CSAI	Comitê Setorial de Acesso à Informação
CSEP	Comissão Setorial de Ética Pública
CI	Comitê de Integridade
IAM	Gerenciamento de identidade e acesso
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados
MFA	Mecanismos de autenticação multifator
NUTIC	Núcleo Tecnologia da Informação e Comunicação
OSC	Organização da Sociedade Civil
PoSIC	Política de Segurança da Informação e Comunicação
SEAS	Superintendência do Sistema Estadual de Atendimento Socioeducativo
SIC	Serviço de Informação ao Cidadão
SIC	Serviço de Informação ao Cidadão
TI	Tecnologia da Informação

1. DISPOSIÇÕES GERAIS

1.1 A Política de Segurança da Informação e Comunicação (PoSIC) estabelece princípios, diretrizes, normas e procedimentos gerais para a gestão da segurança da informação dos ambientes de Tecnologia da Informação e Comunicação da Superintendência do Sistema Estadual de Atendimento Socioeducativo - Seas, gerenciados pelo Núcleo Tecnologia da Informação e Comunicação - Nutic, com vista à preservação da integridade, da confidencialidade e da disponibilidade das informações do órgão e à proteção contra diversos tipos de ameaças que, se efetivadas, possam gerar prejuízos à organização.

1.2. A PoSIC deve ser seguida por todas as áreas e aplicada às instalações, equipamentos, materiais, documentos, pessoas e sistemas de informações da Seas, assim como às atividades dos servidores, colaboradores, consultores, estagiários e prestadores de serviços que exercem atividades no âmbito da sede da Superintendência ou dos Centros Socioeducativos, quanto aos serviços de rede de dados, internet, telecomunicações, estações de trabalho, correio eletrônico e demais recursos de informação e comunicação.

2. OBJETIVOS

2.1. São objetivos desta PoSIC:

I. Apresentar, de forma clara, a visão desta instituição e de sua administração superior relacionada à segurança da informação e comunicação;

II. Definir diretrizes que orientarão a criação de normas e procedimentos relacionados à segurança da informação e comunicação no âmbito desta instituição;

III. Prover meios para atingir a excelência na qualidade dos serviços prestados pela instituição quanto à confidencialidade, integridade, disponibilidade, autenticidade e não-repúdio das informações;

IV. Fomentar uma cultura de conscientização em segurança da informação e cibernética, garantindo que todos os usuários compreendam e sigam as políticas e procedimentos estabelecidos.

3. PRINCÍPIOS

3.1. São princípios desta PoSIC:

I. Autenticidade: diz respeito ao conjunto de meios que permite assegurar que os dados enviados e recebidos provêm das entidades declaradas;

II. Confidencialidade: se baseia em conceitos que permitam assegurar que a informação não pode ser acessada por pessoas não autorizadas;

III. Disponibilidade: é o princípio que garante que a informação estará sempre disponível para uso legítimo do destinatário;

IV. Integridade: diz respeito às técnicas que possibilitam verificar se os dados foram alterados ou suprimidos indevidamente;

V. Não-Repúdio: são formas de impedir que uma entidade (emissor ou receptor) negue a participação em uma troca de informação;

VI. Legalidade: diz respeito à obediência aos princípios constitucionais, administrativos e legais aplicáveis.

4. COMPETÊNCIAS E RESPONSABILIDADES

4.1. São competências comuns a todos os usuários:

I. Estar ciente, manter-se atualizado e seguir as diretrizes desta PoSIC, suas normas complementares e procedimentos relacionados, buscando informações junto ao Nutic sempre que não estiver absolutamente seguro quanto à obtenção, tratamento, uso e/ou descarte de informações;

II. Comunicar ao Nutic, via sistema de chamados, e-mail ou canal de whatsapp, qualquer incidente de segurança de que venha a tomar conhecimento, seja suspeito ou confirmado;

III. Cumprir e difundir as regulamentações descritas nesta política;

IV. Reportar descumprimentos desta política ao Nutic;

V. Contribuir para a melhoria dos níveis de segurança da informação e comunicação;

VI. Responder por toda atividade executada por meio de sua identificação;

VII. Zelar pela segurança de seu usuário corporativo, departamental ou de rede local, bem como de seus respectivos dados e credenciais de acesso;

VIII. Seguir, de forma colaborativa, às orientações fornecidas pelos setores competentes em relação ao uso dos recursos corporativos de informação e comunicação, utilizando-os sempre de forma ética, legal e consciente;

4.2. São competências do Nutic:

I. Desenvolver ações para capacitar e conscientizar os membros da instituição sobre segurança da informação;

II. Desenvolver ações relacionadas à gestão de risco, conforme previsto nesta política;

III. Desenvolver ações relacionadas à auditoria e conformidade, conforme previsto nesta política;

IV. Monitorar as ações que envolvam informações e comunicação, sempre que possível, de forma a identificar a ocorrência de incidentes de segurança;

V. Definir processos para tratar e responder aos incidentes de segurança identificados e reportados;

VI. Desenvolver ações relacionadas à gestão de continuidade, conforme previsto nesta política;

VII. Propor normas e procedimentos seguindo as diretrizes desta política;

VIII. Auditar o cumprimento desta política, bem como das normas e procedimentos ligados a esta;

IX. Homologar e autorizar o uso e acesso de ativos, sistemas e dispositivos de processamento de informações em suas instalações;

X. Realizar a gestão do acesso do usuário a recurso computacional da Seas, ao colaborador que for desligado da instituição ou a qualquer tempo, quando evidenciados riscos à segurança da informação, e informar o incidente ao gestor máximo da instituição;

XI. Propor, analisar e aprovar normas, procedimentos e soluções específicas que atendam às necessidades de segurança da informação e comunicação;

XII. Apoiar a implementação das ações de segurança da informação e comunicação;

XIII. Analisar os casos relacionados à segurança da informação e comunicação omissos nesta política.

4.3. São competência da autoridade máxima da Seas:

I. Aprovar a Política de Segurança da Informação e Comunicação e seus normativos;

II. Garantir os recursos necessários para implementação destas diretrizes;

III. Promover, incentivar e disseminar permanentemente esta PoSIC;

5. CONCEITOS E DEFINIÇÕES

5.1. Para os fins desta política, considera-se:

I. Acesso: ato de entrar, visualizar ou usar informações e recursos da instituição;

II. Artefato Malicioso: programa ou código criado para danificar, roubar informações ou interromper sistemas;

III. Ativo: qualquer recurso, físico ou digital, que possui valor para a instituição;

IV. Ativo de Informação: recurso que armazena e processa informações valiosas;

V. Backup: cópia de segurança de dados usada para recuperação em caso de perda ou dano;

VI. Capacitação em Segurança da Informação: treinamentos para ensinar aos colaboradores sobre práticas seguras no manejo de informações;

VII. Classificação da Informação: processo para definição do nível de proteção necessário para cada tipo de informação;

VIII. Conformidade: aderência às leis, normas e políticas de segurança da informação;

IX. Conscientização em Segurança da Informação: campanhas e ações para educar os colaboradores sobre a importância da segurança da informação;

X. Conteúdo Ilegal: qualquer dado ou material que viole leis ou regulamentos vigentes;

XI. Centro de Tratamento de Incidentes: unidade responsável por gerenciar e responder a incidentes de segurança;

XII. Dados Sensíveis: informações pessoais ou institucionais que, se divulgadas, possam causar danos ou discriminação;

XIII. Diretrizes: instruções que orientam a criação de normas e procedimentos de segurança;

XIV. E-mail Institucional: serviço de correio eletrônico fornecido pela instituição para comunicação oficial;

XV. Evento: qualquer ocorrência relevante em um sistema ou rede de computadores;

XVI. Evento Adverso: ocorrência negativa que impacta a segurança da informação, como falhas de sistemas ou acessos não autorizados;