POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO DO HOSPITAL DE CLÍNICAS DE ITAJUBÁ (POSIC-HCI)

Código: LGPD-POL-0001 **Versão:**1

1. OBJETIVO

A Política de Segurança da Informação e Comunicações (POSIC) tem por objetivo a instituição de diretrizes estratégicas que visam garantir a disponibilidade, integridade, confidencialidade e a autenticidade dos dados, informações, documentos e conhecimentos produzidos, armazenados ou transmitidos por qualquer meio dos sistemas de informação do Hospital de Clínicas de Itajubá (HCI) contra ameaças e vulnerabilidades, de modo a preservar os seus ativos de informação, inclusive a sua imagem institucional.

Seu propósito é direcionar as ações do HCI à gestão de riscos e ao tratamento de incidentes de Segurança da Informação e Comunicações (SIC), alinhadas e em conformidade com a Política de Segurança da Informação e Comunicações (POSIC) e com a legislação aplicável (Lei Geral de Proteção de Dados Pessoais).

1.1 ABRANGÊNCIA

O conhecimento desta POSIC aplica-se ao HCI, sendo de responsabilidade de todos os servidores, empregados, colaboradores internos ou externos, bem como a todas as pessoas ou organizações que utilizam os meios físicos ou lógicos do HCI. Todos esses atores são responsáveis por garantir a segurança das informações a que tenham acesso.

2. CONCEITOS E DEFINIÇÕES

Para os efeitos desta POSIC são estabelecidos os seguintes conceitos e definições:

- Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a acessibilidade de usar os ativos de informação de um órgão ou entidade;
- Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
- Análise de riscos: uso sistemático de informações para identificar fontes e estimar o risco;
- Atividade: processo ou conjunto de processos executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;
- Ativo: qualquer componente (seja humano, tecnológico, software ou outros) que sustente uma ou mais atividades e que tenha ou gere valor para a organização;
- Ativos de Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;
- Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;
- Avaliação de riscos: processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco; Celeridade: as ações de segurança da informação e comunicações devem oferecer respostas rápidas a incidentes e falhas;
- Classificação da informação: identificação de quais são os níveis de proteção que as informações demandam e estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas;

- Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade autorizados;
- Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;
- Custodiante do ativo de informação: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia;
- Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;
- Ética: os direitos dos agentes públicos devem ser preservados sem comprometimento da Segurança da Informação e Comunicações;
- Evento de segurança da informação: ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da política de segurança da informação, ou falta de controle, ou situação previamente desconhecida que possa ser relevante para a segurança da informação;
- Gerenciamento de ativos: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles desses ativos;
- Gerenciamento de Riscos de Segurança da Informação e Comunicações: conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;
- Gestão de segurança da informação e comunicações: ações e métodos que visam à integração das 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 segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, no âmbito da tecnologia da informação e comunicações;
- Incidente de SIC: evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período inferior ao tempo objetivo de recuperação;
- Informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;
- Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- Política de Segurança da Informação e Comunicações: documento aprovado pela autoridade responsável do órgão ou entidade da Administração Pública Federal, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações; Proprietário de ativos de informação: unidade administrativa responsável por gerenciar determinado segmento de informação e todos os ativos relacionados;
- Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;
- Resiliência: poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre;
- Responsabilidade: os agentes públicos devem conhecer e respeitar todas as normas de segurança da informação e comunicações da instituição;
- Risco de SIC: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;
- Terceiros: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos ao HCI;
- Tratamento de incidentes: é o processo que consiste em receber, filtrar, classificar e responder às solicitações e alertas; e realizar as prováveis correções dos incidentes de segurança, procurando

extrair informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências;

- Usuário: qualquer pessoa que obteve autorização do responsável pela área interessada para acesso aos ativos de Informação;
- Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

3. REFERENCIAS NORMATIVAS

Esta POSIC está em conformidade com a legislação aplicável, regimento interno do HCI e estatuto da AISI, bem como demais documentos institucionais e aplica-se no âmbito do HCI, mantido pela AISI.

4. PRINCÍPIOS

Esta POSIC e suas ações serão norteadas pelos seguintes princípios, assim definidos:

- Celeridade: As ações de SIC devem oferecer respostas rápidas à incidentes e falhas de segurança;
- Ética: Os direitos e interesses legítimos dos usuários e agentes públicos devem ser preservados, sem comprometimento da SIC;
- Clareza: As regras de segurança dos ativos de segurança da informação e comunicações devem ser precisas, concisas e de fácil entendimento;
- Legalidade: As ações de segurança devem respeitar as atribuições regimentais, bem como as leis, normas e políticas organizacionais, administrativas, técnicas e operacionais do HCI-AISI;
- Publicidade: Transparência no trato da informação, observados os critérios legais.

5. DIRETRIZES LEGAIS:

As diretrizes de segurança da informação estabelecidas nesta POSIC aplicam-se às informações armazenadas, acessadas, produzidas e transmitidas pelo HCI, e que devem ser seguidas pelos usuários, incumbindo a todos a responsabilidade e o comprometimento com sua aplicação.

Seja qual for a forma ou o meio pelo qual a informação seja apresentada ou compartilhada, será sempre protegida adequadamente, de acordo com esta política. Os recursos de Tecnologia da Informação e Comunicação (TIC) disponibilizados pelo HCI serão utilizados estritamente para seu propósito. É vedado, a qualquer usuário do HCI, o uso dos recursos de TIC para fins pessoais (próprios ou de terceiros), entretenimento, veiculação de opiniões político-partidárias ou religiosas, bem como para perpetrar ações que, de qualquer modo, possam constranger, assediar, ofender, caluniar, ameaçar, violar direito autoral ou causar prejuízos a qualquer pessoa física ou jurídica, assim como aquelas que atentem contra a moral e a ética ou que prejudiquem o cidadão ou a imagem da instituição, comprometendo a integridade, a confidencialidade, a confiabilidade, autenticidade ou a disponibilidade das informações.

As diretrizes desta POSIC constituem os principais pilares da Gestão de Segurança da Informação, norteando a elaboração de todos os documentos necessários para guarnecer o sigilo e a segurança exigida. Os casos omissos e as dúvidas surgidas na aplicação do disposto nesta POSIC, devem ser direcionados ao Comitê de Segurança da Informação do Hospital de Clínicas de Itajubá (CSI-HCI).

6. DIRETRIZES ESPECÍFICAS:

6.1 Comitê de Segurança da Informação do Hospital de Clínicas de Itajubá – CSI-HCI.

Deve ser formalmente constituído por colaboradores nomeados pela Diretoria Geral, em conjunto com a Coordenadoria e Encarregado de Dados do HCI. O CSI deverá reunir-se mensalmente. Reuniões extras devem ser realizadas sempre que for necessário, para deliberar sobre algum incidente grave ou definição relevante para o HCI. O CSI poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico.

7. COMPETÊNCIAS DE RESPONSABILIDADES:

Diretoria Geral do HCI:

- Promover a cultura de segurança da informação e comunicações;
- Aprovar a Política de Segurança da Informação e Comunicações (POSIC);
- Nomear o Comitê de Segurança da Informação do Hospital de Clínicas de Itajubá (CSI-HCI).

Comitê de Segurança da Informação do Hospital de Clínicas de Itajubá:

- Promover a cultura de SIC;
- Elaborar, avaliar, revisar e analisar criticamente a POSIC e suas normas complementares, visando a sua aderência aos objetivos institucionais do HCI e às legislações vigentes;
- Coordenar as ações de segurança da informação e comunicações;
- Aprovar a abertura de processo administrativo mediante constatação de quebra de segurança da informação;
- Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança e submeter à Diretoria Geral do HCI os resultados consolidados de tais investigações e avaliações;
- Propor recursos necessários às ações de Segurança da Informação e Comunicações;
- Realizar e acompanhar estudos de novas tecnologias, quanto aos possíveis impactos na segurança da informação e comunicações;
- Propor e atualizar normas relativas à Segurança da Informação e Comunicações;
- Prover os meios necessários para capacitação, o aperfeiçoamento técnico dos usuários do HCI, bem como prover a infraestrutura necessária para o seu funcionamento;
- Divulgar no âmbito do HCI essa POSIC.

Proprietário de Ativos de Informação:

- Proteger e manter os ativos de informação;
- Seguir os requisitos de segurança para os ativos de informação sob sua responsabilidade em conformidade com essa POSIC;
- Garantir a segurança dos ativos de informação sob sua responsabilidade através de monitoramento contínuo;
- Comunicar as exigências de SIC a todos os usuários sob sua responsabilidade;
- Conceder e revogar acessos aos ativos de informação;
- Comunicar ao superior ou ao CSI-HCI a ocorrência de incidentes de SIC; e
- Designar custodiante dos ativos de informação, quando aplicável.

Custodiante dos Ativos de Informação:

- Proteger e manter os ativos de informação;
- Controlar o acesso, conforme requisitos definidos pelo proprietário da informação e em conformidade com essa POSIC.

- Seguir os requisitos de segurança para os ativos de informação sob sua responsabilidade em conformidade com essa POSIC.

Terceiros e Fornecedores:

- Tomar conhecimento dessa POSIC;
- Fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato; e
- Fornecer toda a documentação dos sistemas, produtos e serviços relacionados às suas atividades.

Usuários:

- Proteger e manter os ativos de informação sob sua responsabilidade;
- Conhecer e cumprir essa POSIC;
- Assinar o "Termo de compromisso junto ao RH e TI do HCI";
- Comunicar os incidentes que afetam à segurança dos ativos de informação e comunicações ao superior ou responsável imediato.

8. MÉTODOS COMPULSÓRIOS

Gerenciamento de Segurança da Informação e Comunicações:

Todos os mecanismos de proteção utilizados para a SIC devem ser mantidos com o objetivo de garantir a continuidade das atividades hospitalares. As medidas de proteção devem ser planejadas e os gastos da aplicação de controles devem ser compatíveis com o valor do ativo protegido. Os requisitos de proteção de dados pessoais devem ser explicitamente citados em todos os termos celebrados entre a instituição e terceiros, através de cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta política, da política de privacidade e demais deliberações do Comitê de Segurança da Informação.

Gerenciamento de Riscos de Segurança da Informação e Comunicações:

O GRSIC é um conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos. Qualquer instância administrativa, assistencial ou técnica do HCI torna-se uma área responsável por ativos de informação. A GRSIC deve ser realizado no âmbito do HCI, visando identificar os ativos relevantes e determinar ações de gestão apropriadas, e deve ser atualizado periodicamente, ou tempestivamente, em função de inventários de ativos, de mudanças, ameaças ou vulnerabilidades.

Tratamento da Informação:

- A informação deve ser protegida de forma preventiva, com o objetivo de minimizar riscos às atividades e serviços do HCI.
- Os dados, as informações e os sistemas de informação do HCI devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a disponibilidade, integridade, confidencialidade e autenticidade desses bens.
  A informação deve ser protegida de acordo com o seu valor, sensibilidade e criticidade classificando a informação.

Contratos, Convênios, Acordos e Instrumentos Congêneres:

Todos os contratos, convênios, acordos e instrumentos congêneres deverão conter cláusulas que estabeleçam a obrigatoriedade de observância desta POSIC e da LGPD. O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar essa POSIC e suas normas complementares aos empregados, prepostos e todos os envolvidos em atividades vinculadas ao HCI.

9. DIVULGAÇÃO E CONSCIENTIZAÇÃO

- A divulgação das regras e orientações de segurança aplicadas aos usuários deve ser objeto de campanhas internas permanentes, disponibilização integral e contínua nas redes internas e sociais, seminários de conscientização e quaisquer outros meios, como forma de ser criada uma cultura de segurança da informação no âmbito do HCI.
- Cabe ao CSI-HCI providenciar a divulgação interna dessa POSIC e das normas, inclusive com publicação permanente na página do HCI, para que seu conteúdo possa ser consultado a qualquer momento e desenvolver processo permanente de divulgação, sensibilização, conscientização e capacitação dos usuários sobre os cuidados e deveres relacionados à SIC.

10. ATUALIZAÇÃO

A segurança da informação e comunicações, seja ela digital ou física, é tema de permanente acompanhamento e aperfeiçoamento, devendo ser constantemente revista e atualizada, visando à melhoria contínua da qualidade dos processos internos. Quaisquer complementações ou alterações necessárias, de acordo com nuances e mudanças de processos, deverá passar pelo Comitê de Segurança da Informação, objetivando a validação. Os instrumentos normativos gerados a partir dessa POSIC deverão ser revisados sempre que se fizer necessário, em função de alterações na legislação pertinente ou de diretrizes políticas e normativas legais.

SITUAÇÃO	NOME	CARGO/SETOR	DATA DE APROVAÇÃO
Elaboração	Paulo Henrique C. Teixeira	Juridico/ Encarregado de Dados	02/06/2023
Consenso	Dr. Seleno Glauber de Jesus Marcela Rodrigues S. Prado Micaela de O. P. Cavalheiro Paula Gonçalves Ribeiro Luiz André da Silva Campos Maiza Marcelino da Silva Marcelo Pereira de Oliveira Antônio Carlos de Alagão Andreia Cristina dos Passos Leandro dos Santos Lima Dr. Kleber Lincoln Gomes	Coordenador Feral da Residência Médica, Estágios Coordenador Médico do centro Cirúrgico-CME e Vice-diretor Técnico Gerente de Assistencial Gerente de RH Gerente do faturamento e Gestão de Leitos Controladoria Gerente Qualidade/ Hospitalidade Gerente de TI Diretor Clínico Supervisora da Farmácia Gerente Gestão ADM Presidente AISI	05/05/2023
Aprovador final	Dr. Rodolfo S, Cardoso	Diretor Geral HCI	06/06/2023