PORTARIA Nº 493/2024 - SEAS

Dispõe sobre a criação da Política de Segurança da Informação e Comunicações - PoSIC da Superintendência do Sistema Estadual de Atendimento Socioeducativo - Seas e dá outras providências.

O Superintendente do Sistema Estadual de Atendimento Socioeducativo do Ceará - Seas, no uso de suas atribuições e tendo em vista o Decreto Estadual nº 34.100, de 08 de junho de 2021, que dispõe sobre a Política de Segurança da Informação e Comunicação dos Ambientes de Tecnologia da Informação e Comunicação – TIC do Governo do Estado do Ceará e sobre o Comitê Gestor de Segurança da Informação do Governo do Estado do Ceará – CGSI, **RESOLVE:**

Art. 1º Instituir a Política de Segurança da Informação e Comunicações - PoSIC, no âmbito da Superintendência do Sistema Estadual de Atendimento Socioeducativo do Estado do Ceará - Seas, com o objetivo de estabelecer diretrizes, normas e procedimentos gerais para a gestão da segurança da informação, nos termos desta Portaria e seus Anexos.

Parágrafo único. As diretrizes, normas e procedimentos gerais contidas na PoSIC são aplicadas a todos os colaboradores e usuários que tenham acesso aos recursos de tecnologia da Seas, se estendendo para todos aqueles que trabalham nos Centros Socioeducativos e para as entidades executoras da gestão compartilhada através de parcerias, convênios ou congêneres.

Art. 2º A divulgação da PoSIC será feita por meio de disponibilização integral e contínua na internet, seminários de conscientização e quaisquer outros meios adequados e pertinentes.

Art. 3º Esta Portaria entra em vigor na data de sua publicação.

Fortaleza-CE, data da assinatura digital.

Roberto Bassan Peixoto
Superintendente do Sistema Estadual de Atendimento Socioeducativo

ANEXO A

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO - POSIC DA SUPERINTENDÊNCIA DO SISTEMA ESTADUAL DE ATENDIMENTO SOCIOEDUCATIVO - SEAS

Novembro/2024

SUPERINTENDÊNCIA DO SISTEMA ESTADUAL DE ATENDIMENTO SOCIOEDUCATIVO - SEAS

Superintendente
Roberto Bassan Peixoto
Superintendente Adjunto
Jean Marçal Lima Cunha
Assessora Especial de Gestão e Comunicação
Larissa de Almeida Morais Camerino
Coordenadora Administrativo Financeira
Wilma Jales de Brito
Coordenadora da Assessoria Jurídica
Analuisa Macedo Trindade
Corregedor
Carlos Eduardo Nunes Sena
Ouvidor
Domingos Alves Evangelista Neto
Assessora Especial de Diretrizes Socioeducativas
Ana Paula Iris Medeiros
Coordenador de Desenvolvimento Institucional e Planejamento
Alberto Sergio Holanda Banhos
Assessora Especial de Infraestrutura e Logística
Bianca Aderaldo Lobo Moreira
Coordenador da Rede Socioeducativa
Adilson José dos Santos
Coordenadora de Monitoramento e Avaliação
Ana Maria Tavares Cruz
Núcleo Escola Estadual de Socioeducação
Jéssica Muriel de Sousa

FICHA TÉCNICA

Elaboração 08/08/2024	**Revisão** 14/11/2024
Alberto Sergio Holanda Banhos Analuisa Macedo Trindade Bianca Aderaldo Lobo Moreira Carlos Eduardo Nunes Sena Domingos Alves Evangelista Neto Jean Marçal Lima Cunha Larissa de Almeida Morais Camerino Letícia Simões Rivelini Roberto Jackson Silva Filho Wilma Jales de Brito	Alberto Sergio Holanda Banhos Analuisa Macedo Trindade
Aprovação	
Roberto Bassan Peixoto	

SIGLAS E ABREVIATURAS

AILOG	Assessoria Especial de Infraestrutura e Logística
CEGEP	Célula de Gestão de Pessoas
CGAI	Comitê Gestor de Acesso à Informação
CGSI	Comitê Gestor de Segurança da Informação
CPD	Centro (Central) de Processamento de Dados
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;
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;
8.4 Todos os colaboradores devem reportar imediatamente qualquer suspeita de incidente de segurança ao Nutic por meio das ferramentas de comunicação, utilizando o sistema de chamados, e-mail ou canal de whatsapp.
8.5 Os usuários devem entender os riscos associados à sua condição e cumprir rigorosamente as políticas, normas e procedimentos vigentes de segurança da informação e comunicações.
8.6 Cada gestor deverá manter os processos sob sua responsabilidade aderentes às políticas, normas e procedimentos específicos de segurança da informação e comunicação da Seas, adotando as ações necessárias para cumprir tal responsabilidade.

9. USO ADEQUADO DOS RECURSOS DE TI

9.1 Os recursos de TI devem ser utilizados exclusivamente para fins relacionados ao trabalho, de acordo com as responsabilidades e funções dos usuários na organização.
9.2 O uso pessoal dos recursos de TI deve ser limitado, não interferindo nas atividades profissionais e não deve comprometer a segurança ou o desempenho dos sistemas.
9.3 O usuário deve sempre bloquear o equipamento ao se ausentar de sua mesa/ilha/local de trabalho através do comando Ctrl + Alt + Del ou botão Windows + L.
9.4 Os ativos de TI físicos, sejam servidores, roteadores, desktops, laptops, dispositivos de rede, equipamentos de sistema de CFTV e periféricos, deverão ser instalados em locais adequados, conforme normas e procedimentos contidos no anexo B (NP-2).
9.5 As regras e os procedimentos para prevenir o acesso físico não autorizado a interferências nas instalações e informações, além de proteger e restringir acesso a informações ou sistemas que armazenem dados sigilosos da instituição considerando perímetros de segurança estão contidos no anexo B (NP-2).

10. PENALIDADES

10.1 Todo prejuízo ou dano decorrente da não obediência às diretrizes e normas referenciadas nesta PoSIC e nas normas e procedimentos específicos dela decorrentes é de inteira responsabilidade do usuário que o der causa.
10.2 A Seas poderá, a qualquer tempo, revogar credenciais de acesso concedidas a usuários em virtude do descumprimento desta PoSIC ou das normas complementares e procedimentos específicos dela decorrentes.
10.3 O desconhecimento das regras desta PoSIC não exime o usuário de suas responsabilidades por atos praticados em sua desconformidade.
10.4 As violações das diretrizes, normas ou procedimentos que, juntas, formam esta PoSIC resultarão em responsabilização administrativas, cíveis e penais, sendo devidamente aplicadas as sanções cabíveis, conforme previsão legal.
10.5 Fica assegurada a observância dos princípios do contraditório e da ampla defesa nas eventuais penalidades decorrentes da aplicação destas normas.

ANEXO B - NORMAS E PROCEDIMENTOS

NP 1 - NORMAS E PROCEDIMENTOS PARA O USO DA INTERNET	
I.	Para acessar o serviço de Internet, o usuário deverá ser autenticado.
II.	É bloqueado o acesso a sítios com conteúdos indevidos ou inadequados ao ambiente de trabalho da Seas.
III.	É vedada a instalação de software sem a devida autorização.
IV.	Os acessos realizados pelos usuários serão monitorados e os logs de acessos serão armazenados.
V.	É proibida a utilização de software P2P (tais como µTorrent, BitTorrent, Emule e similares).
VI.	É proibida a realização de download de software que infrinja os direitos autorais.
VII.	É proibida a utilização de serviços de anonimato para acesso à internet.
VIII.	As informações e os recursos de TI para acesso à rede desta instituição e seus recursos agregados devem ser disponibilizados, única e exclusivamente, àqueles que necessitem deles para o exercício de suas funções.
IX.	É proibido divulgar sua senha de acesso à rede para qualquer pessoa, por ser informação de caráter pessoal e intransferível.
X.	É proibido acessar ou utilizar arquivos e dados de outro usuário sem a devida autorização.

NP 2- NORMAS E PROCEDIMENTOS PARA USO ADEQUADO DOS RECURSOS DE TI	
I.	Condicionamento dos equipamentos de TI: o Nutic ficará responsável pelo procedimento que se aplica aos ativos de TI na infraestrutura da Seas, incluindo desktops, notebooks, roteadores, switchs, firewall e outros dispositivos de rede.
II.	Instalação de equipamentos: os equipamentos de TI devem ser instalados em locais devidamente inspecionados pela equipe da Nutic ou Ailog, garantindo os requisitos de energia, climatização e layout da sala.
III.	Configurações de software: equipamentos de TI que haja necessidade de instalação/configuração de software, deverão ser executados por profissionais do Nutic, observando o licenciamento e atualizações do aplicativo.
IV.	Das não conformidades: Não será permitida alteração de mesas nos layout das salas preestabelecidas pela Ailog.
V.	Não será permitida a instalação de software não licenciado.
VI.	Os servidores e estações de trabalho devem possuir e manter ativos sistemas de detecção e bloqueio de programas maliciosos (*malware*), tais como, detecção de intrusos, programas antivírus, programas de análise de conteúdo, etc.
VII.	O uso de ativos de TI externos, sejam eles cedidos ou adquiridos, só será permitido após passarem por revisão e homologação pelo Nutic, levando em consideração as regras de atualizações e licenciamento contidas nesta política de segurança.

NP 3 - NORMAS E PROCEDIMENTOS PARA PARA O USO DE E-MAIL	
I.	O E-mail é uma ferramenta de comunicação interna/externa empregada para melhor desempenhar atividades da Seas em ambiente corporativo.

II.	A concessão de contas de e-mail corporativo depende de pedido fundamentado pelo(a) gestor(a) responsável pela respectiva área, informando: nome completo do usuário, cargo, setor no qual está desempenhando suas atividades e justificativa da necessidade da conta de e-mail.
III.	As mensagens de e-mail devem ser escritas em linguagem profissional e que não comprometa a imagem do Seas, bem como não vá de encontro à legislação vigente e nem aos princípios do Código de Ética da Seas.
IV.	O usuário do correio eletrônico institucional terá responsabilidade e responderá pelo seu uso inadequado.
V.	Caso o usuário receba, por algum motivo, uma mensagem que por erro lhe foi enviada deve proceder da seguinte maneira: a) caso seja uma mensagem de endereço @Seas.ce.gov.br, informe ao remetente o ocorrido e remova a mensagem da sua caixa de entrada; b) caso não seja do ambiente @Seas.gov.br, considere a exclusão da mensagem da sua caixa de entrada.
VI.	O usuário deve alterar a senha fornecida no primeiro acesso e guardar a nova senha em sigilo.
VII.	É vedado o encaminhamento de e-mails para listas de distribuição não autorizadas.
VIII.	É vedado o uso da conta de correio eletrônico para fins pessoais.
IX.	O usuário é responsável por utilizar os serviços de correio eletrônico de maneira profissional, ética e legal.
X.	Não devem ser solicitadas informações pessoais dos usuários através de correio eletrônico.
XI.	O usuário não deve clicar em links que solicitem a atualização de suas informações pessoais
XII.	O usuário deve reportar ao Nutic sobre o recebimento de mensagens suspeitas ou que violem estas normas.
XIII.	O usuário tem total responsabilidade pelo envio de anexos nas mensagens, ficando o mesmo também responsável pela garantia da não violação do princípio da legalidade.
XIV.	Quando o usuário for passar um período sem acessar o e-mail, o mesmo deverá deixar uma mensagem de ausência e indicar quem pode ser procurado no seu lugar.
XV.	O usuário deve excluir com frequência e-mails desnecessários, inclusive e-mails da lixeira e da pasta de mensagens enviadas, para não sobrecarregar os recursos tecnológicos.
XVI.	É proibido encaminhar mensagens que representem a opinião pessoal do autor, colocando-a em nome da Seas.
XVII.	As mensagens eletrônicas por e-mail e respectivos arquivos anexados a elas, devem sofrer verificação por ferramenta antivírus.

NP 4 - NORMAS E PROCEDIMENTOS PARA INATIVAÇÃO, EXCLUSÃO E BACKUP DE CONTAS DE E-MAILS INSTITUCIONAIS	
I.	O usuário não deve manter qualquer expectativa de privacidade sobre as mensagens criadas, armazenadas, enviadas ou recebidas por meio do sistema de e-mail corporativo.

II.	A Seas, como proprietária do sistema de e-mail corporativo, poderá, a qualquer tempo e sem aviso prévio, monitorar o uso do sistema e inclusive o conteúdo das mensagens quando julgar necessário.
III.	Os e-mails corporativos são disponibilizados aos usuários como ferramenta de trabalho e, portanto, são propriedades da Seas.
IV.	Após o desligamento do usuário com a Seas, a conta de e-mail será desativada sem acesso de leitura por parte do usuário, seja via IMAP, POP3 ou Webmail. As mensagens armazenadas na caixa postal no momento da desativação serão mantidas por 6 meses.
V.	Antes do término do vínculo ativo com a Seas, cabe ao usuário efetuar cópia de segurança (backup) de dados de seu interesse.
VI.	Sob hipótese alguma será fornecido conteúdo de caixa postal desativada para usuário sem vínculo ativo com a Seas.
VII.	Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora dos centros de processamento de dados mantidos pelas unidades de TI, ficando sob a responsabilidade do indivíduo que usa o(s) dispositivo(s).
VIII.	A comunicação da dispensa é de responsabilidade da Cegep, que informará ao Nutic. Caso a mesma não seja efetuada, o gestor assumirá a responsabilidade do usuário que ainda esteja com acessos a informações corporativas.
IX.	A Cegep deverá estabelecer os procedimentos e fluxos para que as áreas de gestão de pessoas de cada unidade da Seas informe sobre situações de movimentação, aposentadoria e desligamento de servidores no âmbito da Superintendência, para fins de atualização das contas de e-mail da Seas.
X.	O não cumprimento das regras descritas neste documento que complementa a PoSIC, constitui falta grave e o usuário estará sujeito a penalidades administrativas e/ou contratuais.
XI.	Cabe ao(à) gestor(a) responsável pela área do usuário do e-mail inativado, informar ao Nutic antes do período de 6 meses sobre a necessidade de realizar o backup de dados contidos ou ampliação de espera.
XII.	O pedido de acesso aos dados do e-mail inativado dependerá de prévia autorização do CSEP e CI.
XIII.	Sempre que julgar necessário para a preservação da integridade dos recursos computacionais da Seas, dos serviços fornecidos aos usuários ou das informações contidas nestes serviços, os administradores do serviço de e-mail poderão suspender as contas temporariamente e comunicar aos setores responsáveis pela demanda a suspeita de alguma violação. Nesse caso, o responsável pela conta será devidamente notificado por mensagem de e-mail institucional e/ou pessoal, com as justificativas da suspensão, o tempo de suspensão e os procedimentos para reativar a conta.

NP 5 - NORMAS E PROCEDIMENTOS PARA RECEBIMENTO, ENCAMINHAMENTO, ANÁLISE E RESPOSTAS ÀS SOLICITAÇÕES DE INFORMAÇÃO

RECEBIMENTO DE SOLICITAÇÃO DE INFORMAÇÕES E ENCAMINHAMENTO	Os pedidos de acesso à informação deverão ser apresentados por meio de requerimento ao Serviços de Informação ao Cidadão, seja presencialmente, pelo Site Ceará Transparente ou pela Central de Atendimento Telefônico da Ouvidoria pelo telefone 155.
	Pedidos de informação recebidos por ofício, e-mails, ou por telefone devem ser encaminhados ao SIC, para cadastro e prosseguimento do fluxo.
	Esse fluxo não se aplica aos pedidos de informações provenientes do Poder Judiciário, dos Ministérios Públicos Estadual, Federal e do Trabalho e da Defensoria Pública.
ANÁLISE PRELIMINAR PELO SIC	O operador do SIC deverá analisar se a informação está em transparência ativa. Caso positivo, encaminhar a informação ao cidadão.
	Caso a informação não esteja em transparência ativa, o operador deverá analisar se a informação solicitada encontra-se classificada como sigilosa, pessoal ou sensível. Caso positivo, deve encaminhar ao CSAI para providenciar a certidão de negativa.
	Caso a informação não esteja classificada como sigilosa, pessoal ou sensível, o operador do SIC encaminhará a solicitação para a(s) área(s) internas que disponham das informações, concedendo um prazo de 15 dias para a devolutiva.
ANÁLISE E PROVIDÊNCIAS DA ÁREA INTERNA	Recebido o pedido de informação, a área interna deverá avaliar: 1. a disponibilidade das informações; 2. a possibilidade de encaminhar ao SIC dentro do prazo preestabelecido; 3. a necessidade de prorrogação de prazo; 4. a possibilidade de a resposta não ser apresentada e; 5. a necessidade de trabalho adicional para a coleta e organização dos dados.
	Informar ao SIC caso não disponha das informações, não consiga fornecer dentro do prazo estipulado ou necessite de trabalho adicional para o fornecimento das informações.
	Encaminhar ao SIC dentro do prazo preestabelecido a resposta da solicitação ou as justificativas (não existência, necessidade de mais prazo, necessidade de trabalho adicional); A área interna não possui competência para a negativa de fornecimento, cabendo encaminhar, junto com a resposta, suas alegações para avaliação do CSAI.
ANÁLISE FINAL DO CSAI E PROVIDÊNCIAS	Caso entenda ser possível fornecer os dados, o CSAI autorizará o operador do SIC a encaminhar a resposta.

	Caso delibere pelo não fornecimento, os membros do CSAI devem elaborar a certidão negativa e encaminhar ao solicitante.

NP 6 - NORMAS E PROCEDIMENTOS PARA COLETA DE DADOS	
I.	Para verificação da adequação às normas da LGPD, quando houver interesse de alguma coordenadoria realizar pesquisa, censo ou aplicação de qualquer tipo de questionário, de forma on-line ou presencial, faz-se necessária prévia aprovação do CSEP e CI.
II.	A solicitação de consentimento fornecido deve ser explícita, restando o usuário responsável pela escolha informado. Não se deve usar formulários com ideias implícitas ou de difícil acesso.
III.	O usuário pode requerer que seus dados sejam removidos a qualquer momento.
IV.	O coordenador do setor que aplicará o questionário será o responsável legal pela guarda dos dados coletados.
V.	O acesso à política de privacidade deve ser de fácil localização. Os cookies são considerados dados pessoais, pois conseguem identificar as pessoas por meio de informação adquirida quando acessam a internet.

FUNDAMENTAÇÃO LEGAL E NORMATIVAS

Legislação Federal

Lei Federal 8.777, 11 de maio de 2016 - Institui a Política de Dados Abertos do Poder Executivo federal.

Lei Federal n° 12.527, 18 de novembro de 2011 – Lei Federal de Acesso à Informação.

Lei Federal nº 13.709, 14 de agosto 2018 - Lei Geral de Proteção de Dados.

Lei Federal nº 13.460, 26 de junho de 2017 – Dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública.

Legislação Estadual

Decreto nº 32.555, 22 de março de 2018 – Dispõe sobre o compartilhamento de dados dos órgãos e entidades do poder executivo do Estado do Ceará, para permitir sua utilização pelo projeto “big data ceará”, e dá outras providências.

Decreto nº34.100, de 08 de junho de 2021 - Dispõe sobre a Política de Segurança da Informação e Comunicação dos Ambientes de Tecnologia da Informação e Comunicação – TIC do Governo do Estado do Ceará e sobre o Comitê Gestor de Segurança da Informação do Governo do Estado do Ceará – CGSI.

Lei nº 15.175, 28 de julho de 2012 – Lei Estadual de Acesso à Informação. Define regras específicas para a implementação do disposto na Lei Federal N° 12.527, no âmbito da Administração Pública do Estado do Ceará.

Decreto Estadual n° 31.199/2013 - Dispõe sobre a organização e funcionamento dos comitês setoriais de acesso à informação e dos serviços de informações ao cidadão do poder executivo do Estado do Ceará, instituídos pela Lei Estadual nº 15.175, de 28 de junho de 2012,

Portaria do Comitê Gestor de Acesso à Informação n° 01/2016. - Dispõe sobre a uniformização na classificação de informação sigilosa de matéria comum a todos os órgãos e entidades do Poder Executivo Estadual