Cartilha

Política de Segurança

da Informação e Comunicação

SUPERINTENDÊNCIA DO **SISTEMA ESTADUAL DEATENDIMENTO SOCIOEDUCATIVO**

CEARÁ
GOVERNO DO ESTADO
SECRETARIA DA **PROTEÇÃO SOCIAL**

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

A 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 Socioeducatico (SEAS), preservando a integridade, confidencialidade e disponibilidade das informações do órgão.

Quem está submetido à POSIC?

- Direção superior;
- Gestão superior;
- Servidores;
- Terceirizados.

SE LIGA!

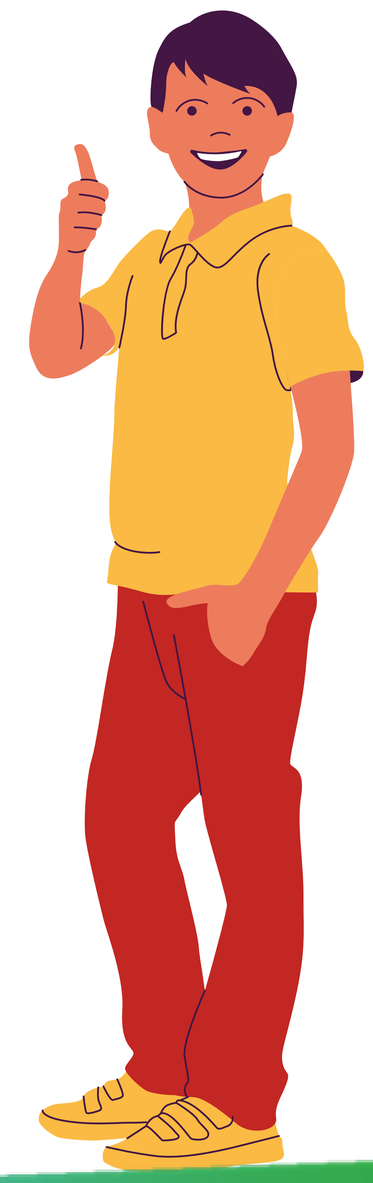
DICAS IMPORTANTES

- Não são permitidas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede, conta ou sistema;

- O colaborador deve sempre bloquear o equipamento ao se ausentar (Ctrl + Al t + Del ou botão Windows + L);

- Materiais com conteúdo impróprio (racistas, eróticos ou preconceituoso) não poderão ser acessados, expostos, armazenados ou distribuídos através de qualquer tipo de ferramenta ou dispositivos utilizados na rede;

- Todos os dados relativos à Seas e suas unidades de negócio devem ser mantidos no servidor, na rede, onde existe sistema de backup periódico;



DEVERES

AGENTES PÚBLICOS

- Cumprir as determinações constantes na POSIC, independentemente do nível hierárquico ou função, bem como do vínculo empregatício;
- Responsabilizar-se pelo ativo de TIC (equipamentos, notebooks, computadores, programas específicos e licenças de software) e por sua adequada utilização;
- Responder por toda violação de segurança praticada por si;
- Comunicar qualquer indício de fragilidade relacionada a Segurança da Informação nos processos de suas áreas;
- Proteger sua senha de acesso contra uso indevido, responsabilizando-se por todas as atividades originadas a partir de sua identificação;

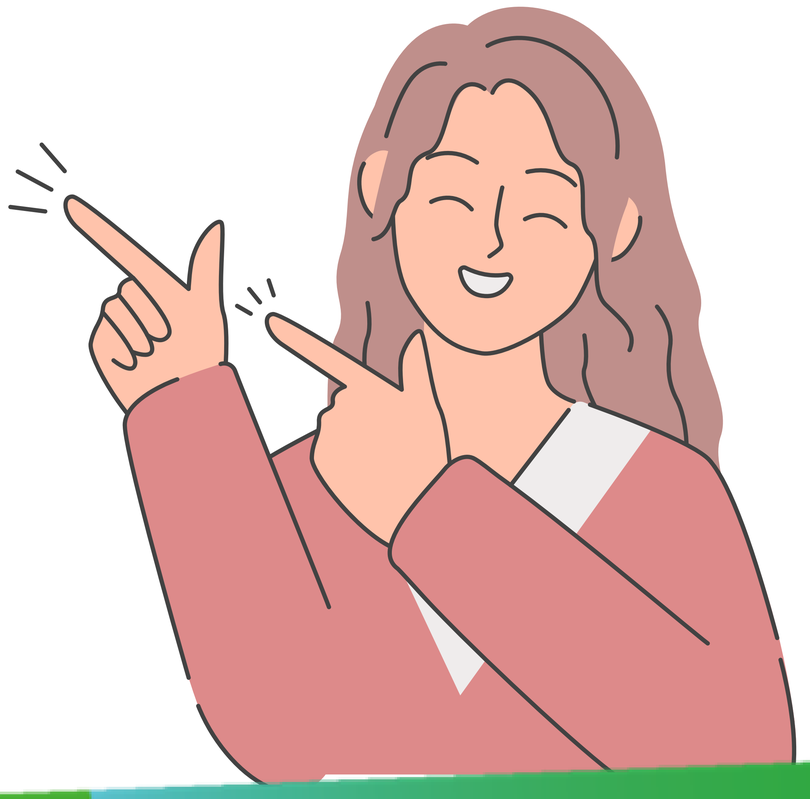
DEVERES

AGENTES PÚBLICOS

Utilizar somente programas legalizados ou analisados tecnicamente pelo NUTIC, sendo expressamente proibido o uso/instalação de software não licenciado

Usar os serviços de forma otimizada e compartilhada, evitando desperdícios tais como utilização inadequada do tempo de rede, Internet, de impressão e espaço em disco;

Repor ativos (equipamentos, notebooks ou computadores) em caso de roubo, furto ou danos, quando caracterizado que o evento decorreu de conduta dolosa ou de culpa exclusiva do agente público, a ser apurada por meio de sindicância.



VEDAÇÕES

AGENTES PÚBLICOS

- Realizar qualquer procedimento que envolva supor te técnico, tais como manutenção de equipamentos, instalação de software, alteração nas configurações do sistema e outras similares, sem a devida autorização do NUTIC;

- Utilizar os serviços e recursos da SEAS para fins comerciais, políticos e particulares, tais como mala direta, propaganda polí tica e venda de objetos pessoais e/ou comerciais;

- Participar, no horário do expediente, de listas de discussão, newsgroups, sessões de chat e redes sociais que não estejam em conformidade com as atividades institucionais da SEAS;

- Acessar, via Internet , sites que comprometam a segurança e infrinjam a legislação e/ou que comprometam as normas estabelecidas da SEAS, a exemplo de sites pornográficos e de conteúdo discriminatório;

VEDAÇÕES

AGENTES PÚBLICOS

- Divulgar sua senha de acesso à rede para qualquer pessoa, pois a informação é de caráter pessoal e intransferível;
- Utilizar arquivos e dados de outro agente público, sem a devida autorização;
- Utilizar identidade falsa para uso do correio eletrônico ou outros usos da rede;

- Utilizar identidade falsa para uso do correio eletrônico ou outros usos da rede;

POSIC

AGENTES PÚBLICOS

ACESSO À INTERNET

Os colaboradores somente deverão acessar sites que tenham relação com as atividades desenvolvidas pela SEAS;

Nos casos em que determinado colaborador necessite acessar algum conteúdo que esteja bloqueado pelos mecanismos de segurança, deverá ser aberto um chamado pelo coordenador da área solicitando a liberação do acesso, onde o NUTIC fará a liberação desde que o conteúdo solicitado não proporcione riscos para à segurança das informações do órgão;

Somente os colaboradores internos poderão acessar o wi-fi corporat ivo da SEAS;

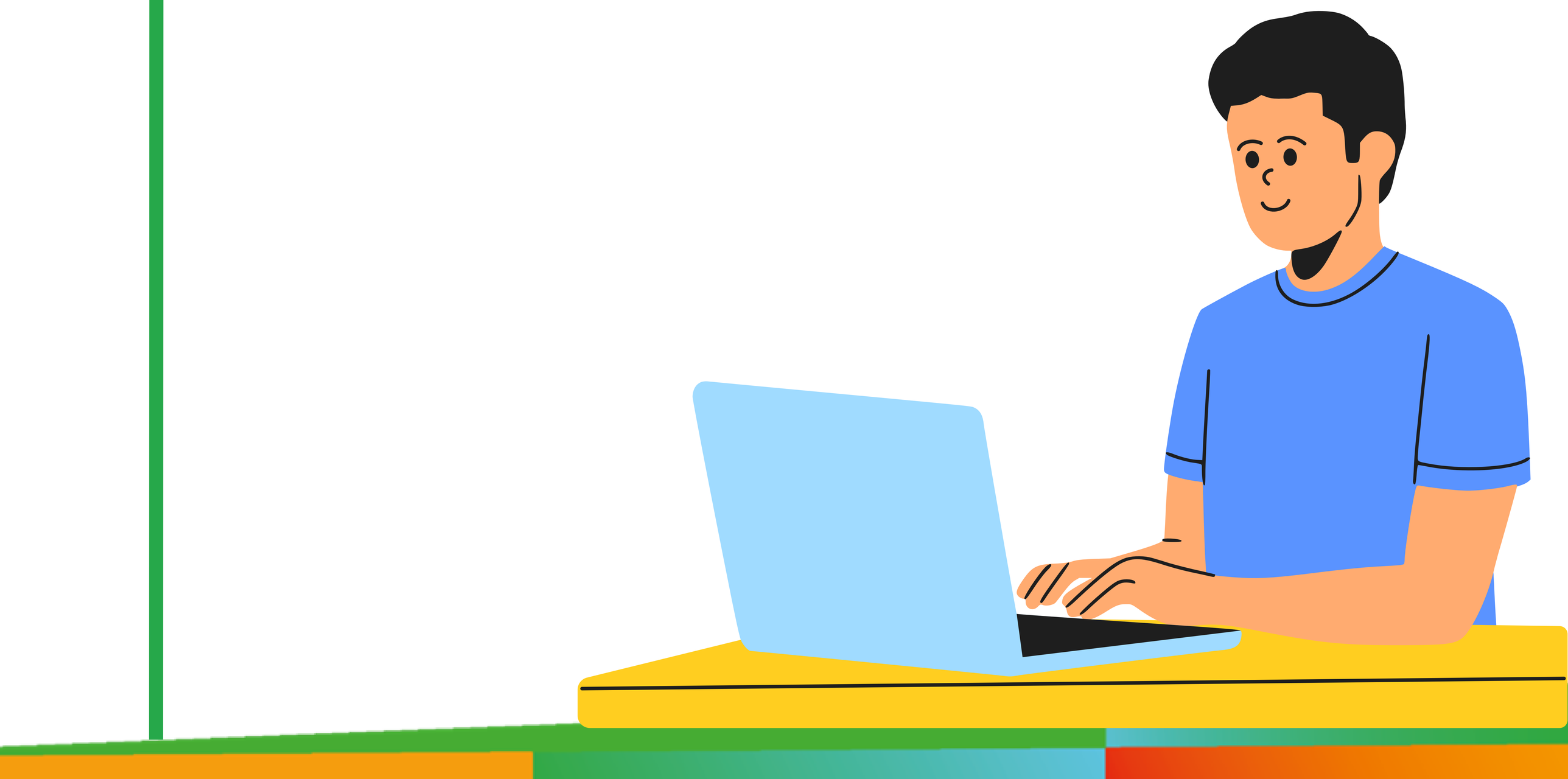
Os visitantes poderão ter acesso a internet por meio do wi-fi exclusivo para esse público, que deverá ser liberado de forma temporária;

ACESSO À INTERNET

A SEAS monitora e bloqueia automaticamente sites de conteúdo erótico, pedofilia, racismo, drogas e outros que contenham conteúdos contrários às legislações vigentes;

Qualquer necessidade de download de programas/softwares deve ser repassada ao NUTIC, sendo registrado o pedido via sistema de abertura de chamados;

O uso da internet é auditado e moni torado constantemente, e o colaborador poderá vir a prestar contas de seu uso.



CORREIO ELETRÔNICO

O NUTIC será responsável pelo gerenciamento, adição, exclusão e adoção de medidas operacionais visando conter a propagação de emails suspeitos no ambiente de tecnologia da SEAS;

A qualquer tempo, mediante detecção pelos sistemas e/ou identificação de e-mails suspeitos pela equipe responsável pela administração do sistema de correio eletrônico, O NUTIC procederá com as configurações necessárias objetivando conter eventuais propagações de e-mails suspeitos na SEAS;

O colaborador deverá efetuar abertura de chamados técnicos no sistema SEAS Atende, quando houver necessidade de análise de emails suspeitos de SPAM pelo NUTIC;

O colaborador é responsável direto pelas mensagens enviadas por intermédio do seu endereço de correio eletrônico;

SUPERINTENDÊNCIA DO **SISTEMA**
ESTADUAL DEATENDIMENTO
SOCIOEDUCATIVO

CEARÁ
GOVERNO DO ESTADO
SECRETARIA DA **PROTEÇÃO SOCIAL**