Secretaria de Educação e Esportes

GOVERNO DE PERNAMBUCO
ESTADO DE MUDANÇA

POLÍTICA
Segurança da Informação

CONTROLE DE VERSÕES

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

Versão	Data	Autor	Descrição
01	23.05.2024	Wilson Carlos	Elaboração do Documento.

1. DISPOSIÇÕES GERAIS:

A Política de Segurança da Informação (PSI) da Secretaria de Educação e Esportes (SEE-PE) representa o comprometimento da gestão com a segurança e proteção das informações, sistemas e infraestrutura corporativos; e estabelece diretrizes e responsabilidades que assegurem técnica e administrativamente os requisitos relacionados à segurança das informações tratadas no âmbito deste órgão.

A Política de Segurança da Informação (PSI) tem como principal objetivo fortalecer a segurança das informações, dados pessoais e corporativos que são processados pela SEE/PE. Além disso, visa garantir a proteção dos ativos de tecnologia, demonstrando o comprometimento da gestão com o apoio à melhoria contínua das atividades de Gestão de Segurança da Informação na SEE/PE.

A Política de Segurança da Informação (PSI) e seus regulamentos específicos aplicam-se a todas as unidades do órgão, incluindo a Sede, Gres, Anexos e Escolas. Essa abrangência engloba estudantes, professores da rede de ensino, funcionários públicos, prestadores de serviços, terceirizados, estagiários, jovens aprendizes e qualquer outra parte que tenha acesso físico ou remoto a informações, sistemas e infraestrutura da SEE/PE (como computadores, data centers, servidores, estações de trabalho, equipamentos, pessoal, informações e recursos relacionados) e/ou desempenhe atividades de tratamento de informações produzidas ou recebidas pela SEE/PE.

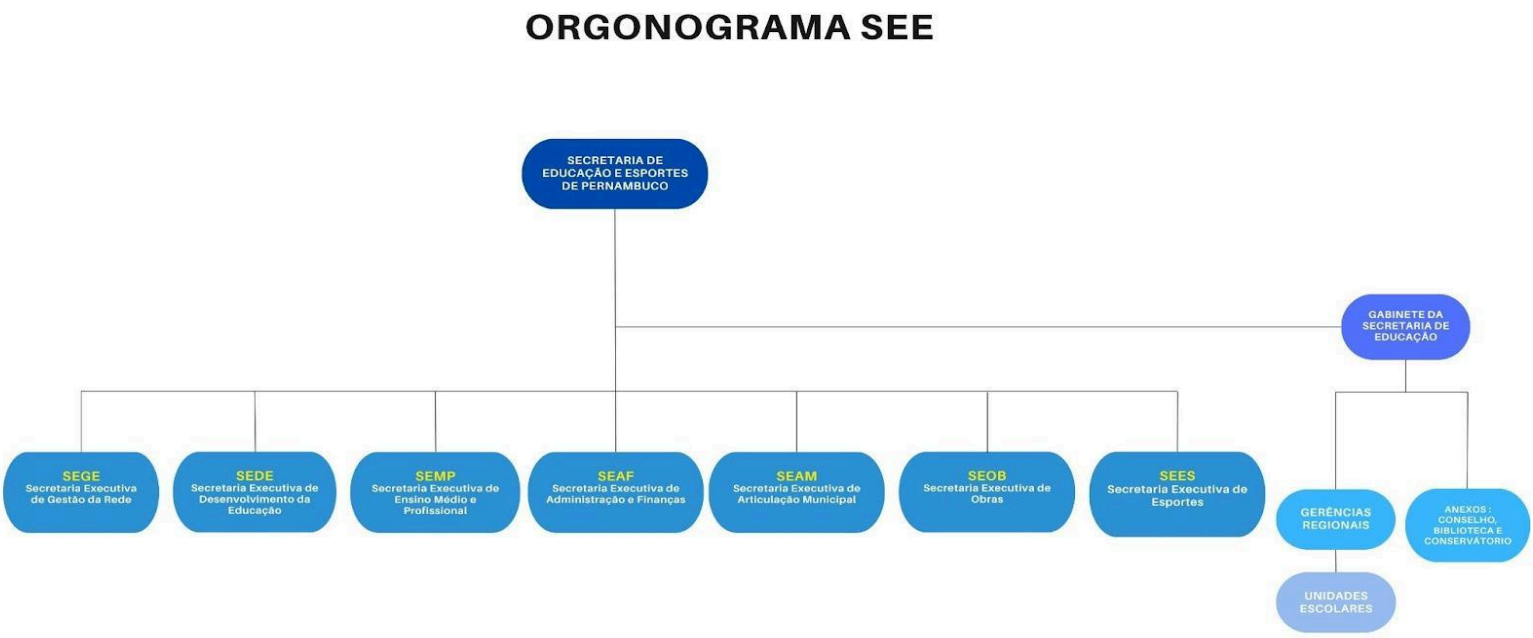

Imagem 1: Organograma da SEE/PE

2. CONCEITOS E DEFINIÇÕES:

Para efeitos da Política de Segurança da Informação da SEE/PE, considera-se:

TERMO	DEFINIÇÃO
Acesso	Regras apropriadas do controle de acesso, direitos de acesso e restrições para papéis específicos dos usuários acessarem seus ativos, com o nível de detalhe e o rigor dos controles que reflitam os riscos de segurança da informação associados.
Ameaça	Evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas.
Ataque	Tentativa não autorizada, com ou sem êxito, de destruir, alterar, desativar ou obter acesso a um ativo (4) ou qualquer tentativa de expor, roubar ou fazer uso não autorizado de um ativo.
Ativos	Qualquer coisa, material ou imaterial, que tenha valor para a organização, incluindo informações, processos e atividades de negócio.
Ativos de TIC	Equipamentos de informática e comunicação, servidores físicos ou virtuais, sistemas e/ou serviços de TIC, softwares, e-mail corporativo, rede local ou internet corporativa, além da própria informação produzida ou armazenada em formato físico ou digital, levando em consideração os ativos que estão cadastrados no Banco de Dados do Gerenciamento de Configuração (BDGC).
Autenticação	Processo que verifica se o usuário identificado é realmente quem ele diz ser, através do uso de sua senha pessoal ou de outros mecanismos (ex.: tokens e smartcards).
Backup	Cópia de segurança de arquivos e sistema
BYOD (Bring Your Own Device)	Traduzido literalmente como “traga seu próprio dispositivo”, refere-se à utilização de dispositivos pessoais no ambiente de trabalho.
Classificação	Atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação.
Confidencialidade	Garantia de que o acesso à informação seja obtido somente por pessoas e processos autorizados.
Controle de Acesso	Meios para assegurar que o acesso físico e lógico a ativos (4.4) é autorizado e restringido com base em requisitos de segurança do negócio e da informação.
Controles	São políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, de natureza administrativa, técnica, de gestão ou legal, com vistas a manter e/ou modificar os riscos identificados.

Credencial de segurança	Certificado, concedido por autoridade competente, que habilita determinada pessoa a ter acesso a dados ou informações em diferentes graus de sigilo.
Disponibilidade	Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos de TIC correspondentes sempre que necessário.
Grau de sigilo	Gradação de segurança atribuída a dados, informações, área ou instalação considerados sigilosos em decorrência de sua natureza ou conteúdo.
Incidente de segurança	Indício de fraude, sabotagem, desvio, falha, perda, evento indesejável ou inesperado que tenha probabilidade de comprometer sistemas de informação ou de redes de computadores.
Informações confidenciais	Informações que não se destinam a ser disponibilizadas ou divulgadas a pessoas, entidades ou processos não autorizados.
Integridade	Incolumidade de dados ou informações na origem, no trânsito ou no destino. As informações não devem ser modificadas ou destruídas sem autorização, devem ser legítimas e permanecer consistentes.
Não-repúdio	Capacidade de provar a ocorrência de um evento ou ação alegados e as suas entidades de origem.
Risco	A combinação da probabilidade de um evento ocorrer quando uma ameaça explora uma vulnerabilidade e o impacto de tal evento na organização.
Senha ou palavra-chave	É uma palavra ou uma ação secreta previamente convencionada entre duas partes como forma de reconhecimento, sendo senhas amplamente utilizadas em sistemas de computação para autenticar usuários e permitir-lhes o acesso a informações personalizadas armazenadas no sistema.
Sigilo	Segredo de conhecimento restrito a pessoas credenciadas e protegido contra revelação não autorizada**.**
Sistemas de Informação	Conjunto de aplicações, serviços, ativos de tecnologias da informação ou outros componentes de tratamento da informação.
Usuário	Qualquer parte interessada que tenha acesso aos sistemas de informação da organização.
Vulnerabilidade	Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

Tabela 1: Termos e definições

3. REFERÊNCIAS LEGAIS:

NORMA	DEFINIÇÃO
Lei Estadual nº 14.804, de 29 de outubro de 2012.	Regula o acesso a informações, no âmbito do Poder Executivo Estadual, e dá outras providências.
Lei Federal nº 12.965, de 23 de abril de 2014	Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
Lei Federal nº 13.709, de 14 de agosto de 2018	Dispõe sobre o tratamento de dados pessoais no âmbito federal - LGPD.
Decreto nº 9.637, de 26 de dezembro de 2018	Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997.
Decreto Estadual nº 49.265, de 6 de agosto de 2020	Institui a Política Estadual de Proteção de Dados Pessoais do Poder Executivo Estadual.
Decreto Estadual nº 49.914, de 10 de dezembro de 2020	Institui a Política Estadual de Segurança da Informação – PESI, no âmbito da administração pública estadual.
Decreto Nacional Nº 11.856, de 26 de dezembro de 2023	Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança.
Controles CIS Versão 8	Conjunto de melhores práticas de segurança cibernética desenvolvidas pelo Center for Internet Security (CIS) para ajudar as organizações a protegerem seus sistemas e dados contra ameaças cibernéticas.
Control Objectives For Information and Related Technology - COBIT 2019	Framework de governança de TI que fornece princípios e diretrizes para ajudar as organizações a alcançarem seus objetivos através da efetiva gestão e controle de seus sistemas de informação.
ISO/IEC 27002:2022	Norma internacional que fornece diretrizes e boas práticas para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação numa organização o SGSI.
ISO/IEC 27701:2019	Norma internacional que estende os requisitos do Sistema de Gestão de Segurança da Informação (SGSI) da ISO/IEC 27001 para incluir diretrizes específicas sobre o gerenciamento de informações pessoais.

Tabela 2: Referências Legais e Normativas

4. PRINCÍPIOS:

A segurança das informações processadas, armazenadas e transmitidas na SEE/PE deverá ser implantada em conformidade com os seguintes princípios:

a) Disponibilidade da informação;
b) Integridade da informação;
c) Autenticidade da Informação;
d) Não-repúdio;
e) Prevenção; e
f) Privacidade.

5. OBJETIVOS:

São objetivos da Política de Segurança da Informação da SEE/PE:

a) Tornar a segurança da informação um insumo no planejamento das atividades da SEE/PE, garantindo a confidencialidade, a integridade, a autenticidade e a disponibilidade das soluções e dos dados utilizados para o processamento, o armazenamento e a transmissão eletrônica ou digital de informações no âmbito desta Secretaria;

b) Fortalecer a integridade institucional, promovendo simultaneamente a proteção dos direitos individuais de cada titular de dados, por meio do diagnóstico de vulnerabilidades, da gestão do risco corporativo e da segurança da informação na SEE-PE;

c) Definir os padrões mínimos obrigatórios para o devido uso e proteção das informações criadas, recebidas, armazenadas, processadas, transmitidas ou impressas na SEE-PE;

d) Estabelecer as competências e as atribuições dos atores envolvidos nesta política;

e) Elencar os controles necessários para atingir um padrão aceitável de segurança da informação, conforme as legislações existentes e os padrões que o mercado estabelece;

f) Difundir no órgão os aspectos relacionados à segurança da informação, assegurar a prevenção de incidentes e de ataques cibernéticos e incrementar a resiliência da SEE/PE a incidentes e ataques;

g) Assegurar a permanente adequação, suficiência e eficácia da direção e do apoio da gestão para a segurança da informação, de acordo com os requisitos legais, estatutários, regulamentares e contratuais; e

h) Fortalecer a educação e o desenvolvimento tecnológico em segurança cibernética; e a cooperação entre órgãos e entidades, públicas e privadas, em matéria de segurança cibernética.

As informações produzidas por esta Secretaria, em sua forma eletrônica, escrita ou falada, são consideradas parte do órgão, tendo este a propriedade legal sobre a informação.

A Política de Segurança da Informação da SEE/PE considerará os controles internos de gestão e será apoiada por normas específicas ou procedimentos dos temas que exigem a implementação de controles de segurança da informação adequados aos riscos identificados.

A Política de Segurança da Informação adotará a Política de Proteção de Dados Pessoais da SEE/PE, alinhando-se aos requisitos estabelecidos nas normas ISO/IEC 27001:2022 e ISO/IEC 27701:2019, de acordo com o contexto da organização. Isso visa assegurar a conformidade nos aspectos de privacidade de dados pessoais.

6. DIRETRIZES GERAIS:

A SEE/PE se compromete com a garantia da proteção adequada utilizando um Sistema de Gestão de Segurança da Informação (SGSI) robusto e alinhado com os requisitos da ISO/IEC 27001:2022, 27002:2022 e ISO/IEC 27701:2019, suportada e mantida com apoio da alta direção, tendo como requisitos:

a) Comprometimento da alta direção no estabelecimento de política de segurança da informação, atribuição de papéis e responsabilidades e provisão de recursos, competências, conscientização e comunicação interna sobre segurança da informação.

b) Estabelecimento de objetivos de segurança da informação e desenvolvimento de um plano de tratamento de riscos.

c) Implementação e execução de controles e medidas de segurança para atender aos requisitos de segurança da informação.

d) Avaliação de Desempenho e Gestão da Qualidade, realizando monitoramento, medição, análise e avaliação do desempenho do SGSI.

e) Implementação de ações de treinamento, capacitação e melhoria contínua do desempenho do SGSI.

f) Tratamento de Riscos, gerando Identificação, avaliação e tratamento dos riscos de segurança da informação.

g) Condução de auditorias internas para verificar a conformidade e eficácia do SGSI.

h) Revisão regular pela alta direção para garantir a eficácia e a relevância contínuas do SGSI.

Promover a implementação efetiva da Política de Segurança da Informação considerando os planos operacionais que abrangem áreas críticas de segurança da informação:

a) Plano de Gerenciamento de Incidentes de Segurança da Informação (PGISI): Detalha os processos para identificar, relatar e responder a incidentes de segurança, minimizando impactos.

b) Plano de Conscientização em Segurança da Informação (PCSI): Estabelece programas educativos para promover a conscientização e o treinamento da equipe.

c) Plano de Administração da Crise (PAC): Estabelece o plano e os procedimentos para a correta gestão de crise por meio do comitê gestor de crise, em concomitância com o PCN e PRD:

I. Plano de Continuidade de Negócios (PCN): Define os procedimentos para garantir a continuidade das operações críticas da organização em situações adversas.

II. Plano de Recuperação de Desastres (PRD): Estabelece diretrizes para a recuperação eficiente de sistemas e dados após eventos catastróficos.

7. PENALIDADES:

O descumprimento do estabelecido na Política de Segurança da Informação por parte dos usuários poderá acarretar sanções administrativas disciplinares e/ou contratuais, sem prejuízo das responsabilizações nas esferas civil e criminal.

8. COMPETÊNCIAS E RESPONSABILIDADES:

Atribui-se às competências e responsabilidades para o gerenciamento da segurança da informação e privacidade na SEE/PE aos seguintes atores:

a) Comitê Estratégico de Governança Digital (CEGD) (PORTARIA SEE Nº 5375 DE 01 DE DEZEMBRO DE 2023);

b) Comitê Gestor de Proteção de Dados (CGPD) (PORTARIA SEE Nº 1782, DE 22 DE ABRIL DE 2021);

c) Gestor do Processo de Segurança da Informação;

d) Equipe Técnica de TIC; e

e) Usuários.

Ao Comitê Estratégico de Governança Digital compete as seguintes funções:

a) Coordenar a formulação de propostas políticas, diretrizes, objetivos e estratégias de Tecnologia da Informação, Comunicação e Governança Digital, em alinhamento à missão, às estratégias e às metas da SEE-PE;

b) Analisar e acompanhar a execução do plano de metas de Tecnologia da Informação, Comunicação e Governança Digital;

c) Coordenar a elaboração, priorização, revisão e a aprovação do Plano Diretor de Tecnologia da Informação (PDTI) da SEE-PE, alinhado com ao Plano de Ações de Metas aprovado para o período;

d) Priorizar as destinações orçamentárias dos recursos em tecnologia da informação, comunicação e governança digital desta SEE-PE;

e) Priorizar ações de capacitação para implantação e manutenção das soluções de tecnologia da informação, comunicação, segurança da informação, privacidade de dados e governança digital;

f) Estabelecer prioridades no atendimento às demandas por soluções de tecnologia da informação comunicação e governança digital, em consonância com a capacidade operacional da SEE-PE;

g) Analisar, manifestar-se a respeito, para aprovação, demandas que tratam do provimento centralizado de soluções de TI de natureza corporativa, assim como demandas de manutenção com impacto significativo sobre os planos de TI;

h) Promover a transformação digital e estimular o uso de soluções digitais na gestão e prestação de serviços no âmbito da SEE-PE;

i) Criar grupos de trabalho e subcomitês para auxiliar o Comitê Gestor de Governança Digital em suas decisões;

j) Elaborar o Regimento Interno do Comitê Estratégico de Governança Digital;

k) Propor e/ou apreciar diretrizes, metas, planos e normas para o desenvolvimento e implantação da Política de Tecnologia da Informação e Comunicação;

l) Aprovar políticas, planos e ações de segurança da informação, privacidade de dados e comunicação;

m) Aprovar atividades de planejamento, gestão, controle, riscos e auditoria na área de Tecnologia da Informação e Comunicação quanto na definição e uso dos serviços, sistemas, softwares, aplicativos e infraestruturas, em relação a segurança da informação da SEE-PE; e

n) Promover e apoiar a implantação do SGSI - Sistema de Gestão de Segurança da informação.

Ao Comitê Gestor de Proteção de Dados (CGPD) compete as seguintes funções:

a) Avaliar os mecanismos de tratamento e proteção dos dados existentes e propor diretrizes, políticas, estratégias e metas para a conformidade da SEE/PE com a legislação de proteção de dados pessoais;

b) Supervisionar a execução dos planos, dos projetos e das ações aprovadas para viabilizar a implantação das diretrizes previstas na Política Estadual de Proteção de Dados Pessoais;

c) Apoiar o encarregado designado pelo órgão na prestação de informações sobre o tratamento e a proteção de dados pessoais; e

d) Aprovar políticas, normas e diretrizes de Segurança da Informação que estejam relacionadas à privacidade e proteção de dados pessoais.

Ao Gestor do Processo de Segurança da Informação compete as seguintes funções:

a) Gerenciar as informações sob sua competência;

b) Autorizar aos usuários o acesso às informações sob sua competência;

c) Realizar, em conjunto com a Equipe Técnica de TIC, a avaliação de riscos de segurança da informação;

d) Elaborar e informar mudanças de perfis de acessos de sua respectiva área ou setor;

e) Classificar a informação sob sua competência, de modo a estabelecer como essas informações podem ser acessadas e administradas, garantindo a segurança da acessibilidade e disponibilidade destas;

f) Promover medidas de mitigação de riscos de segurança da informação;

g) Divulgar normas e procedimentos específicos definidos pela SEE-PE aos usuários sob sua responsabilidade;

h) Notificar à Equipe Técnica de TIC sobre quaisquer incidentes de segurança que envolvam os ativos de TIC sob sua responsabilidade; e

i) Gerenciar as medidas de mitigação de riscos de segurança da informação e avaliar os resultados dos processos sob sua responsabilidade.

À Equipe Técnica de TIC, composta pelos colaboradores da área de tecnologia da informação, compete:

a) Implementar medidas técnicas de segurança solicitadas, com base no valor associado às informações e no impacto oriundo da indisponibilidade ou perda dessas informações;

b) Promover orientação técnica relacionada à segurança da informação;

c) Realizar, em conjunto ao Gestor de Processo, a avaliação de riscos de segurança da informação;

d) Acompanhar e analisar as transações e alterações relacionadas à segurança da informação, para fins de rastreamento e auditoria;

e) Realizar, periodicamente, monitoramento de segurança no ambiente tecnológico;

f) Priorizar medidas preventivas, em detrimento de controles reativos;

g) Apoiar as ações de capacitação na área de Segurança da Informação;

h) Produzir documentação técnica e pareceres referente a Segurança da Informação e Privacidade;

i) Apoiar na elaboração de política, normas , processos e procedimentos concernentes à Segurança da Informação e Privacidade;

j) Viabilizar monitoração e controles com soluções técnicas que não dependam de processos manuais ou não estejam sujeitas a falhas humanas;

k) Apoiar a definição das medidas técnicas de segurança da informação nas aquisições de bens e na contratação de serviços que envolvam ativos de TIC.

Compete aos usuários:

a) Fazer boa utilização dos ativos de informação, prezando sempre pela segurança da informação;
b) Manter-se atualizado sobre as bos práticas e políticas específicas de segurança;
c) Ser responsável por sua senha pessoal;
d) Evitar expor ou compartilhar informações sigilosas ou restritas;
e) Ter ciência da existência de consequências provenientes do uso inadequado dos sistemas computacionais e de informações;
f) Cumprir normas e procedimentos relacionados ao uso de informações e sistemas associados, em conformidade com o estabelecido nesta política e dela derivada.
g) Informar, imediatamente, à Equipe Técnica de TIC qualquer falha em dispositivo, serviço ou processo relacionado à segurança da informação para que providências sejam tomadas em caráter de urgência.

9. NORMAS COMPLEMENTARES:

As normas e os regulamentos complementares deverão estar alinhadas à Política de Segurança da Informação, além de atualizadas, e serão divulgadas na rede interna da SEE-PE. São normas complementares à Política de Segurança da Informação (PSI):

a) Norma de Uso de Senhas: tem como objetivo definir as regras de criação, concessão, proteção, uso e reinicialização de senhas pelos usuários;
b) Norma de Resposta a Incidentes de Segurança da Informação: tem como objetivo definir a estrutura de prevenção, identificação, tratamento e resposta a incidentes de Segurança da Informação na SEE/PE;
c) Norma de Uso da Internet: tem como objetivo estabelecer regras e controles para o uso aceitável da Internet, em conformidade com o estabelecido no Decreto nº 8.771, de 11 de maio de 2016 da Presidência da República, que Regulamenta a Lei no 12.965, de 23 de abril de 2014 (Marco Civil da Internet) e o Decreto nº 40.654, de 29 de abril de 2014, do Governo do Estado de Pernambuco;
d) Norma de Acesso Remoto: tem como objetivo definir as regras de quem e como pode utilizar este serviço de que forma os casos de exceção serão tratados;
e) Norma de Controle de Acesso: tem como objetivo especificar o padrão, as regras e controles que devem ser utilizados para a concessão, alteração, bloqueio e remoção dos acessos lógicos aos sistemas da SEE-PE e acessos físicos às instalações críticas da GGTI, assim como os respectivos responsáveis;
f) Norma de Uso de Dispositivos Móveis: tem como objetivo especificar as regras para utilização de equipamentos pessoais na SEE-PE e tratar a necessidade e tendência crescente do BYOD, principalmente se tratando do ambiente escolar;
g) Norma de Backup Corporativo: tem por objetivo definir as regras concernentes ao backup e restore, período de retenção, periodicidade, responsabilidade, etc.;
h) Norma de Combate a Softwares Maliciosos: tem por objetivo definir as regras para a prevenção e combate à softwares maliciosos na SEE/PE;
i) Norma de Uso de E-mail Institucional: tem como objetivo especificar o padrão e as regras utilizadas para o uso aceitável do correio eletrônico e em conformidade com a política de uso do correio eletrônico estabelecida na ATI;
j) Norma de Gestão de ativos: tem por objetivo comunicar aos usuários de Tecnologia da Informação a utilização aceitável dos recursos de tecnologia da informação, como por exemplo: computadores, servidores, softwares, sistemas e redes. O que é aceitável e o que não será permitido, por não estar em conformidade com os padrões mínimos de segurança; e estabelecer o descritivo dos controles de proteção dos ativos da organização por meio do estabelecimento e manutenção de inventários e definição dos proprietários desses ativos,

visando à manutenção de informações e a eficácia dos controles de segurança, assegurando a proteção adequada;

k) Norma de Classificação da Informação: tem como objetivo definir as regras, responsáveis e níveis de concessão de acesso no uso seguro de informações sensíveis, como forma de criar a cultura de classificação da informação na SEE-PE.

10. CONSIDERAÇÕES FINAIS:

A PSI e suas normas complementares devem ser mantidas e implementadas de forma contínua, buscando manter o alinhamento com a evolução da tecnologia e de seus riscos, identificando fatores internos e externos que podem impactar no alcance dos objetivos do órgão ou da entidade.

A PSI deverá passar por revisões periódicas em até 2 (dois) anos da data da sua publicação, ou quando a Equipe Técnica de TIC e/ou o Comitê Estratégico de Governança Digital ou o Comitê Gestor de Proteção de Dados considerar necessário, para permanecer atualizada com os avanços tecnológicos e fatos que necessitem revisão de controles, ameaças, riscos e diretrizes.

A revisão periódica deverá ser realizada pela Equipe Técnica, com o apoio do Comitê Estratégico de Governança Digital.

Deverá ser realizado processo de avaliação periódica de aderência à PSI pelo público alvo do documento, contemplando todos que estão submetidos à norma. Esta avaliação tem como objetivo perceber pontos de melhoria e dificuldades enfrentadas pelos usuários, para que possam ser tratadas no processo de revisão.