CEARÁ
GOVERNO DO ESTADO
CONSELHO ESTADUAL DE EDUCAÇÃO

Política da Segurança da Informação

Conselho Estadual de Educação
Rua Napoleão Laureano, 500 – Bairro de Fátima – CEP: 60411-170
Fortaleza-CE • Fone: (85) 98238.7314

CEARÁ
GOVERNO DO ESTADO
CONSELHO ESTADUAL DE EDUCAÇÃO

GOVERNADOR
Elmano de Freitas da Costa

PRESIDENTE DO CEE
Ada Pimentel Gomes Fernandes Vieira

VICE-PRESIDENTE
Lúcia Maria Beserra Veras

SECRETÁRIA GERAL
Raimunda Aurila Maia Freire

EQUIPE RESPONSÁVEL PELA ELABORAÇÃO

COORDENADOR DE TECNOLOGIA DA INFORMAÇÃO
ALCIDES GUERRA

ANALISTA DE SISTEMAS IV
VITOR VERAS THOMÉ DA FROTA

ANALISTA DE SISTEMAS I
EDMILSON RAULINO DE SOUSA NETO

CEARÁ
GOVERNO DO ESTADO
CONSELHO ESTADUAL DE EDUCAÇÃO

CONTROLE DE APROVAÇÃO

ELABORAÇÃO	REVISÃO	APROVAÇÃO
EDMILSON RAULINO DE SOUSA NETO	ALCIDES GUERRA	
VITOR VERAS		
ALCIDES GUERRA		ALCIDES GUERRA

CEARÁ
GOVERNO DO ESTADO
CONSELHO ESTADUAL DE EDUCAÇÃO

SUMÁRIO

1. APRESENTAÇÃO

O Conselho Estadual do Ceará (CEE/CE) tem como missão normatizar, deliberar, acompanhar e avaliar o Sistema Estadual de Ensino do Ceará para o desenvolvimento da educação com qualidade e equidade.

Para cumprimento de sua missão institucional é fundamental que os processos executados neste órgão sejam conduzidos de forma segura, com a proteção de seus servidores, preservando a integridade, confidencialidade e disponibilidade das informações.

Esse documento considera, ainda, o disposto no Decreto n° 34.100, de 8 de junho de 2021, que dispõe sobre a Política de Segurança da Informação e Comunicação dos Ambientes de Tecnologia da Informação e comunicação – TIC do Governo do Estado do Ceará.

2. OBJETIVO

O objetivo desta Política de Segurança da Informação e Comunicação (PSI) é estabelecer princípios, diretrizes, normas e procedimentos gerais para a gestão da segurança da informação dos ambientes de Tecnologia da Informação e Comunicação (TIC) do Conselho Estadual de Educação (CEE), de maneira a preservar a integridade, confidencialidade e disponibilidade das informações, descrevendo diretrizes e procedimentos para o manuseio, controle e proteção das informações contra perdas, alterações, divulgações indevidas e acessos não autorizados.

3. ABRANGÊNCIA

A PSI deverá ser aplicada a todas as áreas, instalações, equipamentos, materiais, documentos, pessoas e sistemas de informação, como também às atividades de todos os agentes públicos, incumbindo a cada um a responsabilidade e o comprometimento para a sua aplicação.

A PSI abrange os domínios de segurança e defesa cibernética, segurança física e proteção de dados organizacionais e tem por escopo as ações destinadas a preservação da disponibilidade, integridade, confidencialidade e autenticidade das informações e dados, incluindo:

a) Princípios que são os fundamentos da PSI;

b) Diretrizes que são as regras que representam os princípios e servirão como base para implementação dos processos;

c) Procedimentos: processos específicos a serem implementados para alcançar as estratégias definidas nas diretrizes.

4. SIGLAS E CONCEITUAÇÕES

a) **Agente Público:** É toda pessoa que presta um serviço público, sendo funcionário público ou não, sendo remunerado ou não, sendo o serviço temporário ou não. É todo aquele que exerce ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação, ou qualquer forma de investidura, mandato, cargo, emprego ou função pública;

b) **Ameaça:** causa potencial de um incidente indesejado;

c) **Ativo:** qualquer componente (seja humano, tecnológico, software ou etc.) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio;

d) ***Backup:*** Cópia de segurança de dados;

e) **CEE :** Conselho Estadual de Educação;

f) **Confidencialidade**: garantia de que determinada informação é acessível somente por pessoas autorizadas;

g) **COAFI:** Coordenadoria Administrativo-Financeira;

h) **COTIC:** Coordenadoria de Tecnologia da Informação e Comunicação;

i) **Disponibilidade:** garantia de que usuários autorizados terão acesso às informações sempre que necessário;

j) **Dispositivos móveis:** Qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição como: *notebooks*, *smartphones* e *pendrives*;

k) **Incidente:** evento não planejado que pode causar impactos à organização;

l) **Janela de *backup*:** Períodos em que não há qualquer acesso de usuários ou processos automatizados aos sistemas de informática;

m) **Plano de Recuperação à Desastres:** procedimentos para que a organização operacionalize o retorno das atividades à sua normalidade;

n) **Política de Privacidade**: documento que fornece informações sobre os procedimentos relacionados ao tratamento de dados pessoais;

o) **PSI:** Política de Segurança da Informação;

p) ***Restore:*** Restauração de cópia de segurança de dados;

q) **SPAM:** O termo spam significa *Sending and Posting Advertisement* in Mass, ou "enviar e postar publicidade em massa", ou também: envio de mensagens não-solicitadas, sem propósito específico ao destinatário final;

r) **SSL:** *Secures Sockets Layer*

s) **Usuário:** pessoa que acessa de forma legítima as informações;

t) **TIC:** Tecnologia da Informação e Comunicação;

u) **URL**: *Uniform Resource Locator;*

v) **USB:** *Universal Serial Bus;*

w) **VPN:** *Virtual Private Network* (Rede Virtual Privada).

x) **WAF**: *Web Application Firewall*

y) **Wi-fi**: *Wireless Fidelity* (Rede sem fio)

5. COMPETÊNCIAS E RESPONSABILIDADES

5.1 GESTÃO SUPERIOR DA CEE

Compete à Gestão Superior do CEE:

a) Zelar pelo fiel cumprimento ao estabelecido nesta Política;

b) Garantir recursos necessários para a implementação das diretrizes e procedimentos previstos nesta Política;

c) Promover a disseminação da PSI.

5.2 COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO

Compete à Coordenadoria de Tecnologia da Informação e Comunicação:

a) Implantar, administrar e efetuar a atualização periódica desta Política;

b) Coordenar a execução dos procedimentos e ações de segurança;

c) Mapear os processos relacionados à Segurança da Informação;

d) Definir indicadores para monitorar a execução dos processos relacionados à Segurança da Informação;

e) Identificar e classificar os riscos dos processos relacionados à Segurança da Informação estabelecendo controles para o tratamento adequado dos riscos conforme a sua classificação;

f) Comunicar de forma tempestiva a Gestão Superior qualquer incidente de segurança que possam causar impacto ao adequado funcionamento do CEE;

g) Articular com a área de comunicação do CEE campanhas de conscientização da PSI;

6. PRINCÍPIOS

As ações de segurança da informação do CEE têm como norte as definições contidas na Política de Segurança da Informação e Comunicação dos ambientes de Tecnologia da Informação e Comunicação – TIC do Governo do Estado do Ceará, contendo os seguintes princípios orientadores.

a) Alinhamento Estratégico: considera o alinhamento da Política de Segurança da Informação com o Planejamento Estratégico e com os demais instrumentos de governança do CEE;

b) Diversidade Organizacional: considera a diversidade das atividades da instituição de forma a garantir a continuidade do seu negócio;

c) Garantia da Segurança das Informações: considera a adoção de medidas que visem garantir a confidencialidade, disponibilidade e integridade das informações da instituição;

7. DIRETRIZES

Na PSI foram definidas Diretrizes Gerais e Específicas que devem ser observadas conforme abaixo:

7.1 DIRETRIZES GERAIS

As Diretrizes Gerais da PSI são:

a) As ações relacionadas à Segurança da Informação que serão necessárias ao cumprimento desta Política devem ser consideradas na ocasião da elaboração/revisão do Planejamento Estratégico do CEE;

b) O ativo de TIC constitui patrimônio público, devendo ser disponibilizado para os agentes públicos/sociedade que dele necessitem;

c) Qualquer demanda de agentes públicos relacionados a ativos de TIC devem ser realizadas por meio de abertura de chamado por canal oficial definido pelo CEE;

d) A PSI deverá ser disseminada de forma permanente por meio de campanhas de conscientização com o intuito de assegurar que todos os colaboradores conheçam as suas orientações;

e) Todos os usuários são responsáveis pela segurança dos ativos de informação que estejam sob sua custódia e pelo uso e guarda de suas

credenciais de acesso, sendo vedada a exploração de eventuais vulnerabilidades – que, assim que identificadas, devem ser imediatamente comunicadas às instâncias superiores;

f) Deverá constar em todos os contratos do CEE, quando o objeto for pertinente, cláusula de confidencialidade e de obediência às normas de segurança da informação a ser cumprida por empresas fornecedoras e por todos os profissionais que desempenham suas atividades no CEE, inclusive provenientes de organismos internacionais;

g) Os profissionais prestadores de serviço deverão realizar a entrega do Termo de Confidencialidade e Segurança da Informação (Anexo I), como condição imprescindível para que possa ser concedido acesso aos ativos de informação disponibilizados pelo CEE.

7.2 DIRETRIZES ESPECÍFICAS

As Diretrizes Específicas da PSI são:

7.2.1 ACESSO À INTERNET

a) Os colaboradores somente deverão acessar sites que tenham relação com as atividades desenvolvidas pelo CEE;

b) Nos casos em que determinado colaborador necessite acessar algum conteúdo que esteja bloqueado pelos mecanismos de segurança, deverá ser aberto um chamado pelo Coordenador da área solicitando a liberação do acesso, onde a COTIC fará a liberação desde que o conteúdo solicitado não proporcione riscos para à segurança do CEE.

c) O CEE monitora e bloqueia automaticamente sites de conteúdo erótico, pedofilia, racismo, drogas e outros que contenham conteúdos contrários às legislações vigentes;

d) Qualquer necessidade de download de programas/softwares deve ser repassada à COTIC, sendo registrado o pedido via sistema de abertura de chamados;

e) O uso da internet é auditado e monitorado constantemente, e o colaborador poderá vir a prestar contas de seu uso.

7.2.2 CORREIO ELETRÔNICO

a) A COTIC será responsável pelo gerenciamento, adição, exclusão e adoção de medidas operacionais visando conter a propagação de e-mails suspeitos no ambiente de tecnologia do CEE;

b) A qualquer tempo, mediante detecção pelos sistemas e/ou identificação de e-mails suspeitos pela equipe responsável pela administração do sistema de correio eletrônico, a COTIC procederá com as configurações necessárias objetivando conter eventuais propagações de e-mails suspeitos no CEE;

c) O colaborador deverá efetuar abertura de chamados técnicos no sistema de abertura de chamados do CEE, quando houver necessidade de análise de e-mails suspeitos de SPAM pela COTIC;

d) O colaborador é responsável direto pelas mensagens enviadas por intermédio do seu endereço de correio eletrônico;

e) É proibido o uso do e-mail para cadastro de feed de notícias, sites de compra e venda, rede sociais, faculdade e fornecedores que não sejam da relacionadas ao CEE;

f) Links no corpo do e-mail devem ser clicados apenas quando o remetente for de conhecimento ou confiável.

7.2.3 SISTEMAS

a) Os códigos-fontes dos sistemas gerenciados pela CEE deverão estar armazenados em repositórios no Sistema de Controle de Versão definido pela COTIC;

b) Todos os sistemas do CEE deverão ter ambientes de desenvolvimento, homologação e produção;

c) Os sistemas do CEE deverão ter um padrão para a definição de senhas fortes;

d) No processo de desenvolvimento de sistemas deverão ser observados padrões de segurança que não ocasionem vulnerabilidades as ferramentas do CEE.

7.2.4 PROTEÇÃO DE DADOS PESSOAIS

a) Deverá ser elaborada uma Política de Privacidade de Dados onde serão definidas as diretrizes relacionadas a proteção de dados pessoais;

7.2.5 UTILIZAÇÃO DE ATIVOS

a) Não são permitidas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede, conta ou sistema;

b) O colaborador deve sempre bloquear o equipamento ao se ausentar (Ctrl + Alt + Del ou usando o Bloqueio / Suspender no botão ligar/desligar do windows);

c) Materiais com conteúdo impróprio, como racista, erótico ou

preconceituoso, não podem ser acessados, expostos, armazenados ou distribuídos, através de qualquer tipo de ferramenta ou dispositivos que são utilizados na rede;

d) Todos os dados relativos ao Conselho e suas unidades de negócio devem ser mantidos no servidor, na rede, onde existe sistema de backup periódico;

e) Todos os documentos, vídeos e imagens pessoais não são de responsabilidade do CEE, ou seja, estão sujeitos a exclusão. A estação de trabalho é restritamente para as atividades relacionadas ao trabalho;

f) os colaboradores que estiverem em regime de teletrabalho poderão acessar a rede do CEE por meio de aplicativo de *VPN*;

7.2.6 CONTAS, SENHAS E AUTENTICAÇÃO

a) As senhas para os colaboradores deverão conter no mínimo 8 (oito) caracteres, sendo obrigatório o uso de letras, números e caracteres especiais;

b) Caso o colaborador suspeite do comprometimento de sua senha, deverá modificá-la imediatamente;

c) A senha é individual e intransferível, devendo ser mantida em sigilo. É proibido o seu compartilhamento;

d) As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel etc.), compreensíveis por linguagem humana (não criptografados);

e) Contas que ficarem inativas por mais de 90 dias serão bloqueadas;

f) O tempo de vida das senhas será de, no máximo, 90 (noventa) dias, quando será forçada a sua troca.

8. PROCESSOS ESPECÍFICOS

Para determinados itens específicos desta PSI, por conta da sua criticidade e da necessidade de um monitoramento constante sobre esses, serão definidos processos no âmbito da Gestão de TIC.

8.1 BACKUP

a) A COTIC é responsável por manter e gerenciar todos os dados produzidos ou recebidos pelo CEE;
b) Deverão ser realizados backups diários das informações;
c) Os backups deverão ser realizados em horário pré-estabelecidos para não interferir no funcionamento do CEE;
d) Os backups deverão ser armazenados em local seguro e separado dos sistemas primários;
e) As diretrizes e regras relacionadas ao procedimento de backup deverão ser mapeadas e documentadas na política de backup do CEE;

8.2 CONTROLE DE ACESSO

a) As solicitações de acesso ou desligamento de colaboradores devem ser encaminhadas pelos gestores das unidades ou superiores imediatos para a COTIC através do e-mail cotic@cee.ce.gov.br;
b) Solicitações de acesso a recursos de outras unidades devem ser feitas pelo responsável da unidade solicitada;
c) Cabe à COTIC analisar as solicitações, verificar a legitimidade e necessidade do acesso, conceder ou negar o acesso ao recurso solicitado;
d) Acesso físico a ambientes de TI (salas de servidores, data centers, etc.) somente é permitido a funcionários autorizados da área de TI;
e) Visitantes devem ser acompanhados por um funcionário da área de TI;

8.3 PLANO DE RECUPERAÇÃO À DESASTRES

a) As diretrizes e regras relacionadas ao procedimento de recuperação à desastres deverão ser mapeadas e documentadas na política de recuperação à desastres do CEE;

9. REVISÃO

Essa Política deverá ser revisada no período de 2 (dois) anos a contar da data da sua publicação, podendo haver ajustes ou atualizações em qualquer período caso seja necessário.

10. REFERÊNCIAS

a) Decreto Estadual n° 34.100, de 8 de junho de 2021, que dispõe sobre a Política de Segurança da Informação e Comunicação dos Ambientes de Tecnologia da Informação e comunicação – TIC do Governo do Estado do Ceará;

b) Lei Federal nº 13.709 de 14 de agosto de 2018, Lei Geral de Proteção de Dados;

c) ABNT ISO/IEC 27001 e 27002, Segurança da Informação.