PORTARIA IEC DE 16 DE DEZEMBRO DE 2025

Aprova a Política de Segurança da Informação do Instituto Evandro Chagas (IEC).

O Diretor Substituto do Instituto Evandro Chagas, da Secretaria de Vigilância em Saúde e Ambiente do Ministério da Saúde, designada mediante Apostila/SAA/SE/MS, de 18 de junho de 2024, publicada no Boletim de Serviço Eletrônico do Ministério da Saúde, Edição Extraordinária nº 69 de 19 de junho de 2024, no uso das competências que lhe foram atribuídas pela Portaria nº 1.041, de 30.10.09, publicada no DOU de 03.11.2009, resolve:

N.º 225- Art. 1º - Fica aprovada a Política de Segurança da Informação do Instituto Evandro Chagas (IEC), na forma do Anexo.
Art. 2º. Esta Portaria entra em vigor na data de sua publicação.

BRUNO SANTANA CARNEIRO

ANEXO
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO INSTITUTO EVANDRO CHAGAS (IEC)

CAPÍTULO I - Disposições Gerais

Art. 1º. Fica instituída a Política de Segurança da Informação do Instituto Evandro Chagas (IEC), com a finalidade de estabelecer princípios, diretrizes, responsabilidades e competências para a gestão da segurança da informação.

Art. 2º. Esta Política de Segurança da Informação aplica-se a todas as unidades organizacionais do IEC, e deverá ser observada por todos os usuários de informação, seja servidor ou equiparado, empregado, prestador de serviços ou pessoa habilitada pela administração, por meio da assinatura de Termo de Responsabilidade, para acessar os ativos de informação sob responsabilidade deste órgão.

Art. 3º. São objetivos da Política de Segurança da Informação:

I- estabelecer princípios e diretrizes a fim de proteger ativos de informação e conhecimentos gerados ou recebidos;

II - estabelecer orientações gerais de segurança da informação e, desta forma, contribuir para a gestão eficiente dos riscos, limitando-os a níveis aceitáveis, bem como preservar os princípios da disponibilidade, integridade, confiabilidade e autenticidade das informações;

III - estabelecer competências e responsabilidades quanto à segurança da informação;

IV - nortear a elaboração das normas necessárias à efetiva implementação da segurança da informação;

V - adequar as ações de segurança da informação às estratégias de planejamento organizacional do IEC;

VI - promover o alinhamento das ações institucionais às normas contidas na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), e seus respectivos regulamentos, notadamente o Decreto nº 12.572, de 4 de agosto de 2025, que institui a Política Nacional de Segurança da Informação.

Art. 4º. Para os fins desta Política, considera-se:

I – dado pessoal: informação relacionada à pessoa natural identificada ou identificável;

II – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III – informação: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

IV – ativos de informação: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

V – disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

VI – integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

VII – confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;

VIII – autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

IX – usuário de informação: pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da administração pública federal, formalizada por meio da assinatura de Termo de Responsabilidade;

X – gestão de segurança da informação: processo que visa integrar atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e organizacional, aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação; e

XI – incidente: interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.

Parágrafo único. Aplicam-se a esta Política os termos do Glossário de Segurança da Informação, aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021, ou outros que venham a substituí-lo.

CAPÍTULO II - Dos Princípios e Diretrizes

Art. 5º. As ações de segurança da informação do IEC são norteadas pelos princípios constitucionais e administrativos que norteiam a Administração Pública Federal, bem como pelos seguintes:

I - disponibilidade, integridade, confidencialidade e autenticidade das informações;

II - continuidade dos processos e serviços essenciais para o funcionamento do IEC;

III - economicidade da proteção dos ativos de informação;

IV - respeito ao acesso à informação, à proteção de dados pessoais e à proteção da privacidade;

V - observância da publicidade como preceito geral e do sigilo como exceção;

VI - responsabilidade do usuário de informação pelos atos que comprometam a segurança dos ativos de informação;

VII - alinhamento estratégico da Política de Segurança da Informação com o planejamento estratégico do IEC, assim como demais normas específicas de segurança da informação da Administração Pública Federal;

VIII - conformidade das normas e das ações de segurança da informação com a legislação regulamentos aplicáveis; e

IX - educação e comunicação como alicerces fundamentais para o fomento da cultura e segurança da informação.

Art. 6º. Estas diretrizes constituem os principais pilares da gestão de segurança da informação norteando a elaboração de políticas, planos e normas complementares no âmbito deste Instituto e objetivam a garantia dos princípios básicos de segurança da informação estabelecidos nesta Política.

Art. 7º. As normas, procedimentos, manuais e metodologias de segurança da informação do IEC devem considerar, como referência, além dos normativos vigentes, as melhores práticas de segurança da informação.

Art. 8º. As ações de segurança da informação devem:

I - considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, a estrutura e a finalidade do IEC;

II - ser tratadas de forma integrada, respeitando as especificidades e a autonomia das unidades do IEC;

III - ser adotadas proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente, o valor e a criticidade da informação;

IV - visar à prevenção da ocorrência de incidentes.

Art. 9º. O investimento necessário em medidas de segurança da informação deve ser dimensionado segundo o valor do ativo a ser protegido e de acordo com o risco de potenciais prejuízos ao IEC.
Art. 10. Toda e qualquer informação gerada, custodiada, manipulada, utilizada ou armazenada no IEC compõe o seu rol de ativos de informação e deve ser protegida conforme as normas em vigor.
Parágrafo único. As informações citadas no caput, que tramitem pelo ambiente computacional do IEC, são passíveis de monitoramento e auditoria, respeitados os limites legais.
Art. 11. Pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.
Parágrafo único. É condição para acesso aos recursos de tecnologia da informação do IEC a assinatura, preferencialmente eletrônica, de Termo de Responsabilidade indicando a ciência aos termos desta Política, as responsabilidades e os compromissos em decorrência deste acesso, bem como as penalidades cabíveis pela inobservância das regras previstas nas normas de segurança da informação.
Art. 12. A Política de Segurança da Informação e suas atualizações, bem como normas específicas de segurança da informação do IEC, devem ser divulgadas amplamente a todos os Usuários de Informação, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.
§ 1º Os Usuários de Informação devem ser continuamente capacitados nos procedimentos de segurança e no uso correto dos ativos de informação quando da realização de suas atribuições, de modo a minimizar possíveis riscos à segurança da informação.
§ 2º As ações de capacitação previstas no § 1º devem ser conduzidas de modo a possibilitar o compartilhamento de materiais educacionais sobre segurança da informação.
Art. 13. Todos os contratos de prestação de serviços firmados pelo IEC conterão cláusula específica sobre a obrigatoriedade de atendimento a esta Política de Segurança da Informação, bem como normas correlatas.
CAPÍTULO III - Da Gestão de Segurança da Informação
Art. 14. A Gestão da Segurança da Informação é constituída, no mínimo, pelos seguintes processos:
I - tratamento da informação;
II - segurança física e do ambiente;
III - gestão de incidentes em segurança da informação;
IV - gestão de ativos;
V - gestão do uso dos recursos operacionais e de comunicações, tais como e-mail, acesso à internet, mídias sociais e computação em nuvem;
VI - controles de acesso;
VII - gestão de riscos;
VIII - gestão de continuidade;
IX - auditoria e conformidade.
§ 1º O IEC poderá definir outros processos de Gestão de Segurança da Informação, desde que alinhados aos princípios e às diretrizes desta Política e destinados à implementação de ações de segurança da informação.
§ 2º Para cada um dos processos que constituem a Gestão de Segurança da Informação, deve ser observada a pertinência de elaboração de políticas, normas, procedimentos, orientações ou manuais que disciplinem ou facilitem o seu entendimento, em conformidade com a legislação vigente e boas práticas de segurança de informação.
§ 3º As unidades organizacionais do IEC devem realizar periodicamente auditorias internas de sua segurança da informação para assegurar que ela esteja em conformidade com esta Política e com outros requisitos de segurança da informação aplicáveis.
§ 4º Todas as ações, realizadas pelas unidades do IEC, que envolvem a segurança da informação devem estar em conformidade com as leis e regulamentos aplicáveis a esta temática.
§ 5º As atividades, produtos e serviços desenvolvidos no IEC devem estar em conformidade com requisitos de privacidade e proteção de dados pessoais constantes de leis, regulamentos, resoluções, normas, estatutos e contratos jurídicos vigentes
Art. 15. A Política de Segurança da Informação e demais normas correlatas integram o arcabouço normativo da Gestão de Segurança da Informação.
Art. 16. A estrutura de Gestão de Segurança da Informação é composta por:
I - Alta Administração;
II - Comitê de Segurança da Informação;
III - Gestor de Segurança da Informação;
IV - Gestor de Tecnologia da Informação e Comunicação;
V - Encarregado pelo Tratamento de Dados Pessoais;
VI - Seção de Transparência e Conformidade Normativa (SETCN);
VII - Setor de Tecnologia da Informação e Comunicação (SETIC); e
VIII - Usuários de Informação.
Art. 17. Compete à Alta Administração:
I - fornecer os recursos necessários para assegurar o desenvolvimento e a implementação da Gestão de Segurança da Informação do IEC, bem como com o tratamento das ações e decisões de segurança da informação em um nível de relevância e prioridade adequados; e
II - formalizar e aprovar a Política de Segurança da Informação do IEC, bem como suas alterações e atualizações.
Art. 18. Compete ao Comitê de Segurança da Informação:
I - assessorar na implementação das ações de segurança da informação;
II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;
III - participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação;
IV - propor alterações à Política de Segurança da Informação e às normas internas de segurança da informação;
V - deliberar sobre normas internas de segurança da informação;
VI - avaliar as ações propostas pelo gestor de segurança da informação.
Parágrafo único. A composição, estrutura, recursos e funcionamento do Comitê de Segurança da Informação será definido em ato administrativo próprio, de acordo com a legislação vigente.
Art. 19. Compete ao Gestor de Segurança da Informação:
I - coordenar o Comitê de Segurança da Informação;
II - coordenar a elaboração da Política de Segurança da Informação e das normas internas de segurança da informação do órgão, observadas a legislação vigente e as melhores práticas sobre o tema;
III - assessorar a Alta Administração na implementação da Política de Segurança da Informação;
IV - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;
V - promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão;
VI - incentivar estudos de novas tecnologias, e seus eventuais impactos relacionados à segurança da informação;
VII - propor recursos necessários às ações de segurança da informação;
VIII - acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;
IX - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;
X - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação;
XI - manter contato direto com as autoridades competentes em assuntos relativos à segurança da informação.
Parágrafo único. O Gestor de Segurança da Informação do IEC será designado em ato administrativo próprio, de acordo com a legislação vigente.
Art. 20. Compete ao Gestor de Tecnologia da Informação e Comunicação, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Portaria SGD/ME nº 778, de 4 de abril de 2019, planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, considerando a cadeia de suprimentos relacionada à solução.
Art. 21. Compete ao Encarregado pelo Tratamento dos Dados Pessoais, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Lei nº

13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD) e demais normativos e orientações emitidas pela Autoridade Nacional de Proteção de Dados (ANPD), conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis.
Art. 22. Compete à SETCN, dentre outras atribuições dispostas na legislação vigente, apoiar, supervisionar e monitorar as atividades desenvolvidas pela primeira linha de defesa prevista pela Instrução Normativa CGU nº 3, de 9 de junho de 2017, ou por outras normas que venham a substitui-la.
Art. 23. Compete ao SETIC:
I - facilitar, coordenar e executar as atividades de prevenção, tratamento e resposta a incidentes cibernéticos no IEC;
II - monitorar as redes computacionais;
III - detectar e analisar ataques e intrusões;
IV - tratar incidentes de segurança da informação;
V - identificar vulnerabilidades e artefatos maliciosos;
VI - recuperar sistemas de informação;
VII - promover a cooperação com outras equipes, e participar de fóruns e redes relativas à segurança da informação.
Art. 24. Compete aos Usuários de Informação conhecer, cumprir e fazer cumprir as normas contidas nesta Política, bem como outras normas correlatas.
Parágrafo único. Todos os Usuários de Informação são responsáveis pela segurança dos ativos de informação que estejam sob a sua responsabilidade.
CAPÍTULO IV - Das Vedações e Disposições Finais
Art. 25. É vedada a utilização dos recursos de tecnologia da informação disponibilizados pelo IEC para acesso, guarda e divulgação de material incompatível com ambiente do serviço, que viole direitos autorais ou que infrinja a legislação vigente.
Art. 26. São vedados o uso e a instalação de recursos de tecnologia da informação que não tenham sido homologados ou adquiridos pelo IEC.
Art. 27. É vedada a divulgação a terceiros de mecanismos de identificação, autenticação e autorização baseados em conta e senha ou certificação digital, de uso pessoal e intransferível, que são fornecidos aos usuários.
Art. 28. É vedada a exploração de eventuais vulnerabilidades, as quais devem ser comunicadas às instâncias superiores assim que identificadas.
Art. 29. A unidades organizacionais do IEC devem promover ações de treinamento e conscientização para que os seus colaboradores entendam suas responsabilidades e procedimentos voltados à segurança da informação e à proteção de dados.
Parágrafo único. A conscientização, a capacitação e a sensibilização em segurança da informação devem ser adequadas aos papéis e responsabilidades dos colaboradores.
Art. 30. As denúncias de violação a esta Política podem ser comunicadas ao Gestor de Segurança da Informação.
Art. 31. O cumprimento desta Política, bem como dos normativos que a complementam devem ser avaliados periodicamente por meio de verificações de conformidade, buscando a certificação do cumprimento dos requisitos de segurança da informação e da garantia de cláusula de responsabilidade e sigilo constantes de termos de responsabilidade, contratos, convênios, acordos e instrumentos congêneres.
Art. 32. A não observância do disposto nesta Política, bem como em seus instrumentos normativos correlatos, sujeita o infrator à aplicação de sanções administrativas conforme a legislação vigente, sem prejuízo das responsabilidades penal e civil, assegurados sempre aos envolvidos o contraditório e a ampla defesa.
Art. 33. Esta Política será revisada periodicamente, para refletir as mudanças no ambiente do IEC, nos riscos à segurança da informação e nas melhores práticas de segurança da informação.
Art. 34. Os casos omissos e as dúvidas sobre a Política de Segurança da Informação e seus documentos devem ser submetidas à Alta Administração, que decidirá com o auxílio do Comitê de Segurança da Informação.
Art. 35. Esta Política entra em vigor na data da sua publicação.

SECRETARIA DE SAÚDE INDÍGENA

DISTRITOS SANITÁRIOS ESPECIAIS INDÍGENAS

Alagoas e Sergipe

PORTARIA DSEI/ALSE DE 09 DE OUTUBRO DE 2025

O Coordenador Distrital da Saúde Indígena do DSEI Alagoas e Sergipe, no uso de suas atribuições conferidas pela portaria nº 403 de 09 de março de 2023, publicada no Diário Oficial da União de 03 de abril de 2023, resolve:

Nº 125 Designar os servidores abaixo indicados, com observância à legislação vigente, para atuarem como fiscais das Atas de Registro de Preços n° 52/2025, nº 53/2025, nº 54/2025, nº 57/2025, nº 58/2025, nº 59/2025, nº 60/2025, nº 61/2025, 73/2025, 74/2025, nº 80/2025, nº 81/2025 e nº 82/2025, cujo o objeto é o registro de preços para aquisição de materiais médico-hospitalares destinados ao abastecimento de todas as unidades básicas de saúde indígena (UBSI) e polo Base de abrangência do Distrito Sanitário Especial Indígena de Alagoas e Sergipe, referente a Licitação nº 90011/2025, que integra estas Atas, bem como as propostas cujos preços tenham sido registrados, independentemente de transcrição, firmadas entre o DSEI/ALSE e as empresas constantes nas referidas Atas. (Processo SEI nº 25034.000342/2025-20).
TITULAR
Tamara Rita Freitas Sobral– SIAPE 1225897
SUBSTITUTO
Fábio Roberto dos Anjos– SIAPE 1100966
Art.2º Esta portaria entra em vigor na data de sua publicação”

PORTARIA DSEI/ALSE DE 11 DE DEZEMBRO DE 2025

O Coordenador Distrital da Saúde Indígena do DSEI Alagoas e Sergipe, no uso de suas atribuições conferidas pela portaria nº 403 de 09 de março de 2023, publicada no Diário Oficial da União de 03 de abril de 2023, resolve:

Nº 124 Designar os servidores abaixo indicados, com observância da legislação vigente, para atuarem como fiscais das ATAS DE REGISTRO DE PREÇO nº 62/2025, 63/2025, 64/2025, 65/2025, 66/2025, 67/2025, 68/2025, 69/2025, 70/2025, 71/2025 e 72/2025 do Processo Administrativo nº 25034.001009/2024-57, cujo o objeto do presente instrumento é aquisição de materiais destinados à desenvolver as ações dos programas de atendimento (triagem e consultas), vacinação, educação em saúde e recreação infantil da Divisão de Atenção a Saúde Indígena – DIASI, decorrente do Pregão Eletrônico nº 90006/2025, firmado entre o DSEI/ALSE e as Empresas: AUTOMX SOLUÇÕES LTDA, CENTRAL HOLDING LOGÍSTICA LTDA, EQUIMED EQUIPAMENTOS MÉDICOS HOSPITALARES LTDA, FOCCUS DISTRIBUIDORA DE EQUIPAMENTOS LTDA, HUBNET E-COMMERCE LTDA, ONIX COMÉRCIO DE PRODUTOS ODONTOLÓGICOS LTDA, SETEFARMA INDÚSTRIA, COMÉRCIO, IMPORTAÇÃO E EXPORTAÇÃO DE PRODUTOS PARA SAÚDE LTDA, THAINA BETANIA BARBOSA DE AZEVEDO, UNITY INSTRUMENTOS DE TESTES E MEDIÇÃO LTDA, VALTARE SOLUÇÕES EMPRESARIAIS E COMÉRCIO e SIS COMÉRCIO DE MATERIAIS E EQUIPAMENTOS LTDA (Processo SEI nº 25034.001009/2024-57).
TITULAR
Tamara Rita de Freitas Sobral - SIAPE 1225897
SUBSTITUTO
Fábio Roberto dos Anjos - SIAPE 1100966
Art.2º Esta portaria entra em vigor na data de sua publicação”