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:	