III – existência de elementos concretos caracterizadores da materialidade e autoria;
IV – observância aos princípios de razoabilidade, pertinência e motivação.
Parágrafo único. Caberá à CSEP-ESP/CE decidir sobre a apuração de denúncias anônimas, situação em que a admissibilidade da denúncia dispensará a observância do inciso I do artigo anterior.
Art. 24. Admitida a denúncia ou aprovada a proposta de apuração de um dos membros da CSEP, o(a) Presidente da Comissão, por sorteio, indicará seu relator, iniciando-se a apuração do processo, por meio de sua Secretaria Executiva, coletando dados e informações e promovendo a notificação do denunciado no prazo de 5 (cinco) dias úteis a contar da admissão da denúncia.
Parágrafo único. A notificação será realizada pela Secretaria-Executiva, mediante comunicação formal ao notificado, assegurando-se o prazo de 15 (quinze) dias úteis, prorrogável por igual período, contados do efetivo recebimento da notificação, para apresentação de defesa por escrito, com a utilização de todos os meios de prova admitidos em direito, inclusive a prova testemunhal.
Art. 25. Recebida a manifestação do denunciado, a Secretaria-Executiva encaminhará os autos ao relator no prazo de três dias.
Art. 26. O relator proferirá seu voto no prazo de 15 (quinze) dias úteis, prorrogável por igual período, após o recebimento dos autos, prazo em que deverá solicitar junto à Secretaria-Executiva da CSEP-ESP/CE a inclusão do processo na pauta da reunião ordinária seguinte.
§1º. Na sessão convocada, o relator apresentará o seu voto, cuja votação seguirá pela Comissão, decidindo o caso, na forma do artigo 16, inciso IV deste Regimento.
§2º. Qualquer membro titular ou suplente, em substituição do titular, poderá pedir vista do processo que terá de devolvê-lo com parecer complementar até a próxima reunião ordinária para manifestar sua apreciação, ou, a qualquer tempo, em reunião extraordinária.
Art. 27. Terminada a votação, a Secretaria-Executiva confeccionará a respectiva ata e providenciará a notificação do agente acerca da deliberação feita pela Comissão.
Art. 28. A Secretaria-Executiva resumirá a decisão da CSEP-ESP/CE em ementa numerada e, em seguida, comunicará, mediante cópia, à CEP, conforme o Decreto Estadual nº 29.887/2009. Como também comunicará à autoridade máxima da autarquia.
Parágrafo único. Decorrido o prazo de interposição do recurso, a Secretaria-Executiva arquivará o processo.
Art. 29. As partes têm o direito a obter cópias reprográficas dos dados e documentos que integram o processo, ressalvados os dados e documentos protegidos por sigilo ou pelos direitos à privacidade, à honra e à imagem.
Art. 30. A CSEP-ESP/CE não poderá se eximir de fundamentar a decisão sobre falta cometida pelo servidor, alegando a falta de previsão no Código de Ética, cabendo-lhe aplicar a analogia, os costumes e os princípios gerais de direito.
Art. 31. Os trabalhos da Comissão devem ser desenvolvidos com celeridade e observância aos princípios de independência e imparcialidade dos seus membros na apuração dos fatos.

Seção IV
Do Recurso

Art. 32. É admissível recurso contra a decisão da CSEP-ESP/CE, que será recebido com efeito suspensivo e deverá ser interposto no prazo de 5 (cinco) dias, contados da notificação da deliberação.
Parágrafo único. O recurso deverá ser interposto perante a CEP, a qual compete atuar como instância recursal das decisões das CSEPs, conforme preceitua o artigo 7º, inciso III, do Decreto Estadual nº 29.887/2009.
Art. 33. Nos casos em que haja recurso à CEP, o arquivamento na CSEP-ESP/CE somente ocorrerá após o trânsito em julgado, conforme disposto no artigo 14, parágrafo único do Decreto Estadual nº 29.887/2009.

CAPÍTULO VII
DAS DISPOSIÇÕES FINAIS

Art. 34. Os membros titulares, em suas ausências e impedimentos, serão substituídos por membros suplentes.
Art. 35. O(a) Secretário(a) executivo(a), em sua ausência e impedimentos, será substituído(a) por um membro da CSEP-ESP/CE.
Art. 36. As opiniões, palavras e votos dos membros da CSEP-ESP/CE serão resguardados pelo princípio da inviolabilidade.
Art. 37. Aos membros da Comissão é assegurada a utilização de horas mensais a serem dedicadas às atividades da CSEP-ESP/CE.
Parágrafo único. É assegurado ao(a) Secretário(a)-Executivo(a) horas mensais para o exercício de suas atribuições, conforme deliberação da CSEP-ESP/CE.
Art. 38. As regras de impedimento e suspeição observarão o disposto no Código de Processo Civil – CPC.
Parágrafo único. O membro da CSEP-ESP/CE que se declarar suspeito ou impedido deverá ser substituído imediatamente.
Art. 39. O presente Regimento somente poderá ser modificado, no todo ou em parte, mediante aprovação da maioria absoluta dos membros titulares e suplentes, em sessão convocada exclusivamente para este fim.
Art. 40. As despesas necessárias para o cumprimento das atribuições previstas no presente regimento serão custeadas pelo orçamento da ESP/CE.
Art. 41. Os casos omissos serão deliberados pela CSEP-ESP/CE.
Art. 42. Este Regimento entra em vigor na data de sua publicação.

*** *** ***

RESOLUÇÃO Nº03/2026 – COMGO/ESP/CE.

APROVA A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO DOS AMBIENTES DE TIC (POSIC) DA ESCOLA DE SAÚDE PÚBLICA DO CEARÁ PAULO MARCELO MARTINS RODRIGUES – ESP/CE.

O Comitê de Governança, por meio do seu Presidente, no uso de suas atribuições legais conferidas no inciso XIII, do Art. 30 do Decreto n.º 35.544, de 22 de junho de 2023; CONSIDERANDO que a Escola de Saúde Pública do Ceará Paulo Marcelo Martins Rodrigues, por força da Lei Estadual n.º 17.476 de 10 de maio de 2021, constitui-se Instituição Científica, Tecnológica e de Inovação Pública, nos termos da Lei Federal n.º 10.973, de 2 de dezembro de 2004 e da Lei n.º 14.220, de 16 de outubro de 2008; e demais normas aplicáveis; CONSIDERANDO a Lei n.º 13.494, de 22 de junho de 2004, alterada pela Lei n.º 16.921, de 08 de julho de 2019 – Lei de Proteção de Dados Pessoais (LGPD); CONSIDERANDO as orientações definidas no Decreto n.º 34.100 de 8 de junho de 2021 (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); CONSIDERANDO a importância do estabelecimento de normas e procedimentos de forma a garantir a integridade, confidencialidade e disponibilidade das informações no contexto da ESP/CE; CONSIDERANDO que foi deliberada a aprovação da Política de Segurança da Informação e Comunicação dos Ambientes de TIC (POSIC) pelo Comitê de Governança durante a 21ª Reunião realizada no dia 18 de novembro de 2025, conforme informações contidas no NUP n.º 24022.008837/2025-73: RESOLVE:

Art. 1º Aprovar a Política de Segurança da Informação e Comunicação dos Ambientes de TIC (POSIC) da Escola de Saúde Pública do Ceará Paulo Marcelo Martins Rodrigues, na forma do Anexo Único desta Resolução.

Art. 2º Esta Resolução entra em vigor na data de sua publicação, revogadas as disposições em contrário.

Fortaleza, 06 de abril de 2026.

Luciano Pamplona de Góes Cavalcanti
PRESIDENTE DO COMITÊ DE GOVERNANÇA

ANEXO ÚNICO DA RESOLUÇÃO Nº03/2026.
Política de Segurança da Informação e Comunicação dos Ambientes de TIC (POSIC)

1. INTRODUÇÃO

A segurança da informação e comunicação representa a salvaguarda das informações, frente a uma variedade de ameaças, com o objetivo primordial de assegurar a continuidade do negócio da instituição, mitigar riscos, otimizar o retorno sobre os investimentos e maximizar as oportunidades.
A efetiva segurança da informação e comunicação é alcançada mediante a implementação de um conjunto apropriado de controles, abrangendo políticas, processos, procedimentos, estruturas organizacionais e componentes de software e hardware. É imperativo que esses controles sejam devidamente estabelecidos, implementados, monitorados, submetidos a análises críticas regulares e aprimorados, quando necessário, a fim de garantir a realização dos objetivos institucionais e de segurança. É aconselhável que tais medidas sejam integradas harmoniosamente com outros processos de gestão.
A informação, acompanhado dos sistemas e redes de computadores que a suportam, representam ativos de significativa importância para as operações da Instituição. Portanto, a definição, o alcance, a manutenção e a melhoria da segurança da informação e comunicação constituem atividades vitais para assegurar o desempenho eficaz, a conformidade com requisitos legais e a reputação da Instituição perante a sociedade.
Nesse contexto, as organizações, somado a seus sistemas de informação e redes de computadores, estão expostas a uma diversidade de ameaças à segurança da informação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndios e inundações. Além disso, as ameaças representadas por códigos maliciosos e intrusões de hackers tornam-se cada vez mais frequentes, ambiciosas e notavelmente sofisticadas.
Em conformidade com o Decreto nº 34.100, de 08 de junho de 2021, uma das diretrizes estratégicas do Governo do Estado é a adequação da segurança da informação e a proteção de dados pessoais. Nesse contexto, a política de segurança tem como objetivo contribuir de forma efetiva para esse propósito, assegurando a proteção das informações sensíveis, a integridade do parque tecnológico e a continuidade dos serviços prestados pela ESP/CE. Além disso, busca garantir o interesse público, oferecendo atendimento de qualidade no âmbito da saúde pública.
A crescente interconexão de redes públicas e privadas, bem como o compartilhamento de recursos de informação, aumentam a complexidade do controle de acesso. É importante observar que muitos sistemas de informação não foram concebidos com foco na segurança. Portanto, a segurança da informação e comunicação que pode ser obtida por meios técnicos é inerentemente limitada e requer o respaldo de uma administração sólida e procedimentos adequados.
A identificação e implementação dos controles necessários demandam planejamento meticuloso e atenção aos detalhes.

A Escola de Saúde Pública do Ceará Paulo Marcelo Martins Rodrigues (ESP/CE) tem como missão "Promover o desenvolvimento de excelência da força de trabalho em saúde por meio da Educação Permanente, apoiado pela ciência, inovação e tecnologia, visando o fortalecimento do SUS e a melhoria da qualidade de vida das pessoas", contribuindo para a melhoria da saúde pública, em benefício da sociedade. Para cumprimento de sua missão institucional é fundamental que os processos executados nesta Instituição sejam conduzidos de forma segura, com a proteção de seus ativos, preservando a integridade, confidencialidade e disponibilidade das informações.

2. SOBRE A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO (POSIC)

2.1. A presente Política de Segurança da Informação e Comunicação (POSIC) está em conformidade com as legislações em vigor no Brasil, sendo formulada com base no Decreto Estadual Nº34.100, datado de 08 de junho de 2021. Além disso, a POSIC encontra-se alinhada à missão institucional e ao planejamento estratégico da ESP/CE, seguindo as recomendações preconizadas pela norma ABNT NBR ISO/IEC 27002:2022.

3. CONCEITOS E DEFINIÇÕES

3.1. Ameaça: causa potencial de um incidente indesejado.

3.2. Ativo: todo e qualquer bem da ESP/CE seja físico ou digital, como também a informação e os recursos que permitem seu tratamento, tráfego e armazenamento.

3.3. Backup: Cópia de segurança de dados.

3.4. Código Malicioso: programa que possibilita ações danosas, como vírus, worms, trojans, spywares, malware, botnet, ransomware, entre outros.

3.5. Colaborador Interno: qualquer pessoa que execute atividade profissional e que possua algum tipo de vínculo com a ESP/CE (Exemplos: servidores, terceirizados e bolsistas).

3.6. Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

3.7. Custodiante: quem detém a guarda da informação, mas não é necessariamente seu proprietário.

3.8. Dados: são registros brutos de fatos, eventos ou observações, em diferentes formas como números, textos, imagens, sons ou símbolos, que ao serem organizados e interpretados em um contexto específico transformam-se em informação útil.

3.9. Dados Pessoais: informação relacionada a pessoa natural/física identificada ou identificável.

3.10. DICIT: Diretoria de Inovação, Ciência e Tecnologia em Saúde

3.11. Disponibilidade: garantia de que os usuários autorizados obtenham, sempre que necessário, acesso à informação e aos ativos correspondentes.

3.12. ESP/CE: Escola de Saúde Pública do Ceará Paulo Marcelo Martins Rodrigues.

3.13. GETIC: Gerência de Tecnologia da Informação e Comunicação da ESP/CE.

3.14. Informação: todo e qualquer conteúdo ou conjunto de dados que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para o uso restrito ou exposta ao público para consulta ou aquisição.

3.15. Incidente: segundo a ABNT NBR ISO/IEC 27000:2018, um incidente de segurança da informação é definido como um evento ou uma série de eventos indesejados ou inesperados relacionados à segurança da informação que têm probabilidade significativa de comprometer as operações do negócio e ameaçar a segurança da informação.

3.16. Integridade: de acordo com a ABNT NBR ISO/IEC 27000:2018, integridade é definida como a propriedade de salvaguardar a exatidão e a completeza de ativos.

3.17. LGPD: Lei Geral de Proteção de Dados Pessoais.

3.18. Usuário Interno: pessoa vinculada à instituição (como servidor, funcionário ou bolsista) que utiliza seus sistemas e recursos para atividades internas e institucionais

3.19. Usuário Externo: pessoa que não possui vínculo com a instituição, mas acessa seus sistemas, serviços ou informações para fins específicos ou eventuais, como cidadãos, empresas ou outras entidades.

3.20. POSIC: Política de Segurança da Informação e Comunicação dos Ambientes de TIC.

3.21. Spam: e-mails não solicitados e normalmente enviados para um grande número de pessoas.

3.22. TIC: Tecnologia da Informação e Comunicação.

3.23. Usuário: colaboradores internos e externos que tenham acesso aos recursos oferecidos pela ESP/CE.

3.24. Vírus: programa malicioso que se propaga e infecta dispositivos.

3.25. WAF: Firewall de aplicativos Web (Web Application Firewall). É uma solução de segurança que protege aplicações web contra os ataques, filtrando e monitorando o tráfego HTTP entre a aplicação e a internet.

3.26. Worm: programa semelhante ao vírus, que infecta o sistema, tendo como característica a auto replicação.

4. OBJETIVO

4.1. O propósito da presente Política consiste em estabelecer princípios, diretrizes, normas e procedimentos gerais para a administração da segurança da informação nos ambientes de Tecnologia da Informação e Comunicação (TIC) da ESP/CE. Isso visa preservar a integridade, confidencialidade e disponibilidade das informações, delineando orientações e procedimentos para a manipulação, controle e salvaguarda das informações contra perdas, alterações, divulgações indevidas e acessos não autorizados.

5. ABRANGÊNCIA

5.1. A POSIC aplica-se de forma abrangente a todas as áreas, instalações, equipamentos, materiais, documentos, pessoas, sistemas de informação e demais ativos da Escola de Saúde Pública do Ceará – ESP/CE. Nos termos das diretrizes estabelecidas pela Lei nº 13.709/2018 e do Decreto Estadual nº 34.100, esta Política, estende-se, obrigatoriamente a:

I – servidores públicos;
II – empregados públicos;
III – terceirizados;
IV – bolsistas;
V – estagiários;
VI – prestadores de serviço;
VII – consultores externos;
VIII – parceiros institucionais;
IX – quaisquer terceiros que, direta ou indiretamente, tenham acesso a dados, informações ou ativos de TIC da ESP/CE.

5.2. A POSIC abrange os domínios de segurança e defesa cibernética, segurança física e proteção de dados organizacionais e tem por escopo as ações destinadas a preservação da confidencialidade, Integridade, disponibilidade, e autenticidade das informações.

5.3. Cada usuário é responsável por manter-se continuamente atualizado em relação a esta Política e às normas correlatas. Sempre que houver dúvidas quanto à aquisição, utilização, compartilhamento ou descarte de informações, deverá buscar orientação junto ao gestor imediato ou à GETIC, de modo a garantir a correta aplicação das diretrizes estabelecidas.

5.4. O descumprimento das disposições desta Política sujeitará o infrator às medidas administrativas, civis e penais cabíveis, conforme legislação aplicável.

6. COMPETÊNCIAS E RESPONSABILIDADES

6.1. DIREÇÃO SUPERIOR DA ESP/CE

6.1.1. À Direção Superior da ESP/CE cabe:

6.1.1.1. Zelar pelo fiel cumprimento ao estabelecido nesta Política;

6.1.1.2. Garantir recursos necessários para a implementação das diretrizes e procedimentos previstos nesta Política;

6.1.1.3. Promover a disseminação da POSIC.

6.2. DIRETORIA DE INOVAÇÃO, CIÊNCIA E TECNOLOGIA EM SAÚDE

6.2.1. Ao Diretor da DICIT cabe:

6.2.1.1. Coordenar as ações para implantação das Políticas de Segurança da informação no âmbito da ESP/CE;

6.2.1.2. Analisar, aprovar, acompanhar e avaliar as principais iniciativas de Segurança da Informação nos ambientes de TIC da ESP/CE;

6.2.1.3. Planejar e coordenar a execução dos programas, planos, projetos e ações de segurança;

6.2.1.4. Deliberar sobre as questões que lhe tenham sido encaminhadas.

6.3. GERÊNCIA DE TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO

6.3.1.Ao Gerente da GETIC cabe:

6.3.1.1 Supervisionar, analisar e avaliar a efetividade dos processos, procedimentos, sistemas e dispositivos de segurança da informação;

6.3.1.2. Monitorar e auditar continuamente o uso da internet, sendo o colaborador passível de prestar contas sobre sua utilização;

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

6.3.1.4. Suspender, a qualquer tempo, o acesso de usuário a recurso computacional quando evidenciado riscos à segurança da informação, informando a alta gestão e demais interessados;

6.3.1.5. Promover a elaboração e implantação de planos de contingência e recuperação de desastres de TIC;

6.3.1.6. Recepcionar, organizar, armazenar e tratar adequadamente as Informações de eventos e incidentes de segurança da informação da ESP/CE, determinando aos respectivos gestores as ações corretivas ou de contingência em cada caso;

6.3.1.7. Comunicar imediatamente à DICIT toda e qualquer violação de Segurança da Informação, incluindo violação de dados pessoais, bem como informar as demais áreas quando houver necessidades específicas.

6.4. GESTORES DAS ÁREAS DA ESP/CE

6.4.1. Aos Gestores das áreas cabe:
6.4.1.1. Manter postura em relação à Segurança da Informação e servir de modelo de conduta para os colaboradores sob a sua gestão;
6.4.1.2. Disseminar a POSIC para os colaboradores de suas áreas;
6.4.1.3. Comunicar de forma tempestiva, pelos meios oficiais instituídos, a revogação de acessos e recursos computacionais de colaboradores das suas áreas quando for pertinente;
6.4.1.4. Garantir a implementação de mecanismos necessários para o descarte seguro das informações;
6.4.1.5. Solicitar formalmente à GETIC os devidos acessos aos ativos de informação a serem utilizados pelo setor ou compartilhados com terceiros, usando os meios homologados pela ESP/CE;
6.4.1.6. Adaptar os processos, procedimentos e normas sob sua responsabilidade para atender à POSIC;
6.4.1.7. Observar e zelar pela aplicação das regras e legislações de proteção de dados;
6.5. USUÁRIOS INTERNOS
6.5.1. Os usuários internos têm as seguintes responsabilidades:
6.5.1.1. Cumprirem as determinações constantes nesta Política, independentemente do nível hierárquico ou função, bem como do vínculo empregatício;
6.5.1.2. Buscar orientação da GETIC quando houver dúvidas relacionadas à Segurança da Informação;
6.5.1.3. Responsabilizar-se pelo ativo de TIC e por sua adequada utilização;
6.5.1.4. Responder por toda violação de segurança praticada por si;
6.5.1.5. Utilizar os serviços e recursos somente para as necessidades autorizadas, assegurando que os recursos tecnológicos sejam utilizados apenas para fins profissionais aprovados e de interesse da Instituição;
6.5.1.6. Proteger sua senha de acesso e não compartilhar, sendo responsável por todas as ações realizadas com sua identificação;
6.5.1.7. Utilizar somente programas legalizados ou analisados tecnicamente pela GETIC, sendo expressamente, proibido o uso/instalação de software não licenciado;
6.5.1.8. 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;
6.5.1.9. Prezar pela segurança das informações confidenciais, incluindo todo e qualquer dado pessoal a que tiver acesso;
6.5.1.10. Atender à LGPD, protegendo os dados a que tiver acesso ou que venha a manuseá-los, sempre em conformidade às regras da ESP/CE;
6.5.1.11. Assumir a responsabilidade por eventuais prejuízos ou danos sofridos ou causados à ESP/CE e/ou a terceiros, em decorrência da não obediência às diretrizes e às normas aqui referidas.
6.5.2. É vedado aos colaboradores internos:
6.5.2.1. Realizar qualquer procedimento que envolva suporte técnico, tais como manutenção de equipamentos, instalação de software, alteração nas configurações do sistema e outras similares, sem a devida autorização da GETIC;
6.5.2.2. Acessar, via Internet, sites que comprometam a segurança e infrinjam à cultura organizacional, a legislação e as normas estabelecidas da ESP/CE;
6.5.2.3. Divulgar sua senha de acesso à rede para qualquer pessoa, pois a informação é de caráter pessoal e intransferível;
6.5.2.4. Utilizar arquivos e dados de outro colaborador interno, sem a devida autorização;
6.5.2.5. Enganar ou subverter as medidas de segurança dos sistemas e da rede de comunicação.
6.6. USUÁRIOS EXTERNOS
6.6.1. Os usuários externos têm as seguintes responsabilidades:
6.6.1.1. Cumprir os preceitos estipulados por esta POSIC, quando estiverem executando atividades no ambiente da ESP/CE;
6.6.1.2. Responder por toda atividade executada por meio de sua identificação;
6.6.1.3. Responder por toda violação de segurança praticada por si, sem prejuízo da responsabilização da contratada ou de entidade/órgão ao qual está vinculado;
6.6.1.4. Seguir as recomendações e as boas práticas de utilização dos recursos ofertados pela ESP/CE para a execução de suas atividades;
6.6.1.5. Assinar o Termo de Compromisso, formalizando a ciência e o aceite da Política de Segurança e de suas normas.
7. PRINCÍPIOS
7.1. Os equipamentos de tecnologia da informação e comunicação, os sistemas e as informações devem ser utilizados para a realização de atividades profissionais, com senso de responsabilidade e preceitos éticos comuns à sociedade e dentro da legalidade. Respeitar a privacidade dos usuários, agindo de forma ética e atendendo aos princípios da Lei Geral de Proteção de Dados.
7.2. As ações de segurança da informação da ESP/CE têm como norte as definições contidas na Política de Segurança da Informação e Comunicação dos ambientes de Tecnologia da Informação e Comunicação – TIC do Governo do Estado do Ceará, contendo os seguintes princípios orientadores:
7.3. Alinhamento Estratégico: considera o alinhamento da Política de Segurança da Informação com o Planejamento Estratégico e com os demais instrumentos de governança de TIC do Governo do Estado do Ceará;
7.4. Diversidade Organizacional: considera a diversidade das atividades da Instituição de forma a garantir a continuidade do seu negócio;
7.5. Garantia da Segurança das Informações: considera a adoção de medidas que visem garantir a confidencialidade, disponibilidade e integridade das informações da Instituição;
7.6. Propriedade da Informação: considera que toda informação produzida ou armazenada no Estado é de sua propriedade e não de seus colaboradores, exceto os casos onde a Instituição atua como custodiante da informação, devendo seu uso ser destinado, exclusivamente, a atender aos interesses da Instituição e seguindo todos os preceitos estabelecidos pela LGPD;
7.7. Alinhamento com Aspectos Legais: considera o alinhamento da Política de Segurança da Informação com as legislações vigentes e os demais regulamentos específicos aplicáveis à Administração Pública Estadual.
8. DIRETRIZES
8.1. Na POSIC foram definidas diretrizes que devem ser observadas conforme abaixo:
8.1.1. As ações relacionadas à Segurança da Informação que serão necessárias ao cumprimento desta Política devem ser consideradas na ocasião da elaboração/revisão do Planejamento Estratégico da ESP/CE;
8.1.2. Os colaboradores internos deverão realizar a entrega do Termo de Confidencialidade e Segurança da Informação, como condição imprescindível para que possa ser concedido acesso aos ativos de informação disponibilizados pela ESP/CE;
8.1.3. Qualquer demanda de colaboradores internos relacionados a ativos de TIC deverá ser realizada por meio do sistema de chamado definido pela ESP/CE;
8.1.4. A POSIC deverá ser disseminada de forma permanente por meio de campanhas de conscientização com o intuito de assegurar que todos os colaboradores conheçam as suas orientações;
8.1.5. Todos os usuários são responsáveis pela segurança dos ativos de informação que estejam sob sua custódia e pelo uso e guarda de suas credenciais de acesso, sendo vedada a exploração de eventuais vulnerabilidades – que, assim que identificadas, devem ser imediatamente comunicadas à DICIT/GETIC;
8.1.6. Deverá constar em todos os contratos da ESP/CE, quando o objeto for pertinente, cláusula de confidencialidade e de obediência às normas de segurança da informação a ser cumprida por empresas fornecedoras e por todos os profissionais que desempenham suas atividades na ESP/CE, inclusive provenientes de organismos internacionais.
9. DIRETRIZES ESPECÍFICAS
9.1. As Diretrizes Específicas da POSIC são:
9.1.1. ACESSO À INTERNET
9.1.1.1. Os colaboradores devem acessar exclusivamente ferramentas, sites e aplicativos relacionados ao trabalho que desempenham;
9.1.1.2. Nos casos em que determinado colaborador necessite acessar algum conteúdo que esteja bloqueado pelos mecanismos de segurança, deverá ser aberto um chamado solicitando a liberação do acesso, onde a DICIT/GETIC fará a liberação desde que o conteúdo solicitado não proporciona riscos para a segurança da ESP/CE;
9.1.1.3. Os visitantes poderão ter acesso à internet por meio do wi-fi exclusivo para esse público ESP-VISITANTES;
9.1.1.4. Cabe à DICIT/GETIC, monitorar e bloquear automaticamente sites que contenham conteúdos contrários às legislações vigentes;
9.1.1.5. Qualquer necessidade de download de programas/softwares deve ser repassada à DICIT/GETIC, sendo registrado o pedido por meio de canal oficial definido pela ESP/CE;
9.1.2. CORREIO ELETRÔNICO
9.1.2.1. A GETIC será responsável pelo gerenciamento, adição, exclusão e adoção de medidas operacionais visando conter a propagação de e-mails suspeitos no ambiente de tecnologia da ESP/CE em conformidade com a política de segurança da informação do Estado;
9.1.2.2. A qualquer tempo, mediante detecção pelos sistemas e/ou identificação de e-mails suspeitos pela equipe de suporte responsável pelo monitoramento do sistema de correio eletrônico, a GETIC procederá com as configurações necessárias objetivando conter eventuais propagações de e-mails suspeitos na ESP/CE;
9.1.2.3. O colaborador deverá efetuar abertura de chamados técnicos no sistema de abertura de chamados da ESP/CE, quando houver necessidade de análise de e-mails suspeitos de SPAM pela GETIC;
9.1.2.4. O colaborador é responsável direto pelas mensagens enviadas por intermédio do seu endereço de correio eletrônico;
9.1.2.5. O colaborador deverá evitar o envio de informações sensíveis por e-mail, a menos que seja estritamente necessário, sempre observando a LGPD;
9.1.2.6. O colaborador deverá acessar e utilizar o correio eletrônico somente para fins relacionados ao trabalho sempre respeitando as políticas de privacidade estabelecidas pela Instituição;
9.1.2.7. Antes de abrir anexos ou links enviados por remetentes desconhecidos, o colaborador deverá consultar a GETIC para análise, a fim de evitar a propagação de vírus;

9.1.2.8. O colaborador deverá participar de treinamentos sobre a LGPD e as políticas internas relacionadas à privacidade de dados, quando oferecidos pela ESP/CE.
9.2. GESTÃO DE INCIDENTES
9.2.1. O colaborador da ESP/CE deverá notificar à GETIC de forma imediata caso tenha conhecimento sobre qualquer incidente de segurança;
9.2.2. A GETIC deverá elaborar um Plano de Resposta a Incidentes para estabelecer as ações a serem realizadas e o(s) colaborador(es) que será(ão) acionado(s) para os possíveis incidentes de segurança da informação.
9.3. SISTEMAS
9.3.1. Os códigos-fonte dos sistemas gerenciados pela ESP/CE deverão estar armazenados em repositórios de controle internos oficiais da Instituição;
9.3.2. Todos os sistemas da ESP/CE deverão ter ambientes de desenvolvimento e produção, podendo ter, ainda, ambientes de testes e homologação;
9.3.3. Os sistemas web da ESP/CE deverão utilizar um certificado válido SSL;
9.3.4. Os sistemas da ESP/CE deverão ter um padrão para a definição de senhas fortes;
9.3.5. A ESP/CE deverá utilizar um WAF (Web Application Firewall) para proteger suas aplicações web de possíveis ataques;
9.3.6. No processo de desenvolvimento de sistemas deverão ser observados padrões de segurança que não ocasionam vulnerabilidades nas ferramentas da ESP/CE.
9.4. PROPRIEDADE INTELECTUAL
9.4.1. As informações de propriedade da ESP/CE devem ser utilizadas exclusivamente para os fins a que se destinam, sendo expressamente vedada a sua apropriação por qualquer usuário, seja interno ou externo.
9.5. PROTEÇÃO DE DADOS PESSOAIS
9.5.1. A ESP/CE aplicará as diretrizes dispostas na LGPD e demais leis de proteção de dados homologadas pelas instâncias de Governo superiores.
9.6. UTILIZAÇÃO DE ATIVOS
9.6.1. Não serão permitidas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede, conta ou sistema;
9.6.2. O colaborador deverá ativar o bloqueio de acesso do seu usuário na estação de trabalho sempre que se ausentar temporariamente do equipamento;
9.6.3. Materiais que violem a legislação vigente, as normas internas da instituição ou as políticas de uso aceitável não podem ser acessados, exibidos, armazenados ou distribuídos por meio de quaisquer ferramentas ou dispositivos utilizados na rede;
9.6.4. Todos os dados relativos à ESP/CE e suas áreas devem ser mantidos preferencialmente no servidor de arquivos e/ou alternativamente no drive da nuvem, onde existem sistemas de backup periódico;
9.6.5. Todos os documentos digitais - como vídeos, imagens, planilhas, textos, entre outros - que sejam de uso pessoal, não são de responsabilidade da ESP/CE, ou seja, estão sujeitos à exclusão definitiva, sem a possibilidade de recuperação;
9.6.6. O acesso ao Datacenter é restrito exclusivamente à equipe da DICIT/GETIC. Caso haja necessidade de entrada por parte de outra área ou de prestadores de serviço, o acesso somente será permitido mediante o acompanhamento de um colaborador autorizado da equipe de infraestrutura.
9.7. CONTAS, SENHAS E AUTENTICAÇÃO
9.7.1. As senhas para os colaboradores deverão conter no mínimo 8 (oito) caracteres, sendo obrigatório o uso de letras maiúsculas e minúsculas, números e caracteres especiais;
9.7.2. Em caso de suspeita de comprometimento da senha, o colaborador deverá alterá-la de imediato;
9.7.3. A senha é individual e intransferível, devendo ser mantida em sigilo. É proibido o seu compartilhamento;
9.7.4. As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos, blocos de anotações, agendas ou qualquer outro meio acessível em linguagem compreensível por humanos, sem o devido uso de criptografia;
9.7.5. A senha do usuário institucional será alterada a cada 90 (noventa) dias.
10. REQUISITOS DA POSIC
10.1. A POSIC deve ser comunicada a todos os colaboradores visando à efetividade e à real cultura de uso ético e legal dos recursos tecnológicos, bem como à Segurança da Informação da ESP/CE.
10.2. Sempre que uma parceria ou contratação de fornecedor envolver acesso a informações e/ou recursos tecnológicos da ESP/CE, a gerência contratante deverá informar à GETIC.
10.3. Serão criados e implementados controles adequados, bem como trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas que a ESP/CE considerar necessários, visando reduzir os riscos aos ativos de informação.
10.4. Os dados coletados seguem rigorosamente o disposto nas leis de proteção de dados, em especial à LGPD.
10.5. A ESP/CE reserva-se o direito de adotar as medidas administrativas e judiciais cabíveis no caso de descumprimentos dessa política de segurança, bem como de analisar dados e evidências para a obtenção de provas a serem utilizadas em processos investigativos e judiciais.
10.6. O não cumprimento dos requisitos previstos nesta POSIC acarretará violação às regras internas da Instituição, e o usuário estará sujeito a medidas administrativas e legais cabíveis.
11. REVISÃO
11.1. Essa Política deverá ser revisada a cada 2 (dois) anos, a contar da data da sua publicação, podendo haver ajustes ou atualizações em qualquer período caso seja necessário.
12. SANÇÕES
12.1. 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.
12.2. A DICIT/GETIC 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.
12.3. O desconhecimento das regras desta POSIC não exime o usuário de suas responsabilidades por atos praticados em sua desconformidade.
12.4. As violações das diretrizes, normas ou procedimentos que, juntas, formam esta POSIC resultarão em responsabilizações administrativas, cíveis e penais, sendo devidamente aplicadas as sanções cabíveis, conforme previsão legal.
13. CONSIDERAÇÕES FINAIS
13.1. A POSIC representa um marco estratégico para a Escola de Saúde Pública do Ceará (ESP/CE), consolidando o compromisso institucional com a segurança da informação e a governança digital. A política estabelece diretrizes claras para proteger dados, processos e sistemas, garantindo a confidencialidade, integridade, autenticidade, disponibilidade e conformidade legal das informações.
14. REFERÊNCIAS
a) Decreto Estadual n° 34.100, de 8 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;
b) Lei Federal no 13.709 de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoas;
c) Lei nº 12.965, de 23 de abril de 2014;
d) Lei Nº 12.527, de 18 de novembro de 2011;
e) Lei Estadual nº 15.175, de 28 de junho de 2021 (DOE 11.07.12)
f) Lei n.º 13.494, de 22 de junho de 2004, alterada pela Lei n.º 16.921, de 08 de julho de 2019 – Lei de Proteção de Dados Pessoais (LGPD);
g) ABNT ISO/IEC 27001 e 27002, Segurança da Informação.

TERMO DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO
IDENTIFICAÇÃO DO CONTRATO:

No Contrato	
Nome da Empresa	
CNPJ	
Objeto Resumido	
Vigência	

Termos:
OS funcionários abaixo qualificados declaram ter pleno conhecimento de suas responsabilidades no que concerne ao sigilo a ser mantido sobre as atividades desenvolvidas ou as ações realizadas no âmbito deste Contrato, bem como todas as informações que eventualmente tomem conhecimento, comprometendo-se a guardar sigilo necessário nos termos da legislação vigente e prestar total obediência às normas de segurança da informação, vigentes no ambiente da Contratante.
De Acordo:

IDENTIFICAÇÃO DOS DECLARANTES	ASSINATURAS
Nome: CPF: Nome: CPF:	