POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE EDUCAÇÃO DE PERNAMBUCO

Faça disso um hábito!

SUMÁRIO

HISTÓRICO DE VERSÕES

DATA	VERSÃO	DESCRIÇÃO	AUTOR
15/02/17	1.0	Versão elaborada e publicada	Equipe de Elaboração
31/07/18	2.0	Versão revisada	Equipe de Elaboração

1. CONCEITOS, TERMOS E ABREVIAÇÕES

TERMOS/ABREVIAÇÕES	SIGNIFICADO
ABNT	Associação Brasileira de Normas Técnicas.
Agente Público	Que serve ao poder público como instrumento de sua vontade ou ação, independentemente do vínculo jurídico, podendo ser por nomeação, contratação, designação ou convocação. Independe, ainda, de ser essa função temporária ou permanente e com ou sem remuneração. Assim, quem quer que desempenhe funções estatais, enquanto as exercita.
Ambiente de Desenvolvimento	Ambiente tecnológico composto por um conjunto de ferramentas necessárias para criação e manutenção de sistemas de informação
Ambiente de teste	Ambiente tecnológico com configuração similar ao ambiente de desenvolvimento composto por um conjunto de ferramentas necessárias para que usuários recebam e validem versões de sistemas de informação instáveis, para garantir a equalização comportamental dos sistemas de informação em teste.
Ambiente de Homologação	Ambiente tecnológico similar ao ambiente de produção, que possa simular situações muito próximas das que se encontra no dia a dia, composto por um conjunto de ferramentas necessárias para que usuários recebam e validem versões de sistemas de informação.
Ambiente de produção	Entende-se por ambiente de produção o conjunto composto de ferramentas necessárias para que usuários recebam versões finais de sistemas de informação que serão utilizadas no seu dia a dia;
Ameaça	Risco potencial de um incidente indesejado que pode resultar em dano para um sistema ou para a organização.
Aplicação	Programa de computador que auxilia o usuário a desempenhar uma atividade específica (ex.: AutoCAD, para a área de engenharia e arquitetura; Skype, para telefonemas e conferências).
Ativo	Qualquer coisa, material ou imaterial, que tenha valor para a organização.
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 sistemas
BYOD (*Bring Your Own Device*)	Traduzido literalmente como “traga seu próprio dispositivo móvel”, refere-se à utilização de dispositivos pessoais no ambiente de trabalho.
Colaborador	Termo utilizado no documento para Agente Público na Secretaria de Educação do Estado de Pernambuco.
Comitê de Acesso à Informação (CAI)	Comitê designado por ato do Governador do Estado de Pernambuco, conforme Decreto Estadual nº 38.787/2012, para analisar os Termos de Classificação da Informação (TCI), ratificando ou não as informações classificadas como ultrassecretas e secretas.
Confidencialidade	Termo utilizado em segurança da informação para garantir que as informações não sejam disponibilizadas ou divulgadas a pessoas ou processos não autorizados.
Contas de Serviço	Contas não associadas a usuários, que podem ter privilégios locais ou de domínio, usadas por um aplicativo ou serviço para interagir com o sistema operacional ou acessar recursos para realizar suas funcionalidades.
Disponibilidade	Termo utilizado em segurança da informação que garante que todas as informações e serviços importantes ao negócio estejam disponíveis, sempre que necessário, a pessoas e processos autorizados.

Evento de Segurança da Informação	Ocorrência identificada em um serviço ou rede que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação anteriormente desconhecida, que possa ser relevante para a segurança da informação.
FTP (*File Transfer Protocol*)	Traduzido literalmente como "protocolo de transferência de arquivos", trata-se de uma forma bastante rápida e versátil de transferir arquivos, sendo uma das mais usadas na Internet.
Gestor da Informação	Colaborador que exerce a chefia de área na Secretaria de Educação de Pernambuco (SEE-PE), responsável pela informação em sua área de competência.
ID	Conjunto de caracteres usados para identificar o usuário em um determinado sistema. Também pode ser chamado de *logon nam*e, *login name* ou *user name*.
Integridade	Termo utilizado em segurança da informação que garante que as informações estejam protegidas de modificações, manipulações ou reproduções não autorizadas.
Login	Processo que permite a identificação, autenticação e autorização de acesso a um determinado sistema por um usuário. Também pode ser chamado de *logon*.
Não-repúdio	Ato de evitar que uma entidade negue a execução de uma ação.
Negação de Serviço ou DoS (*Denial of Service*)	Técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet.
PC	Políticas Complementares
PSI	Política de Segurança da Informação
Restore	Recuperação de arquivos e sistemas.
SAD-PE	Secretaria de Administração do Estado de Pernambuco
SEE-PE	Secretaria de Educação do Estado de Pernambuco
Senha	Conjunto de caracteres usados para autenticar um usuário em um determinado sistema.
Sistemas de Informação	Todo aplicativo, software e sistemas de informação que sejam adquiridos, desenvolvidos ou mantidos pela equipe técnica da SEE-PE ou empresa por ela contratada.
Software	Um termo genérico para definir um programa de computador composto por uma sequência de instruções, que é interpretada e executada por um processador ou por uma máquina virtual. Essa sequência deve seguir padrões específicos que resultam em um comportamento desejado.
Sinistro	Fato que remete a um acidente ou desastre que cause prejuízo, podendo provocar perda, dor, morte ou dano material.
VPN (Rede Privada Virtual)	Conexão estabelecida sobre uma infraestrutura pública (internet), usando protocolos de criptografia por tunelamento que fornecem a confidencialidade, autenticação e integridade necessárias para garantir a privacidade das comunicações requeridas.

2. INTRODUÇÃO

São princípios para o Sistema de Gestão de Segurança da Informação a Confidencialidade, a Integridade e a Disponibilidade, conforme norma de mercado para a Segurança da Informação (NBR/ISO 27001-2013). Esses devem ser preservados, controlados e auditados para garantir que as informações estejam protegidas nas medidas exigidas para sua utilização na Secretária de Educação do Estado de Pernambuco (SEE-PE).

Esta Política de Segurança da Informação (PSI), em conjunto com as Políticas Complementares (PC), aprovada através da portaria SEE nº 1269 de 15 de fevereiro de 2017 e publicada em diário oficial (DO) no dia 16 de fevereiro de 2017, compreende as diretrizes e normas que servem de base para atender aos princípios fundamentais da Segurança da Informação da SEE-PE.

3. PRINCÍPIOS

A Política de Segurança da Informação tem por princípio a proteção dos dados, informações e conhecimento, classificados como sigilosos, além da preservação do direito pessoal e coletivo no que se refere à intimidade e ao sigilo das correspondências eletrônicas, informações e comunicações individuais.

4. OBJETIVOS

- Tornar a segurança da informação como um dos elementos fundamentais no planejamento estratégico da Secretaria de Educação de Pernambuco (SEE-PE);
- Definir os padrões mínimos obrigatórios para o devido uso e proteção das informações criadas, recebidas, armazenadas, processadas, transmitidas ou impressas na SEE-PE;
- Estabelecer as competências e atribuições dos atores envolvidos nesta política;
- Elencar os processos necessários para atingir um padrão aceitável de Segurança da Informação, conforme as legislações existentes e os padrões que o mercado estabelece;
- Difundir os aspectos relacionados à Segurança da Informação na SEE-PE.

5. ABRANGÊNCIA

Esta política se aplica a todos os colaboradores da SEE-PE, quais sejam: servidores públicos, estagiários, menor aprendiz, terceirizados ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, a infraestrutura ou as informações da SEE-PE. Todos esses colaboradores serão tratados nesta política como usuários.

6. ATRIBUIÇÕES

6.1. Comitê de TI

Formado por colaboradores indicados pelos respectivos Secretários Executivos juntamente com o gestor responsável para área de tecnologia da informação e comunicação ou seu representante, com o objetivo de deliberar a respeito de assuntos relacionados à tecnologia da informação e comunicação da SEE-PE. Assim deve:

a. Promover a disseminação e conscientização da segurança da informação;

b. Disponibilizar os recursos necessários para que ações de segurança da informação sejam executadas;

c. Coordenar a atualização da Política de Segurança da Informação (PSI), propondo revisão e novas políticas complementares, bem como procedimentos que assegurem o controle das ações de política de segurança da informação.

NOTA: A deliberação só se dará, se houver no mínimo 3(três) representantes presentes.

6.2. Gestores das Áreas

Formado pelos colaboradores que exercem a chefia de área ou setor na Secretaria de Educação de Pernambuco (SEE-PE), responsáveis pela informação em sua área de competência. Assim devem:

a. Gerenciar as informações sob sua competência;

b. Autorizar os colaboradores acesso ou decesso às informações sob sua competência;

c. Informar o desligamento dos colaboradores de sua respectiva área ou setor;

d. Indicar a classificação da informação sob sua competência, de modo a estabelecer como essas informações podem ser acessadas e administradas, garantindo a segurança da acessibilidade e disponibilidade destas.

6.3. Equipe Técnica

Formado por colaboradores da área de tecnologia da informação para:

a. Manter o ambiente tecnológico estável, operacional, atualizado, íntegro, disponível e monitorado;

b. Elaborar e atualizar os procedimentos relativos à operacionalidade do ambiente tecnológico;

c. Instalar e configurar os ativos de software e hardware necessários à operacionalidade do ambiente tecnológico;

d. Relatar mensalmente ao Comitê de TI ou representante indicado os incidentes de Segurança da Informação identificados, ocorridos no ambiente tecnológico.

6.4. Usuários

Todos os colaboradores da SEE-PE, quais sejam: servidores públicos, estagiários, menor aprendiz, terceirizados ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, a infraestrutura ou as informações da SEE-PE.

a. Cumprir as normas e procedimentos relacionados ao uso de informações e sistemas associados, em conformidade com o estabelecido nesta política;

b. Informar, imediatamente, à Central de Atendimento qualquer falha em dispositivo, serviço ou processo relacionado à Segurança da Informação para que uma ação seja tomada urgentemente;

c. Utilizar as informações como patrimônio da SEE-PE e mantê-las disponíveis, conforme sua classificação.

6.5. Equipe de Segurança da Informação

Formada por equipe multidisciplinar de funcionários públicos ou comissionados, indicados pelos respectivos Secretários Executivos, com o objetivo de deliberar a respeito de assuntos relacionados à segurança da informação da SEE-PE. Assim deve:

a. Implementar mecanismos de segurança com base no valor associado às informações e ao impacto oriundo da perda dessas informações;

b. Promover instrução relacionada à Segurança da Informação;

c. Acompanhar e analisar as transações e alterações relacionadas à Segurança da Informação, para fins de rastreamento e auditoria;

d. Realizar, periodicamente, monitoramento e auditoria de segurança no ambiente tecnológico;

e. Priorizar medidas preventivas, em detrimento de controles reativos;

f. Viabilizar monitoração e controles com soluções técnicas que não dependam de processos manuais ou não estejam sujeitas a erros humanos.

NOTA: A deliberação só se dará, se houver no mínimo 3(três) representantes presentes.

7. DIRETRIZES

a. Cabe a cada usuário vinculado à SEE-PE zelar e proteger as informações criadas, manuseadas, tramitadas e guardadas no exercício de suas atividades, agindo no sentido de preservar as diretrizes e normas que estão relacionadas à segurança dessa informação, pois são de propriedade da SEE-PE;

b. A Política de Segurança da Informação da SEE-PE parte do pressuposto de atender às leis e regulamentações no âmbito federal e estadual, além de seguir as melhores práticas do mercado oriundas de recomendações tratadas em diretrizes e normas estabelecidas em padrões técnicos de mercado;

c. Os direitos de propriedade intelectual devem ser preservados, conforme legislações e acordos contratuais;

d. A SEE-PE deve manter todos os licenciamentos apropriados na utilização de seus recursos e todos os usuários devem honrar os direitos de propriedade intelectual, bem como relatar à Central de Serviço se houver conhecimento de quaisquer violações;

e. Os contratos e termos de confidencialidade e/ou responsabilidade devem ser respeitados por todos os usuários ligados à SEE-PE;

f. A segurança da informação deve fazer parte da rotina diária dos usuários ligados à SEE-PE, buscando garantir a disponibilidade, confidencialidade e integridade;

g. Qualquer violação da Política de Segurança da Informação deve ser relatada à Central de Serviços para que ações urgentes sejam tomadas na preservação dos aspectos de Segurança da Informação da SEE-PE;

h. Os acessos aos ambientes tecnológicos devem ser realizados através de autenticação (ID e senha, logon e senha, digital, etc.) e de acordo com o perfil funcional do usuário, sendo a autenticação pessoal e intransferível;

i. O gestor da área deve analisar e classificar as informações sob sua competência, conforme grau de importância em relação ao impacto de sua divulgação;

j. A utilização de serviços de conectividade (ex.: internet, e-mail, etc.) deve ser restrita, controlada e voltada às atividades de trabalho do usuário;

k. Todos os equipamentos disponibilizados pela SEE-PE às respectivas áreas devem ser utilizados no exercício das atividades de trabalho e ter um responsável;

l. O desenvolvimento, aquisição e manutenção das aplicações sistêmicas devem estar em conformidade com as legislações, regulamentações, contratos, acordos e procedimentos existentes, que preservem entre as respectivas partes os princípios base da segurança da informação;

m. Como forma de garantir e preservar a segurança da informação, o ambiente tecnológico deve ser monitorado e auditado periodicamente;

n. A Política de Segurança da Informação deverá ser revisada a cada 3(três) anos, ou quando a Equipe de Segurança da Informação e/ou o Comitê de TI achar necessário, assim como todos os outros documentos relacionados devem estar disponíveis a todos os usuários;

o. O não cumprimento do estabelecido na Política de Segurança da Informação da SEE-PE poderá acarretar sanções administrativas disciplinares e/ou contratuais, sem prejuízo das responsabilizações nas esferas civil e criminal.

8. POLÍTICAS COMPLEMENTARES (PC)

A Política de Segurança da Informação (PSI) no âmbito da SEE-PE está estruturada com as Políticas Complementares indicadas a seguir, que tratam da gestão dos recursos tecnológicos e devem ser atendidas conforme sua especificidade:

8.1. PC01 – Política de Uso de Senhas

Estabelecer critérios para a criação de senhas fortes, proteção dessas senhas, bem como a frequência de suas atualizações.

8.2. PC02 – Política de Uso do Correio Eletrônico

Estabelecer critérios que determinem as exigências mínimas de segurança para uma comunicação através do correio eletrônico institucional.

8.3. PC03 – Política de Resposta a Incidentes de Segurança da Informação

Estabelecer medidas a serem tomadas nos tratamentos de incidentes, envolvendo a segurança das informações. Os Incidentes de Segurança da Informação em eventos podem resultar em perda, dano ou acesso não autorizado às informações.

8.4. PC04 – Política de Classificação da Informação

Estabelecer padrões na determinação de quais informações podem ser divulgadas fora da SEE-PE, bem como ser sensível em relação às informações que não devem ser divulgadas sem a devida autorização.

8.5. PC05 – Política de Aquisição, Desenvolvimento e Manutenção de Sistemas de Informações

Estabelecer as exigências mínimas que devem ser atendidas no desenvolvimento, aquisição e suporte das aplicações sistêmicas.

8.6. PC06 – Política de Uso da Internet

Estabelecer as exigências mínimas de segurança da informação para o uso seguro da Internet.

8.7. PC07 – Política de Acesso Remoto

Estabelecer regras e requisitos para acesso externo à rede da SEE-PE e minimizar o risco potencial para danos que possam resultar do uso não autorizado.

8.8. PC08 – Política de Gestão de Ativos

Estabelecer a formalização da gestão de ativos da SEE-PE.

8.9. PC09 – Política de Controle de Acesso

Estabelecer as exigências mínimas na criação de identidades em conformidade com as atividades funcionais e no controle de acesso dos usuários.

8.10. PC10 – Política de Dispositivos Móveis

Estabelecer regras e padrões na utilização e armazenamento dos dispositivos móveis utilizados nas atividades de trabalho da SEE-PE.

8.11. PC11 – Política de Backup Corporativo

Estabelecer padrões para a cópia e restauração, com a finalidade de continuidade e disponibilidade das informações, observando a relevância e criticidade destas.

8.12. PC12 – Política de Combate a Softwares Maliciosos

Estabelecer as exigências mínimas de segurança para a proteção contra softwares maliciosos (vírus, trojan, entre outros).

9. ADEQUAÇÃO À POLÍTICA

a. Os novos projetos de desenvolvimento ou novas aquisições de sistemas devem seguir os padrões estabelecidos nesta política;

b. As implementações para o ambiente tecnológico existente deverão ser adequadas a esta política no prazo máximo de 3(três) anos, a partir de sua publicação. O escalonamento de implementação, deve seguir a seguinte ordem: 01- PC07 – Política de Acesso Remoto; 02- PC11 – Política de Backup Corporativo; 03- PC01 – Política de Uso de Senhas; 04- PC09 – Política de Controle de Acesso; 05- PC02 – Política de Uso do Correio Eletrônico; 06- PC06 – Política de Uso da Internet; 07- PC08 – Política de Gestão de Ativos; 08- PC10 – Política de Dispositivos Móveis; 09- PC04 – Política de Classificação da Informação; 10- PC03 – Política de Resposta a Incidentes de Segurança da Informação; 11- PC12 – Política de Combate a Softwares Maliciosos e 12- PC05 – Política de Aquisição, Desenvolvimento e Manutenção de Sistemas de Informações.

c. Caso não seja possível a adequação das ferramentas, o Comitê de TI da SEE-PE ou seus representantes devem documentar essa informação, bem como seus motivos, para fins de auditoria interna.

10. REFERÊNCIAS LEGAIS E NORMATIVAS

Os documentos de referência desta política são normas e legislações referentes às estratégias públicas adotadas pela SEE-PE, quais sejam:

DOCUMENTOS DE REFERÊNCIA	
Referência Legal	**Teor**
ISO 27040:2013	Código de prática de armazenamento. Fornece orientações sobre como as organizações devem armazenar suas informações, tais como: documentos, planilhas e até mesmo a base de sistemas. Também conscientiza sobre políticas de recuperação de backup e a maneira de descarte de mídias que já foram utilizadas como backup.
NBR ISO 55000: 2014	Norma que fornece uma visão geral de gestão de ativos, seus princípios e terminologia, bem como os benefícios esperados.
NBR ISO 55001:2014	Norma que especifica requisitos para um sistema de gestão de ativos dentro do contexto da organização.
NBR ISO 55002:2014	Norma que fornece diretrizes para a aplicação de um sistema de gestão de ativos, de acordo com os requisitos da ABNT NBR ISO 55001.
NBR ISO/IEC 27001:2013	Norma que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Esta Norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização.
NBR ISO/IEC 27002:2013	Norma que fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.
NBR ISO/IEC 27005:2011	Norma que fornece diretrizes para o processo de gestão de riscos de segurança da informação.
ISO/IEC 15504	Tecnologia da Informação – Estabelece uma estrutura padrão para os processos de vida no desenvolvimento de software.
PASS 55	Especificação da Instituição Britânica de Padrões (*British Standards Institution*) para o gerenciamento de ativos físicos e infraestrutura.
CMMI (Capability Maturity Model – Integration ou Modelo de Maturidade em Capacitação – Integração)	Modelo de referência para desenvolvimento e manutenção de software.
***Control Objectives For Information end Related Technology* - COBIT 5**	Conjunto de boas práticas que visa dar suporte a Governança e Gerenciamento dos processos de tecnologia da informação

***Information Technology Infrastructure Library* – ITIL V3**	Conjunto de boas práticas para utilização na infraestrutura, operação e gerenciamento de serviços de tecnologia da informação.
MPS.BR (Melhoria de Processos do Software Brasileiro	Movimento para melhoria da qualidade de processo do Software Brasileiro.
Lei nº 14.804, de 29 de outubro de 2012	Regula o acesso a informações, no âmbito do Poder Executivo Estadual.
Decreto Estadual nº 38.787/2012 (Política de Acesso à Informação)	Regulamenta a Lei no 14.804/2012.
Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)	Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
Decreto nº 8.771, de 11 de maio de 2016	Regulamenta a Lei nº 12.965, de 23 de abril de 2014.
Lei nº 12.527, de 18 de novembro de 2011	Lei de acesso a informações.
Lei nº 9.609, de 19 de fevereiro de 1998	Lei dos Direitos Autorais.
Lei n° 9.610, de 19 de fevereiro de 1998	Lei que altera, atualiza e consolida a legislação sobre direitos autorais.
Lei nº 11.781, de 6 de junho de 2000	Legislação que regula o processo administrativo no âmbito da Administração Pública Estadual.
Lei nº 6.123, de 20 de julho de 1968.	Estatuto dos Funcionários Públicos do Estado de Pernambuco.
Lei complementar nº 131, de 27 de maio de 2009	Lei da Transparência.

11. BIBLIOGRAFIA COMPLEMENTAR

AGU – Política de Segurança da Informação e das Comunicações – Diretrizes e Normas, http://www.agu.gov.br/page/content/detail/id_conteudo/228893, 2013.

Cartilha de Segurança para Internet, desenvolvida pelo CERT.br, mantido pelo NIC.br, com inteiro teor em http://cartilha.cert.br/, 07/10/2016.

Diógenes, Yuri; Mauser, Danel - Certificação Security + da Prática Para o Exame SYO-301, Editora Nova Terra, 2011.

Ferreira, Fernando Nicolau Freitas; Araújo, Márcio Tadeu de – Política de Segurança da Informação – Guia Prático para Elaboração e Implantação 2ª Edição Revisada, Editora Ciência Moderna, Rio de Janeiro, 2008.

Fontes, Edison – Políticas e Normas para a Segurança da Informação, Editora Brasport, Rio de Janeiro, 2012.

Fontes, Edison – Praticando a Segurança da Informação, Editora Brasport, Rio de Janeiro, 2008.