Portaria SES/PE nº 129, de 26 de fevereiro de 2026

Institui no âmbito da Secretaria Estadual de Saúde de Pernambuco (SES-PE), a Política de Segurança da Informação (PSI) e estabelece o Sistema Gestor de Segurança da Informação (SGSI).

A Secretária Estadual de Saúde, no uso das atribuições legais que lhe foram conferidas com base na delegação do Ato Governamental nº **198**, publicado no Diário Oficial do Estado em **24** de **janeiro** de **2023**, e,

CONSIDERANDO o firme compromisso da gestão em garantir níveis satisfatórios de segurança e proteção, estabelecer diretrizes,

responsabilidades e controles para garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações;

CONSIDERANDO que as informações produzidas, coletadas de terceiros, hospedadas, armazenadas ou em trânsito por esta Secretaria Estadual de Saúde, representadas em formatos físicos ou digitais, podem ser vulneráveis a incidentes que comprometa sua integridade, como desastres naturais, acessos não autorizados, mau uso, falhas de equipamentos, extravio e furto;

CONSIDERANDO a importância de aprimorar o desenvolvimento das práticas de governança e gestão da Segurança da Informação, com o objetivo de alinhar-se de forma contínua aos cenários em constante evolução dos riscos cibernéticos;

CONSIDERANDO a NBR ISO/IEC 27001:2022, que estabelece diretrizes para práticas de gestão e normas de segurança da informação;

CONSIDERANDO a Lei Federal nº 13.709, de 14 de agosto de 2018 que institui a Lei Geral de Proteção de Dados Pessoais (LGPD);

CONSIDERANDO o Decreto Estadual nº 49.914, de 10 de dezembro de 2020, que institui a Política Estadual de Segurança da Informação – PESI, no âmbito da Administração Pública Estadual.

Resolve:

Art. 1º Fica instituída a Política de Segurança da Informação (PSI) no âmbito da Secretaria Estadual de Saúde de Pernambuco (SES-PE) e estabelece seu Sistema Gestor de Segurança da Informação (SGSI).

Parágrafo único. Todos os instrumentos normativos gerados a partir da Política de Segurança da Informação - PSI são partes integrantes desta e procedem dos princípios e diretrizes nela estabelecidos.

Art 2º Esta Política de Segurança da Informação (PSI) abrange todos os recursos de informação, sistemas, processos e colaboradores da SES, independentemente do formato ou meio em que as informações são armazenadas, processadas ou transmitidas.

Art 3º Dos princípios de Segurança da Informação:

Esta PSI adotará os seguintes princípios de segurança da informação:

Art 3.1 Quanto à **confidencialidade das informações**: A Secretaria Estadual de Saúde de Pernambuco (SES-PE) prioriza a confidencialidade de todas as informações sob sua responsabilidade, especialmente dados de saúde dos cidadãos. O acesso a informações sensíveis será restrito a profissionais autorizados, mediante controles rigorosos e criptografia. Esta política está alinhada aos objetivos estratégicos da SES, visando proteger a privacidade e a segurança dos dados. A violação da confidencialidade resultará em medidas disciplinares e legais, conforme aplicável. A SES-PE compromete-se a manter a confidencialidade como pilar fundamental de suas operações, garantindo a confiança da população.

Art 3.2 Quanto à **integridade das informações:** A Secretaria Estadual de Saúde de Pernambuco (SES-PE) considera a integridade das informações como um princípio essencial em todas as suas operações, especialmente no que diz respeito aos dados de saúde dos cidadãos. A SES-PE implementa rigorosos controles de acesso e auditorias regulares, essas práticas estão alinhadas aos objetivos estratégicos da SES, que buscam assegurar a qualidade e a precisão dos dados. Qualquer alteração não autorizada ou comprometimento da integridade das informações resultará em ações corretivas e, se necessário, em medidas legais ou disciplinares, de acordo com a gravidade da situação. A SES-PE reafirma seu compromisso em manter a integridade como um dos pilares fundamentais de seu funcionamento, promovendo a confiança e a proteção dos dados da população. Todos os colaboradores são responsáveis por zelar pela integridade dos dados, seguindo as diretrizes da política de segurança.

Art 3.3 Quanto à **disponibilidade das informações:** A Secretaria Estadual de Saúde de Pernambuco (SES-PE) prioriza a disponibilidade dos dados de saúde dos cidadãos, assegurando que as informações estejam sempre acessíveis para profissionais autorizados. Para isso, a SES-PE implementa uma infraestrutura robusta que inclui redundância de sistemas, backups regulares e monitoramento contínuo de servidores, minimizando o risco de interrupções ou falhas. Essas práticas visam garantir que os dados estejam disponíveis quando necessário, permitindo uma resposta ágil e eficaz em situações críticas. Em caso de incidentes que possam comprometer a disponibilidade das informações, a SES-PE possui um plano de respostas a incidentes que assegura a rápida restauração dos serviços. O compromisso da SES-PE em manter a disponibilidade como um pilar fundamental de suas operações é essencial para garantir a continuidade do atendimento à população e a confiança nos serviços prestados.

Art 3.4 Quanto à **autenticidade das informações:** A Secretaria Estadual de Saúde de Pernambuco (SES-PE) considera a autenticidade dos dados de saúde como um princípio essencial para garantir a confiança nas informações. Qualquer tentativa de comprometer a autenticidade dos dados será rigorosamente investigada e sujeita a medidas disciplinares e legais, conforme aplicável. O compromisso da SES-PE em manter a autenticidade como pilar

fundamental é vital para proteger os dados dos cidadãos e preservar a confiança da população nos serviços oferecidos.

Art 3.5 Quanto ao **não repúdio das informações**: A Secretaria Estadual de Saúde de Pernambuco (SES-PE) assegura a responsabilidade e transparência na gestão de dados dos cidadãos, fortalecendo a confiança nas comunicações digitais. A individualização de acessos e alterações nos sistemas garante a autoria das ações, prevenindo fraudes e contestação de responsabilidades. Cada profissional é responsável pelas ações que realiza, o que permite rastrear e comprovar a autoria de cada evento. Essa prática demonstra o compromisso da SES-PE com a segurança da informação, assegurando um ambiente digital confiável. A violação dessa norma pode acarretar em investigações e medidas disciplinares e legais, conforme aplicável.

Art 4º Do Sistema Gestor de Segurança da Informação (SGSI)

Art 4.1 O objetivo da Política de Segurança da Informação da Secretaria de Saúde do Estado de Pernambuco (SES-PE) é estabelecer diretrizes claras e efetivas para a implementação e manutenção do seu Sistema de Gestão da Segurança da Informação (SGSI). Essa política visa garantir a proteção, confidencialidade, integridade e disponibilidade das informações relacionadas à saúde pública, assegurando que os dados dos cidadãos estejam protegidos contra acessos não autorizados, vazamentos e outras ameaças.

Através da adoção do SGSI, a SES-PE busca promover uma cultura de segurança da informação que envolva todos os colaboradores, desde a alta administração até os usuários finais, enfatizando a responsabilidade coletiva na proteção dos ativos de informação.

O SGSI permitirá a identificação e avaliação contínua de riscos, a implementação de controles adequados e a resposta eficaz a incidentes de segurança.

Art 4.2 Processos organizacionais do Sistema de Gestão da Segurança da Informação (SGSI)

Art 4.2.1 Quanto ao **Planejamento Estratégico** das Ações de Segurança da Informação:

O planejamento estratégico das ações de segurança da informação visa a proteção dos dados sensíveis e garantia da continuidade das operações de TI no âmbito da Secretaria Estadual de Saúde de Pernambuco. Envolve a identificação de ativos de informação, avaliação de riscos e definição de políticas e diretrizes que assegurem a confidencialidade, integridade e disponibilidade das informações. Estabelece responsabilidades claras e controles de acesso, promovendo um ambiente seguro onde todos os colaboradores são engajados na proteção das informações. Esta abordagem não só minimiza vulnerabilidades, mas também desenvolve uma cultura de segurança interna, essencial para enfrentar ameaças emergentes de forma eficaz.

Art 4.2.2 Quanto a **Execução das Ações** de Segurança da Informação:

Art 4.2.2.1 Da **Classificação da Informação**: As informações precisam ser identificadas e categorizadas de acordo com seu nível de confidencialidade, atribuindo um responsável por cada conjunto de dados, garantindo sua proteção adequada.

Art 4.2.2.2 Do **Controle de Acesso**: Envolve na implementação de políticas que regulam quem pode acessar informações e recursos organizacionais. Inclui processos de autenticação e autorização, seguindo o princípio do menor privilégio. O objetivo é garantir que apenas usuários autorizados tenham acesso a dados sensíveis, protegendo a integridade da informação.

Art 4.2.2.3 Da **Gerencia dos Ativos de TI**: Refere-se ao processo de identificar, catalogar e proteger os recursos tecnológicos da Secretaria Estadual de Saúde de Pernambuco, garantindo que sejam utilizados de forma eficiente e segura. Isso inclui a avaliação contínua dos ativos, a definição de responsabilidades e a implementação de medidas de segurança para mitigar riscos associados. Este gerenciamento eficaz dos ativos de TI é crucial para manter a integridade, disponibilidade e confidencialidade das informações da SES-PE.

Art 4.2.2.4 Da **Gestão dos Riscos de Segurança da Informação**: Envolve a identificação, avaliação e tratamento dos riscos associados à segurança das informações da Secretaria Estadual de Saúde de Pernambuco. Esse processo inclui a realização de análises de risco para determinar vulnerabilidades e ameaças. Estabelecendo medidas de mitigação e priorização de ações de acordo com a criticidade dos ativos. A gestão eficaz dos riscos é fundamental para garantir a integridade, disponibilidade e confidencialidade das informações, alinhando as práticas de segurança aos objetivos e requisitos legais da SES-PE.

Art 4.2.2.5 Do **Plano de Resposta e Tratamento dos Incidentes**: refere-se ao conjunto de práticas e procedimentos estabelecidos para identificar, analisar e remediar incidentes de segurança da informação. Isso inclui a criação de um plano de resposta a incidentes que define papéis e responsabilidades. A resposta eficaz aos incidentes visa minimizar danos, restaurar operações normais rapidamente e aprender com as ocorrências para melhorar continuamente as medidas de segurança e prevenção.

Art 4.2.2.6 Da **Conscientização e Treinamento dos Usuários** em Segurança da Informação: Envolve a implementação de programas educativos que visam informar os colaboradores sobre a importância da segurança da informação e as melhores práticas a serem seguidas.

Art 4.3 Do **Monitoramento das Medidas** de Segurança da Informação

Art 4.3.1 Serão conduzidas análises e revisões dos resultados obtidos, comparando-os com os objetivos previamente estabelecidos. Isso incluirá a coleta de dados, auditorias de conformidade e a verificação de logs de segurança, com o intuito de identificar quaisquer desvios ou falhas nas práticas de segurança adotadas. O feedback gerado é essencial para enfrentar novas e futuras ameaças e vulnerabilidades no ambiente digital da Secretaria Estadual de Saúde de Pernambuco.

Art 4.4 Das Estratégias para **Implementação da Melhoria Contínua** em Segurança da Informação

Art 4.4.1 Como parte do processo de melhoria contínua incluirá a reavaliação das metas de segurança da informação. Serão estabelecidos novos objetivos, alinhando as práticas de segurança às necessidades emergentes e ao cenário atual de ameaças, promovendo uma postura proativa na proteção de dados. Isso inclui: (Avaliação de Resultados, Ajustes nas Políticas e Procedimentos, Documentação das Mudanças, Revisão de Objetivos, Implementação de Novas Ações, Ciclo Contínuo de Melhoria).

Art. 5 Dos **Limites do SGSI**:

Art 5.1 Do **Escopo Organizacional**: Este SGSI aplica-se a todos os setores e unidades da SES-PE que lidam com informações sensíveis, incluindo dados de saúde dos cidadãos, registros administrativos e informações financeiras. Isso abrange tanto os sistemas digitais quanto os documentos físicos que contêm informações relevantes.

Art 5.2 Dos **Tipos de Informação**: Este SGSI abrange todas as categorias de dados que a SES-PE manipula, incluindo dados pessoais, informações de saúde, relatórios de serviços, protocolos de atendimento e qualquer outro tipo de informação que possa impactar a integridade e a confidencialidade dos dados.

Art 5.3 Dos **Ambientes de Operação**: Este SGSI é aplicável em todos os ambientes onde a SES-PE opera, incluindo instalações físicas, sistemas de informação em nuvem, e dispositivos móveis e computadores utilizados por colaboradores. Isso garante que a segurança da informação seja uma prioridade em todos os contextos.

Art 6 Da **Aplicabilidade do SGSI**:

Art 6.1 Dos **Colaboradores**: Esta Política de Segurança se aplica a todos os colaboradores da SES-PE, desde a alta administração até os funcionários de nível operacional. Além disso, deve incluir terceiros e parceiros que tenham acesso às informações da Secretaria, garantindo que todos estejam cientes de suas responsabilidades em relação à segurança da informação. É dever dos colaboradores proteger as informações sensíveis às quais têm acesso, evitando compartilhá-las indevidamente e utilizando senhas fortes e únicas para evitar acessos não autorizados. Os colaboradores devem estar atentos a possíveis incidentes de segurança e vulnerabilidades, reportando imediatamente qualquer suspeita à gestão, contribuindo para a proteção do ambiente organizacional e a rápida resposta a ameaças.

Art 6.2 Os gestores de cada unidade são responsáveis pela implementação e conformidade com a PSI em suas respectivas áreas, garantindo que todos os colaboradores de suas equipes conheçam e sigam as diretrizes estabelecidas.

Art 6.3 Da **Responsabilidade Individual e Coletiva**: Todos os colaboradores são responsáveis por conhecer e seguir as normas de proteção de dados, contribuindo para a defesa dos ativos da Secretaria Estadual de Saúde de Pernambuco. Proteger suas credenciais de acesso (senhas, tokens, etc.) contra uso não autorizado, verificar a identidade de remetentes e destinatários em comunicações eletrônicas, utilizar assinaturas digitais e outros mecanismos de autenticação quando necessário, reportar qualquer atividade suspeita que possa comprometer a autenticidade dos dados ou sistemas.

Art 6.3 Dos **Processos e Procedimentos**: Este SGSI deve ser integrado a todos os processos e procedimentos operacionais da SES-PE, garantindo que as práticas de segurança sejam incorporadas desde o planejamento até a execução das atividades. Isso inclui a realização de avaliações de risco, a implementação de controles de segurança e o plano de resposta a incidentes.

Art 7 Do **Comitê Gestor de Segurança da Informação**:

Art 7.1 O Comitê Gestor de Segurança da Informação será designado para supervisionar a implementação e manutenção da PSI, sendo responsável por avaliar continuamente as políticas e práticas de segurança implementadas, monitorando sua eficácia e propondo melhorias com base nos resultados obtidos e nas mudanças no ambiente de ameaças.

Art 7.2 O Comitê Gestor de Segurança da Informação tem a função de coordenar as ações de segurança da informação em toda a Secretaria Estadual de Saúde de Pernambuco, garantindo que todos os setores estejam alinhados com as diretrizes da Política de Segurança da Informação e que as responsabilidades sejam claramente definidas.

Art 7.3 O Comitê Gestor de Segurança da Informação deve estabelecer procedimentos para a gestão de incidentes de segurança, assegurando que haja um plano de resposta eficaz em caso de violações ou ameaças, além de promover a comunicação adequada sobre os incidentes a todos os envolvidos relevantes.

Art 8 Do **Tratamento de Informações e Dados**

Art 8.1 Toda informação e dados gerados, manipulados, armazenados, transportados, descartados ou sob custódia da Secretaria de Saúde do Estado de Pernambuco (SES) são de responsabilidade da instituição e devem ser geridos de forma adequada. É crucial que esses dados sejam classificados e tratados levando em consideração os princípios fundamentais de confidencialidade, integridade, autenticidade e disponibilidade. Além disso, a proteção de dados pessoais e a privacidade dos cidadãos devem ser garantidas, em conformidade com a legislação aplicável, especialmente a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI) (ACRESCENTAR A LGPD).

Art 8.2 Do **Armazenamento e Manuseio de Dados**: As informações e dados institucionais, quando em formato eletrônico, devem ser armazenados em servidores e bases de dados que estejam sob controle da SES. Para dados não eletrônicos, é fundamental que sejam mantidos em locais físicos adequados e seguros, prevenindo acessos indevidos. Toda informação e dado institucional em formato digital devem ser armazenados em servidores e ser protegidos por meio de cópias de segurança (backup) realizado pela equipe técnica responsável pela solução corporativa de backup da SES. Essas cópias devem ser realizadas em soluções que garantam a preservação e a recuperação dos dados quando necessário, seguindo normas e procedimentos específicos estabelecidos pela SES.

Art 8.3 Da **Proteção e Criptografia**: As informações e dados classificados, conforme a legislação vigente, que sejam produzidos, armazenados ou transportados em meio eletrônico, devem utilizar criptografia adequada ao respectivo grau de sigilo. Essa proteção é especialmente importante para dados sensíveis, incluindo informações de autenticação de usuários que acessam os sistemas administrados pela SES.

Art 8.4 Do **Descarte de Dados**: No processo de descarte de informações e dados institucionais, é imprescindível seguir as diretrizes de classificação, além de observar as políticas, normas e procedimentos internos que serão estabelecidos em regulamento próprio. Adicionalmente, é importante documentar de forma clara e detalhada todo o processo de descarte de informações, incluindo os responsáveis pela execução, as etapas envolvidas e as verificações realizadas para assegurar a conformidade com as diretrizes estabelecidas.

Art 8.5 Da **Classificação e Responsabilidades**: Ao classificar documentos e informações, todos os agentes responsáveis devem agir com critério, adotando como princípio orientador a garantia do direito fundamental de acesso à informação. A responsabilidade pela classificação correta das informações deve ser uma prioridade para todos os envolvidos, que deverão aplicar os procedimentos pertinentes conforme os critérios estabelecidos.

Art 8.5.1 Os usuários de informações, são responsáveis pela proteção da segurança e integridade dos dados em sua posse, devendo se familiarizar com as normas específicas da SES e com a legislação pertinente. Isso garante que as informações sejam geridas de maneira segura e responsável.

Art 8.6 Do **Gerenciamento de Ativos de Informação:** Um processo de inventário e mapeamento dos ativos de informação deve ser mantido e atualizado, visando garantir a segurança das infraestruturas críticas que suportam as informações e dados da Secretaria de Saúde do Estado de Pernambuco. Essa iniciativa permitirá identificar todos os ativos relevantes e criar uma base sólida para a gestão de riscos associados.

Art 8.7 Do **Controle de Acesso à Informação:** Com o objetivo de proteger dados sensíveis, cada usuário deverá possuir uma conta única e intransferível, garantindo uma identificação precisa. O acesso às informações será concedido com base na necessidade do trabalho, seguindo o princípio do menor privilégio, onde cada colaborador terá acesso apenas aos dados essenciais para suas funções.

Art 9 Da **Análise de Ameaças e Vulnerabilidades**

Art 9.1 A Análise de Ameaças e Vulnerabilidades consiste no processo sistemático de identificação, avaliação e documentação de possíveis ameaças que possam comprometer a confidencialidade, integridade e disponibilidade das informações, bem como das vulnerabilidades existentes nos ativos, sistemas, processos e infraestrutura da organização que possam ser exploradas por essas ameaças. Essa análise tem como objetivo antecipar riscos e subsidiar a adoção de controles preventivos, detectivos e corretivos, permitindo a mitigação de impactos potenciais e o fortalecimento da postura de segurança da informação da SES-PE. O

processo deve ser realizado periodicamente, ou sempre que houver mudanças significativas no ambiente tecnológico ou nos processos de negócio.

Art 10 Da **Avaliação de riscos**

Art 10.1 Analisar e priorizar riscos que possam comprometer a segurança da informação da organização. Os riscos e as estratégias de mitigação devem ser revisados periodicamente para garantir que continuem eficazes. Mudanças tecnológicas, novas ameaças e atualizações nos processos organizacionais devem ser incorporadas na avaliação de riscos de forma proativa.

Art 10.2 Do **Tratamento de Riscos**: O Tratamento de Riscos deve ser um processo contínuo e estratégico, garantindo a proteção da SES-PE frente a um cenário de ameaças em constante evolução. Após a implementação das ações de tratamento, é fundamental monitorar continuamente a eficácia das medidas aplicadas e revisar os riscos periodicamente.

Art 10.2 Da **Aceitação do Risco**: O risco pode ser aceito quando seu impacto é baixo ou quando o custo para mitigação é maior do que as perdas potenciais. Essa decisão deve ser documentada e aprovada pela gestão.

Art 10.3 Do **Transferência do Risco**: A SES-PE pode transferir a responsabilidade pelo risco para terceiros, quando previstos contratualmente, como prestadores de serviços especializados, seguradoras, terceirização de serviços de segurança gerenciada para monitoramento de ameaças e resposta a incidentes.

Art 10.4 Da **Eliminação do Risco**: É a ação de remover completamente uma ameaça ou vulnerabilidade de um ativo da informação, de modo que o risco associado deixe de existir. Trata-se da forma mais eficaz de tratamento de riscos, aplicada quando é possível descontinuar um processo, substituir uma tecnologia, ou modificar um ambiente de forma a eliminar a causa raiz do risco identificado. Essa abordagem deve ser considerada sempre que houver viabilidade técnica, operacional e legal para eliminar riscos que possam comprometer a confidencialidade, integridade e disponibilidade das informações sensíveis, especialmente aquelas relacionadas à saúde da população.

Art 10.5 Do **Plano de Ação e Implementação** da gestão de risco:

Para cada risco tratado, deve ser definido um plano de ação, incluindo:

a. Descrição do risco e sua classificação.
b. Medida de tratamento escolhida.
c. Responsáveis pela implementação.
d. Prazos para execução.
e. Indicadores para monitoramento da eficácia da medida adotada.

Art 11 Dos **Controles de Segurança** da Informação:

Art 11.1 Serão implementados controles de segurança baseados nas recomendações da ISO 27002, incluindo, mas não se limitando a:

Art 11.2 Esta política estabelece os controles de segurança da informação a serem implementados, alinhados com as recomendações da ISO 27002, para proteger os ativos de informação da SES-PE. Os controles abrangem as seguintes áreas fundamentais:

Art 11.3 Dos **Controle de Acesso Lógico e Físico**: Controles de acesso serão definidos no **ANEXO A** desta Política de Segurança da Informação (PSI). Isso garantirá que apenas usuários autorizados tenham acesso às informações e recursos críticos, utilizando mecanismos de autenticação adequados.

Art 11.4 Do **Gerenciamento de Ativos**: O gerenciamento de ativos, conforme descrito no **ANEXO B**, incluirá a identificação e a proteção dos principais ativos de informação, assegurando que cada ativo tenha um responsável designado e medidas de segurança apropriadas.

Art 11.5 Da **Criptografia e Proteção de Dados**: Está definido no **ANEXO C**, diretrizes sobre criptografia e proteção de dados aplicadas para proteger dados sensíveis em repouso e em trânsito, assegurando a confidencialidade e integridade das informações.

Art 11.6 Do **Plano de Resposta a Incidentes de Segurança da Informação**: Está definido no **ANEXO D** os procedimentos para o plano de resposta a incidentes de segurança, permitindo a identificação e resposta a eventos de segurança de forma estruturada. Isso inclui a documentação e análise de todos os incidentes para promover melhorias contínuas, contém um plano de resposta a incidentes de SI.

Art 11.7 Das **Políticas de Senhas e Controle de Alterações**: Está definido no **ANEXO E** , em conformidade com as melhores práticas de segurança, serão implementadas políticas de senhas que exigem (comprimento mínimo, combinação de caracteres, etc.)

Art 11.8 Do **Controle de Backup**: Está definido no **ANEXO F**, um plano de controle de backup estabelecido para garantir que dados críticos sejam copiados regularmente e possam ser restaurados em caso de perda.

Art 11.9 Do **Controle de Publicações de Sistema para Produção**: Está definido no **ANEXO G** os procedimentos para o controle de publicações de sistema em produção, garantindo que todas as atualizações e alterações sejam revisadas, testadas e aprovadas antes da implementação.

Art. 11.10 Da Classificação e Rotulagem da Informação: Está definido no **ANEXO H** a Política de **Classificação, Rotulagem e Manuseio da Informação** da SES-PE, estabelecendo **níveis de classificação** (Pública, Interna, Confidencial e Sigilosa), **critérios de enquadramento**, **rótulos padronizados** e **regras de manuseio e descarte** por nível. O **ANEXO H** integra-se aos demais anexos para garantir **controles proporcionais ao nível da informação**, incluindo **controle de acesso (ANEXO A)**, **gerenciamento de ativos (ANEXO**

B), **criptografia e proteção de dados (ANEXO C)**, **resposta a incidentes (ANEXO D)**, **políticas de senhas e controle de alterações (ANEXO E)**, **backup (ANEXO F)** e **controle de publicações em produção (ANEXO G)**.

Art 12 Da **Conformidade Legal e Regulatória**

Art 12.1 A SES compromete-se a cumprir todas as leis e regulamentações aplicáveis relacionadas à segurança da informação.

Art 13 Da **Comunicação e Conscientização**

Art 13.1 Será promovida a conscientização sobre segurança da informação entre os colaboradores, e qualquer violação ou incidente de segurança será comunicado e tratado de acordo com os procedimentos estabelecidos.

Art 14 Da Revisão da Política

Art 14.1 Esta política será revisada periodicamente para garantir sua relevância e eficácia contínua, com atualizações conforme necessário. A SES está comprometida em manter e melhorar continuamente a segurança da informação para proteger os ativos e interesses da secretaria.

Art 15 Da aplicação da Política de Segurança da Informação:

Art 15.1 Esta Política de Segurança da Informação entra em vigor imediatamente após a sua aprovação pela alta direção da SES.

Zilda do Rêgo Cavalcanti
Secretária Estadual de Saúde