis, assegurados o contraditório e a ampla defesa.

O descumprimento das disposições previstas nesta Política poderá acarretar a adoção das medidas disciplinares cabíveis, sem prejuízo das demais responsabilidades e consequências legais aplicáveis.

12. REFERÊNCIAS

Esta Política está fundamentada, principalmente, nos seguintes normativos, normas e referenciais:

- **Lei Federal nº 12.527/2011** – Lei de Acesso à Informação (LAI).
- **Lei Federal nº 13.709/2018** – Lei Geral de Proteção de Dados Pessoais (LGPD).
- **ABNT NBR ISO/IEC 27001:2022** – Sistemas de Gestão de Segurança da Informação – Requisitos.
- **ABNT NBR ISO/IEC 27002:2022** – Controles de Segurança da Informação.
- **NIST Cybersecurity Framework (CSF) 2.0**.
- **CIS Critical Security Controls v8.1**.
- **Política de Segurança da Informação (PSI) da SEE-PE**.

13. DISPOSIÇÕES GERAIS

Esta Política deverá ser revisada anualmente ou sempre que houver necessidade, de modo a assegurar sua conformidade com a legislação aplicável, com as normas institucionais e com as boas práticas de segurança da informação.

Os casos omissos nesta Política serão dirimidos pela Gerência Geral de Tecnologia da Informação e Comunicação (GGTIC), em conjunto com o Comitê de Segurança da Informação.

Esta Política entra em vigor na data de sua publicação, ficando revogadas as disposições em contrário.

ANEXO I – TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO (TCI)

TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO (TCI)
Nº DO DOCUMENTO/PROCESSO:
GRAU DE SIGILO: ( ) Reservado ( ) Secreto
FUNDAMENTO LEGAL PARA CLASSIFICAÇÃO:
RAZÕES PARA A CLASSIFICAÇÃO (resumido):
PRAZO DA RESTRIÇÃO DE ACESSO:
DATA DA CLASSIFICAÇÃO:
AUTORIDADE CLASSIFICADORA:
Nome:
Cargo:
Assinatura:

ANEXO II – ROL DE INFORMAÇÕES CLASSIFICADAS

A ser publicado anualmente no site da SEE-PE, conforme Art. 41 da Resolução TC nº 30/2015.

Nº da Informação	Fundamentação Legal	Data da Classificação	Termo Final de Restrição	Autoridade Classificadora