XVII. Gestor de Ativo: pessoa responsável pela administração e segurança de um recurso específico;
XVIII. Hardening: processos para aumentar a segurança de sistemas e reduzir vulnerabilidades;
XIX. Incidente de Segurança: evento que compromete a segurança das informações ou sistemas;
XX. Log de Dados: registro de atividades e eventos em sistemas computacionais;
XXI. Norma: conjunto de regras que devem ser seguidas para garantir a segurança da informação;
XXII. Membros da Instituição: todos os servidores, funcionários, alunos da Escola de Socioeducação, estagiários e demais colaboradores que utilizam os recursos da instituição;
XXIII. Política de Segurança da Informação: conjunto de princípios e diretrizes que orientam a proteção das informações da instituição;
XXIV. Ponto de Acesso: dispositivo que permite conexão a uma rede de computadores;
XXV. Procedimento: conjunto de ações padronizadas para executar tarefas específicas;
XXVI. Protocolo Criptográfico: métodos para criptografar e proteger dados durante a transmissão;
XXVII. Público-alvo: grupos ou indivíduos atendidos ou afetados pela PoSIC;
XXVIII. Responsável pela Segurança da Informação: pessoa designada para gerenciar e monitorar a segurança da informação na instituição;
XXIX. Serviços de Segurança da Informação: conjunto de procedimentos e ferramentas oferecidos para proteger as informações da instituição;
XXX. Serviço de Anonimato: ferramenta para ocultar a identidade dos usuários na rede;
XXXI. Sensibilização em Segurança da Informação: atividades para alertar sobre práticas seguras no uso de informações;
XXXII. Spam: mensagens eletrônicas não solicitadas enviadas em massa;
XXXIII. Spammer: pessoa ou entidade que envia mensagens de spam;
XXXIV. Tratamento de Incidentes: processo de identificação, análise e resposta a incidentes de segurança;
XXXV. Usuário Autenticado: usuário cuja identidade foi verificada e tem permissão para acessar determinados recursos;
XXXVI. Vulnerabilidade: fraqueza em sistemas ou redes que pode ser explorada para causar danos ou acessos não autorizados.

6. CLASSIFICAÇÃO DE INFORMAÇÃO

6.1 Para fins de adoção das diretrizes previstas nesta Portaria, a informação classifica-se em:
I. De Interesse Público: toda aquela informação não classificada como de caráter pessoal ou como sigilosa, nos termos das legislações estadual e federal;
II. Sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, podendo ser classificada em Reservada, Secreta e Ultrassecreta:
a) Informação Reservada: as que ficam sob sigilo durante o prazo de 5 (cinco) anos;
b) Informação Secreta: as que ficam sob sigilo durante o prazo de 15 (quinze) anos;
c) Informação Ultrassecreta: as que ficam sob sigilo durante o prazo de 25 (vinte e cinco) anos;
III. Pessoal: aquela relacionada à pessoa natural identificada ou identificável;
IV. Sensível: são dados confidenciais que devem ser mantidos seguros e fora do alcance de usuários externos, protegidos pela Lei Geral de Proteção de Dados - LGPD e pelo Estatuto da Criança e do Adolescente -ECA.
6.2 Não é permitida a cessão, fornecimento ou divulgação de informações da Seas que estejam definidas como sigilosas, pessoais ou sensíveis.
6.3 Todos os pedidos de acesso à informação devem ser encaminhados ao Comitê Setorial de Acesso à Informação da Seas - CSAI, a quem cabe deliberar sobre o assunto, conforme determina a legislação federal e estadual, devendo-se observar o fluxo contido no anexo B (NP-5), desta portaria.
6.4 Os pedidos de informações deverão ser analisados pelo CSAI levando em consideração as classificações da Portaria CGAI n° 01/2016, que dispõe sobre a uniformização na classificação de informação sigilosa de matéria comum a todos os órgãos e entidades do Poder Executivo Estadual.

7. CONTROLE DE ACESSO

7.1 O controle de acesso é o conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais e, via de regra, requer procedimentos de autenticação.
7.2 O Nutic deve ter o controle de todos os usuários e terminais utilizados na Seas e a ele caberá:
I. Implementação de políticas de autenticação, autorização e monitoramento de acesso aos sistemas e informações;
II. Uso de sistemas de gerenciamento de identidade e acesso (IAM) para garantir a aplicação das políticas de acesso;
III. Implementação de mecanismos de autenticação multifator (MFA) para acessos críticos e de alto risco;
IV. Suspender os e-mails institucionais de colaboradores afastados em virtude de impedimentos, licenças e férias, após a comunicação pela Célula de Gestão de Pessoas (Cegep) dos respectivos afastamentos;
V. Providenciar o cadastro de notificação automática durante os períodos de ausência dos colaboradores, com a configuração de respostas automáticas informando sobre a ausência e fornecendo contatos alternativos;
VI. Revisar periodicamente as permissões de acesso dos usuários e remoção de privilégios desnecessários.
§ 1º. Fica estabelecido um procedimento para conceder acessos temporários em casos de emergência, por meio de solicitação e validação de um superior responsável pelo setor que pretende realizar o acesso.
§ 2º. São vedadas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede, conta ou sistema, ficando o agente sujeito às penalidades administrativas, civis e penais cabíveis.
7.3 Quanto à segurança em redes e sistemas/aplicações, caberá ao Nutic:
I. Configurar e manter firewalls para proteger a rede interna de ameaças externas;
II. Implementar soluções de detecção e prevenção de intrusões (IDS/IPS) para identificar atividades suspeitas e bloquear ataques;
III. Aplicar patches e atualizações de segurança em sistemas operacionais e aplicativos, seguindo um cronograma de manutenção preestabelecido;
IV. Observar e cumprir de forma integral as políticas, procedimentos e gestão de TIC;
7.4 Quanto à segurança física, caberá ao Nutic:
I. Implementar medidas de segurança para proteger o acesso às áreas críticas e aos dispositivos físicos que armazenam e processam informações, como câmeras de segurança, controle de acesso e alarmes;
II. Estabelecer diretrizes para a destruição segura de mídias físicas e dispositivos de armazenamento de informações.
7.5 Quanto ao acesso a internet:
I. O acesso à internet em ambiente corporativo da Seas e de suas unidades será feito exclusivamente pelos meios autorizados e configurados pelo Nutic, sendo expressamente proibido o uso de proxies externos ou similares;
II. O acesso à internet será disponibilizado pelo Nutic para uso nas atividades relacionadas ao trabalho, sendo o uso para fins pessoais limitado aos princípios da ética, razoabilidade e legalidade;
III. No caso de visitantes, o cadastro de usuário provisório proverá acesso limitado e em separado dos serviços disponibilizados pelo Nutic dentro da rede de dados da Seas;
IV. Para servidores públicos, colaboradores terceirizados e das OSC´s parceiras, os procedimentos para acesso à internet estão contidos no anexo B (NP-1);
V. Por motivos de segurança, todo acesso à internet será monitorado e os registros serão mantidos pelo Nutic;
VI. Em caso de indícios de descumprimento das diretrizes previstas neste procedimento, a chefia imediata ou superior solicitará, justificadamente, ao Nutic a realização de auditoria extraordinária;
VII. Todos os dados relativos à Seas e aos Centros de Socioeducação devem ser mantidos no servidor por meios físicos ou por plataforma em nuvem, onde deve existir sistema de backup periódico.

8. DO TRATAMENTO DE AMEAÇAS E INCIDENTES

8.1 A política de tratamento de incidentes estabelece um conjunto de normas e procedimentos para tratar os incidentes de segurança, de forma a minimizar impactos e restabelecer a normalidade.
8.2 O Nutic deverá prover a atualização de vacinas da ferramenta de antivírus nas estações, notebooks e servidores de rede, bem como os procedimentos a serem seguidos em caso de contaminação por malware.
8.3 O Nutic será responsável por coordenar as ações de resposta a incidentes de segurança da informação mediante as seguintes regras:
I. O incidente deverá ser classificado com base em seu impacto potencial sobre as operações:
a) Baixa: impacto mínimo, sem interrupções significativas.
b) Média: pode causar interrupções em um departamento ou setor específico.
c) Alta: impacto significativo, com potencial de interromper operações críticas.
II. Desenvolver e manter um plano de resposta a incidentes de segurança que contemple a identificação, contenção, erradicação, recuperação e comunicação dos incidentes;
III. Estabelecer um processo de notificação e reporte de incidentes de segurança que envolva todas as partes interessadas e promova a ação rápida e efetiva na resolução de problemas;
IV. Realizar análises pós-incidente para identificar as causas e implementar medidas preventivas;