NORMA DE USO DO E-MAIL CORPORATIVO

Secretaria de Educação e Esportes

GOVERNO DE PERNAMBUCO
ESTADO DE MUDANÇA

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	Criação do documento.

1 DISPOSIÇÕES GERAIS

O e-mail é uma das formas essenciais de comunicação no dia-a-dia da Secretaria de Educação e Esporte de Pernambuco (SEE-PE). Por esse motivo, seu uso deve ser exclusivamente institucional, garantindo um ambiente seguro e controlado, com a possibilidade de recuperação de mensagens, se necessário. Devido à sua relevância, este recurso deve ser utilizado corretamente e com os devidos cuidados, uma vez que é o principal meio de interação do nosso ambiente tecnológico com o mundo externo, tornando-se um alvo frequente de tentativas de invasão.

O mau uso do e-mail pode apresentar riscos à segurança do ambiente tecnológico, como a contaminação por vírus em mensagens com arquivos maliciosos ou a disseminação de conteúdo discriminatório, podendo acarretar na indisponibilidade de sistemas e serviços de TI, e no vazamento de dados pessoais e informações sigilosas da secretaria.

Esta norma de uso de e-mail faz parte da Política de Segurança da Informação - PSI da SEE-PE e deve ser respeitada. Todos os usuários que necessitem de acesso aos recursos tecnológicos de correio eletrônico na rede da SEE-PE devem seguir os padrões aqui estabelecidos. Diante do exposto, os usuários devem observar as condutas aceitáveis na utilização do e-mail institucional, realizando o correto procedimento para inclusão adequada de novos colaboradores, bloqueio efetivo de usuários que não fazem mais parte da SEE-PE e a devida solicitação de transferência ou modificação de perfil funcional.

2 OBJETIVO

Reconhecer a importância da utilização do e-mail institucional e estabelecer os padrões mínimos de segurança e privacidade, visando minimizar os riscos, especialmente quando se trata do uso de e-mails de outros domínios que não são controlados pela SEE-PE. Além disso, pretende-se conscientizar os usuários sobre os requisitos e os padrões de segurança a serem adotados na transferência e armazenamento de mensagens.

3 ESCOPO

Esta norma aplica-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.

O objetivo é assegurar uma abordagem inclusiva que contemple todos os envolvidos, garantindo a aplicação consistente das boas práticas em segurança da informação e preservando a integridade de nossos dados e sistemas.

O objetivo é assegurar uma abordagem inclusiva que contemple todos os envolvidos, garantindo a aplicação consistente das boas práticas em segurança da informação e preservando a integridade de nossos dados e sistemas.

4 CONCEITOS E DEFINIÇÕES

TERMO	DEFINIÇÃO
Endereço de e-mail institucional	É aquele que pertence ao domínio da Secretaria de Educação e Esportes de Pernambuco.
Caixa postal	Área de armazenamento que contém as mensagens do correio eletrônico corporativo.
Lista de distribuição	Agrupamento de diversas caixas postais em um único endereço que, uma vez inserido como destinatário de uma mensagem, permite a distribuição desta mensagem a todas as caixas postais integrantes da lista.
Phishing	Tipo de ataque cibernético que utiliza engenharia social, onde um criminoso finge fazer parte de uma instituição legítima para convencer as vítimas a entregarem suas informações pessoais, por meio de mensagens e sites.
Central de Serviços	Central de atendimento ao usuário para registros de chamados.
Spam	É a prática que consiste em utilizar meios eletrônicos para enviar mensagens de publicidade em massa, que podem ser utilizadas para fins de ataque cibernético.
Extensões de arquivos	Caracteres que aparecem após o nome do arquivo, como sufixo, que identificam o tipo de formato e a função que desempenham.

Tabela 1: Termos e Definições

5 REFERÊNCIAS LEGAIS E DE BOAS PRÁTICAS

ORIENTAÇÃO	SECÇÃO
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – Art. 46, Seção II art. 50
Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Anexo, art.3, Inciso I
Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	Art.4, Art.5, Art.6 , Art.7 e Art.8
Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER)	Anexo, Item 2.3.4 Anexo, Parte II , Item 1.2
ABNT NBR ISO/IEC 27002: 2022. Código de Prática para controles de Segurança da Informação	Observando alguns objetos dos controles 5.1 ,5.15 ,5.16, 5.17, 5.18, 8.2, 8.3, 8.5
CIS (Center for Internet Security)	CIS Control 3,7 e 11

Tabela 2: Referências Legais

6 DESCRIÇÃO DA NORMA

6.1 USO DO E-MAIL CORPORATIVO

a) Acesso aos sistemas e informações deve ser concedido com base no princípio do "mínimo privilégio", ou seja, os usuários terão acesso apenas ao que for necessário para desempenhar suas funções;

b) Senhas deverão seguir as normas institucionais, conforme diretrizes da PSI, devendo ser complexas, alteradas periodicamente e não compartilhadas. A autenticação de dois fatores deve ser utilizada sempre que possível;

c) Cada usuário deve possuir sua própria conta de e-mail institucional;

d) O serviço de e-mail utilizado deve ser obrigatoriamente registrado no domínio institucional da SEE-PE (adm.educacao.pe.gov.br; educacao.pe.gov.br; professor.educacao.pe.gov.br);

e) A solução de e-mail institucional deve disponibilizar os seguintes recursos mínimos necessários para atender às demandas das atividades referentes ao trabalho dos usuários da SEE-PE:

I. Tamanho (espaço) de caixa postal por usuário;
II. Tamanho máximo de envio e recebimento de mensagens;
III. Cópia de segurança das caixas postais;
IV. Administração e gerenciamento dos usuários com controle de nível de Acesso;
V. Aviso de encaminhamento a destinatários que estão fora do domínio ; e
VI. Tempo de retenção das caixas postais.

f) O aplicativo gerenciador de e-mails, web ou local, que permite enviar, receber e personalizar as mensagens, pode ser o Expresso, Sogo, Gmail ou outro equivalente. Para uso de ferramentas locais, é essencial a abertura de um chamado na Central de Serviços, a fim de que as configurações sejam realizadas de acordo com os devidos padrões de segurança. O software adotado deve ser mantido atualizado com as últimas correções de segurança;

g) É proibido a utilização de e-mail não institucional para fins de divulgação em sites ou comunicações em processos corporativos desta secretaria, ex: licitacao.see@gmail.com, compras.see@hotmail.com, matricula.see@bol.com.br, setor.see@yahoo.com;

h) As listas de distribuição devem ter um responsável designado para responder pelo conteúdo das mensagens da lista;

i) As caixas postais dos usuários são de uso individual e não devem ser acessadas sem autorização destes ou dos respectivos gestores de áreas ou superiores;

j) Todas as mensagens enviadas pelos usuários da SEE-PE, por meio do e-mail institucional, devem estar em conformidade com os procedimentos de segurança da informação, privacidade e legislações aplicáveis, incluindo o cuidado com os direitos autorais;

k) É estritamente proibido o envio de mensagens ilegais, fraudulentas, difamatórias, bem como mensagens contendo phishing, spam (conteúdo indesejado), correntes, credenciais de acesso (conta e senha) e informações confidenciais;

l) O envio de dados pessoais ou dados pessoais sensíveis **não consentidos** ou **não previstos em base legal**, como origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organizações de caráter religioso, filosófico ou político partidário, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando relacionados a um indivíduo, não deve ser realizado por meio da ferramenta de e-mail institucional;

m) Arquivos com código executável, como aqueles com extensões .exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf e outros, geralmente utilizados por vírus, devem ser automaticamente bloqueados pelos mecanismos segurança do e-mail, evitadas de ser enviada(s) ou reenviada(s) pelos usuários;

n) Não acessar mensagens de e-mail com remetentes desconhecidos ou conhecidos que contenham conteúdos, arquivos ou link suspeitos, que possam representar uma ameaça;

o) Após o desligamento de um colaborador, o respectivo gestor da área ou superior deve entrar em contato com a Central de Serviços e informar o desligamento, requerendo que a conta do respectivo usuário seja desabilitada, assim como descreve o processo para solicitação de bloqueio ou desativação;

p) As caixas postais eletrônicas desabilitadas passarão por avaliação, dentro dos pré requisitos legais, para sua devida exclusão;

q) No encerramento do vínculo de servidores públicos e estudantes ou em caso de inativação por penalidade, se houver, o conteúdo armazenado no drive de cunho pessoal deverá ser

migrado pelo usuário para outro ambiente ou mídia no prazo de até 30 (trinta) dias corridos. Após esse período, a conta e os arquivos poderão ser excluídos de forma permanente. Os colaboradores terceirizados poderão ter sua conta excluída imediatamente após a solicitação de bloqueio;

r) Será permitida a edição de mensagens automáticas para serem enviadas ao remetente, informando a sua condição de ausência temporária dos colaboradores devido a férias ou licença;

s) É proibido para **usuários não autorizados** o acesso às caixas postais eletrônicas desabilitadas. Caso seja necessária alguma informação das respectivas caixas postais, o gestor de área ou superior deve formalizar solicitação, informando o conteúdo, para que, após análise pela área técnica, seja disponibilizado ou não;

t) As contas de correio eletrônico que não forem utilizadas por um determinado período de tempo, poderão ser desabilitadas automaticamente. Caso seja necessária a reativação, a Central de Serviços deve ser acionada pelo respectivo gestor da área ou superior;

u) É proibido forjar qualquer informação do cabeçalho do remetente;

v) A comunicação de incidentes identificados através da ferramenta de e-mail deverá ser comunicada de forma imediata por meio de abertura de chamado na Central de Serviços, com nome, departamento, e-mail e telefone da pessoa que reporta o incidente, incluindo captura de tela da mensagem recebida;

w) Procedimentos claros e eficazes para lidar com incidentes de segurança devem ser estabelecidos e comunicados a todos os usuários pela área de tecnologia responsável;

x) Todos os usuários devem passar por treinamento regular de segurança da informação para entenderem as melhores práticas e os riscos associados.

7 PENALIDADES

O não cumprimento pelo usuário das normas estabelecidas neste documento, seja isolada ou cumulativamente, poderá ensejar, de acordo com a gravidade e reincidência da infração cometida, desde a exclusão/bloqueio do acesso do usuário até a abertura de procedimento disciplinar, a fim de apurar a responsabilidade do respectivo usuário e, se for o caso, o usuário responderá civil, penal e administrativamente pela má utilização das contas institucionais da SEE.

As infrações sujeitarão o infrator às seguintes sanções administrativas:

I - advertência;

II - Bloqueio temporário, por 24 horas; e

III - Inativação permanente da conta;

8 COMPETÊNCIAS E RESPONSABILIDADES

A Gerência Geral de Tecnologia da Informação e Comunicação - GGTIC é responsável por implementar e monitorar o cumprimento desta norma.

9 DISPOSIÇÕES FINAIS

Esta política entra em vigor a partir da data de sua aprovação e revoga qualquer disposição anterior.

Esta política será revisada anualmente ou sempre que houver necessidade, para garantir sua conformidade com as melhores práticas de segurança da informação.