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