
# Política de Segurança da Informação e Comunicações (POSIC)

**1ª versão**

**2024**

# SUMÁRIO

## 1. ESCOPO

### 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, autenticidade, bem como atitudes adequadas para manuseio, tratamento, controle e proteção dos dados, informações, documentos e conhecimentos produzidos, armazenados, sob guarda ou transmitidos por qualquer meio ou recurso do Hospital da Criança contra ameaças e vulnerabilidades. Desse modo, a política também busca preservar os seus ativos de informação, inclusive a sua imagem institucional.

Seu propósito é direcionar o Hospital da Criança no que diz respeito à gestão de riscos e ao tratamento de incidentes de Segurança da Informação e Comunicações (SIC), em conformidade com as disposições constitucionais, legais e regimentais vigentes.

A POSIC estabelece o comprometimento da alta direção organizacional do hospital, com vistas a prover apoio para a implantação da Gestão dos Riscos de Segurança da Informação e Comunicações (GRSIC).

### 1.2. ABRANGÊNCIA

Esta POSIC aplica-se ao Hospital da Criança, sendo de responsabilidade de todos os funcionários, colaboradores internos ou externos, bem como a todas as pessoas ou organizações que utilizam os meios físicos ou lógicos do Hospital da Criança o conhecimento desta POSIC. 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:

a) **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;

b) **Ameaça:** qualquer evento que explore vulnerabilidades ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

c) **Análise de riscos:** uso sistemático de informações para identificar fontes e estimar o risco;

d) **Análise/avaliação de riscos:** processo completo de análise e avaliação de riscos;

e) **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;

f) **Ativo:** qualquer componente (seja humano, tecnológico, software ou outros) que sustente uma ou mais atividades e que tenha ou gere valor para a organização;

g) **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;

h) **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;

i) **Avaliação de riscos:** processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

j) **Celeridade:** as ações de segurança da informação e comunicações devem oferecer respostas rápidas a incidentes e falhas;

k) **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;

l) **Comunicação do risco:** troca ou compartilhamento de informação

sobre o risco entre o tomador de decisão e outras partes interessadas;

m) **Confidencialidade:** propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado ou não credenciado;

n) **Controle de acesso:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

o) **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;

p) **Desastre:** evento repentino e não planejado que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação;

q) **Descarte:** eliminação correta de informações, documentos, mídias e acervos digitais;

r) **Disponibilidade:** propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

s) **Estimativa de riscos:** processo utilizado para atribuir valores à probabilidade e consequências de um risco;

t) **Eficácia:** realizar um trabalho que atinja totalmente os resultados esperados;

u) **Eficiência:** realizar um trabalho correto, sem erros e de boa qualidade;

v) **Ética:** os direitos dos colaboradores devem ser preservados sem comprometimento da Segurança da Informação e Comunicações;

w) **Evento de segurança da informação:** ocorrência identificada de um procedimento, 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;

x) **Gerenciamento de operações e comunicações:** atividades, processos, procedimentos e recursos que visam disponibilizar e manter serviços, sistemas e infraestrutura que os suporte, satisfazendo os acordos de níveis de serviço;

y) **Gestão de ativos:** processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles desses ativos;

z) **Gestão de continuidade dos negócios:** processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização e suas atividades de valor agregado;

aa) **Gestão 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;

bb) **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;

cc) **Gestor de segurança da informação e comunicações:** é o colaborador responsável pelas ações de segurança da informação e comunicações;

dd) **Identificação de riscos:** processo para localizar, listar e caracterizar elementos do risco;

ee) **Incidente de SIC:** evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

ff) **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;

gg) **Integridade:** propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

hh) **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;

ii) **Proprietário de ativos de informação:** unidade administrativa responsável por gerenciar determinado segmento de informação e todos os ativos relacionados;

jj) **Quebra de segurança:** ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

kk) **Recursos criptográficos:** sistemas, programas, processos e equipamento isolado ou em rede que utilizam algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;

ll) **Resiliência:** poder de recuperação ou capacidade de uma organização

resistir aos efeitos de um desastre;

mm) **Responsabilidade:** os colaboradores devem conhecer e respeitar todas as normas de segurança da informação e comunicações da instituição;

nn) **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;

oo) **Segurança física e do ambiente:** processo que trata da proteção de todos os ativos físicos da instituição, englobando instalações físicas, internas e externas, em todas as localidades em que a organização está presente;

pp) **Sistema estruturante:** conjunto de sistemas informáticos fundamentais e imprescindíveis para a consecução das atividades administrativas, de forma eficaz e eficiente;

qq) **Terceiros:** quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos ao Hospital da Criança;

rr) **Transferir risco:** uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco;

ss) **Tratamento da informação:** conjunto de ações referentes à recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação;

tt) **Tratamento de incidentes:** é o processo que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

uu) **Tratamento dos riscos:** processo e implementação de ações de

segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco;

vv) **Usuário:** colaborador que obteve autorização do responsável pela área interessada para acesso aos ativos de Informação;

ww) **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. REFERÊNCIAS LEGAIS E NORMATIVAS

a) **Lei 8.159, de 8 de janeiro de 1991:** que dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências;

b) **Lei nº 9.983, de 14 de julho de 2000**: dispõe sobre a responsabilidade administrativa, civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública;

c) **Lei nº 12.527, de 18 de novembro de 2011:** regulamenta o acesso às informações públicas;

d) **Decreto-Lei nº 5.452, de 1º de maio de 1943:** aprova a Consolidação das Leis do Trabalho (CLT);

e) **Decreto nº 1.171, de 22 de junho de 1994:** aprova o Código de Ética Profissional do Colaborador Civil do Poder Executivo Federal;

f) **Decreto nº 3.505, de 13 de junho de 2000:** institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

g) **Decreto nº 5.482, de 30 de junho de 2005:** dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da administração pública federal, por meio da Rede Mundial de Computadores – Internet;

h) **Decreto nº 7.845, de 14 de novembro de 2012:** regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

i) **Decreto Nº 8.638, de 15 de janeiro de 2016:** que institui a Estratégia de Governança Digital;

j) **Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008:** disciplina a Gestão de Segurança da Informação e Comunicações da Administração Pública Federal, direta e indireta, e dá outras providências, e respectivas normas complementares;

k) **Instrução Normativa GSI/PR nº 02, de 5 de fevereiro de 2013:** dispõe sobre o credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal;

l) **Norma ABNT NBR ISO/IEC 27001:2013:** estabelece os elementos de um Sistema de Gestão de Segurança da Informação e Comunicações;

m) **Norma ABNT NBR ISO/IEC 27002:2013:** institui o código de melhores práticas para Gestão de Segurança da Informação e da Comunicação;

n) **Norma ABNT NBR ISO/IEC 27005:2011:** estabelece diretrizes para o processo de gestão de riscos de segurança da informação;

o) **PoSIC – Política de Segurança da Informação e Comunicação do Hospital de Clínicas Da UFTM/EBSERH**: estabelece a política de segurança da informação e comunicação dos Hospitais da Rede Ebserh.

## 4. PRINCÍPIOS

Esta Política de Segurança da Informação e Comunicações e suas ações serão norteadas pelos seguintes princípios, assim definidos:

a) **Celeridade:** as ações de SIC devem oferecer respostas rápidas a incidentes e falhas de segurança;

b) **Ética:** os direitos e interesses legítimos dos usuários e colaboradores devem ser preservados, sem comprometimento da SIC;

c) **Clareza:** as regras de segurança dos ativos de segurança da informação e comunicações devem ser precisas, concisas e de fácil entendimento;

d) **Legalidade:** as ações de segurança devem respeitar as atribuições regimentais, bem como as leis, normas e políticas organizacionais, administrativas, técnicas e operacionais do Hospital da Criança;

e) **Publicidade:** transparência no trato da informação, observados os critérios legais.

## 5. DIRETRIZES GERAIS

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

Esta Política de Segurança da Informação tem como base a Política de Segurança da Informação do Hospital de Clínicas da UFTM/EBSERH. Embora seja destinada a um órgão da Administração Pública Federal (com seus requisitos e qualificações específicos) a referida POSIC foi utilizada como documento base para que o Hospital da Criança possa usufruir dos critérios nela contida.

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 Hospital da Criança serão utilizados estritamente para seu propósito.

É vedado a qualquer usuário do Hospital da Criança o uso dos recursos de Tecnologia da Informação e Comunicações 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 das normas de SIC.

Os casos omissos e as dúvidas surgidas na aplicação do disposto nesta POSIC, devem ser direcionados ao Comitê Gestor de Segurança da Informação e Comunicações, com a interveniência do Comitê Gestor de Tecnologia da Informação e Comunicações.

## 6. DIRETRIZES ESPECÍFICAS

### 6.1. GESTÃO DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (GESIC)

Todos os mecanismos de proteção utilizados para a SIC devem ser mantidos com o objetivo de garantir a continuidade do negócio.

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 segurança da informação e comunicações do Hospital da Criança devem ser explicitamente citados em todos os termos de compromisso celebrados entre a instituição e terceiros, através de cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta política, bem como deverá ser exigido um termo de confidencialidade.

### 6.2. GESTÃO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA EM REDE COMPUTACIONAL (GETIR)

A Diretoria de Gestão de Processos e Tecnologia da Informação deverá criar e manter Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), instituída pelo Comitê Gestor de Segurança da Informação e Comunicações

(CGSIC), com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em redes de computadores.

Os eventos e incidentes de SIC devem ser tratados de acordo com um Plano de Gerenciamento de Incidentes específico, comunicados e registrados.

### 6.3. GESTÃO DE RISCOS E SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (GRSIC)

A 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.

As áreas responsáveis por ativos de informação deverão implementar processo contínuo de Gestão de Riscos, que será aplicado na implementação e operação da GRSIC.

A GRSIC deve ser realizada no âmbito do Hospital da Criança, visando identificar os ativos relevantes e determinar ações de gestão apropriadas, e deve ser atualizada periodicamente, no mínimo 01 (uma) vez por ano, ou tempestivamente, em função de inventários de ativos, de mudanças, ameaças ou vulnerabilidades. Trata-se de um instrumento do programa de Gestão de Riscos que deve incluir um Plano de Continuidade de Negócio (PCN) e um Plano de Gerenciamento de Incidentes (PGI).

O Plano de Continuidade de Negócio deverá complementar a análise de riscos, visando limitar os impactos do incidente e garantir que as informações requeridas para que os processos do negócio estejam prontamente disponíveis.

O Plano de Gerenciamento de Incidentes definirá responsabilidades e procedimentos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de SIC.

### 6.4. GESTÃO DE CONTINUIDADE DE NEGÓCIOS (GECON)

A GECON é um processo abrangente de gestão que identifica ameaças potenciais aos ativos de informação do Hospital da Criança e possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma

estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente aos incidentes de SIC e minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do Hospital da Criança, além de recuperar perdas de ativos de informação.

As áreas do Hospital da Criança deverão manter processo de gestão de continuidade de negócios, visando não permitir que os negócios baseados em Tecnologia da Informação sejam interrompidos e, também, assegurar a sua retomada em tempo hábil, quando for o caso.

A resiliência contra possíveis interrupções de sua capacidade em atingir seus principais objetivos deve ser uma prática proativa de todos os titulares das unidades administrativas, de forma a proteger a reputação e a imagem institucional do Hospital da Criança.

Todas as áreas do Hospital da Criança que dependam de recursos de Tecnologia da Informação e da Comunicação deverão criar Planos de Gerenciamento de Incidentes, de acordo com o grau de probabilidade de ocorrências de eventos ou sinistros e estabelecer um conjunto de estratégias e procedimentos que deverá ser adotado em situações que comprometam o andamento normal dos processos e a consequente prestação dos serviços.

As medidas constantes do Plano de Gerenciamento de Incidentes deverão assegurar disponibilidade dos ativos de informação e a recuperação de atividades críticas à normalidade, com o objetivo de minimizar o impacto sofrido diante do acontecimento de situações inesperadas, desastres, falhas de segurança, entre outras, até que se retorne à normalidade.

## 6.5. GESTÃO DE ATIVOS DE INFORMAÇÃO

A gestão de ativos de informação deverá observar normas operacionais e procedimentos específicos para garantir a sua operação segura e contínua.

Os ativos de informação do Hospital da Criança deverão ser inventariados, atribuídos aos respectivos responsáveis e seu uso deve estar em conformidade com os princípios e normas operacionais de SIC e são destinados ao uso

corporativo, sendo vedada a utilização para fins em desconformidade com os interesses institucionais.

Todos os ativos deverão ser classificados em termos de valor, requisitos legais, sensibilidade e criticidade da informação para a instituição.

O usuário deve ter acesso apenas aos ativos necessários e indispensáveis ao seu trabalho, respeitando as recomendações de sigilo de normas e legislação específica de classificação de informação.

É vedado comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo Hospital da Criança.

## 6.6. TRATAMENTO DA INFORMAÇÃO

A informação deve ser protegida de forma preventiva, com o objetivo de minimizar riscos às atividades e serviços do Hospital da Criança.

Os dados, as informações e os sistemas de informação do Hospital da Criança 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, elaborando-se, para tanto, sistema de classificação da informação.

## 6.7. CLASSIFICAÇÃO DA INFORMAÇÃO

Toda informação criada, manuseada, armazenada, transportada ou descartada do Hospital da Criança será classificada de acordo com a Lei nº 12.527, de 18 de novembro 2011.

O usuário deverá ser capaz de identificar a classificação atribuída a uma informação tratada pelo Hospital da Criança e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

As informações sob gestão do Hospital da Criança terão segurança de maneira a serem adequadamente protegidas quanto ao acesso e uso, sendo que para as consideradas de alta criticidade, serão necessárias medidas especiais de tratamento com o objetivo de limitar a exploração das informações exclusivas da instituição.

## 6.8. MONITORAMENTO, AUDITORIA E CONFORMIDADE

O monitoramento, auditoria e conformidade observarão o seguinte:

a) O uso dos recursos de tecnologia da informação e comunicações disponibilizados pelo Hospital da Criança é passível de monitoramento e auditoria, e devem ser implementados e mantidos, sempre que possível, mecanismos que permitam a sua rastreabilidade;

b) A entrada e saída de ativos de informação do Hospital da Criança serão registradas e autorizadas por autoridade competente mediante procedimento formal;

c) O Setor de TI do Hospital da Criança manterá registros e procedimentos, como trilhas de auditoria e outros que assegurem o rastreamento, acompanhamento, controle e verificação de acessos a todos os sistemas corporativos, à rede interna e à internet;

d) Será mantido pela Ouvidoria do Hospital da Criança um canal de comunicação para receber denúncias de infração a qualquer parte desta POSIC.

## 6.9. CONTROLE DE ACESSO E USO DE SENHAS

As regras de controle de acesso a todos os sistemas corporativos, intranet, internet, informações, dados e às instalações físicas do Hospital da Criança deverão ser definidas e regulamentadas, por intermédio de normas internas, com o objetivo de garantir a segurança dos usuários e a proteção dos ativos da instituição.

### 6.10. USO DE E-MAIL

O correio eletrônico é um recurso de comunicação corporativa do Hospital da Criança e as regras de acesso e utilização do e-mail devem atender a todas as orientações desta POSIC e das normas específicas, além das demais diretrizes do governo.

### 6.11. ACESSO À INTERNET

O acesso à rede mundial de computadores (internet), no ambiente de trabalho, deve ser regido por normas e procedimentos específicos, atendendo às determinações desta POSIC, e demais orientações governamentais e legislação em vigor.

### 6.12. USO DAS REDES SOCIAIS

A utilização de perfis institucionais mantidos em redes sociais com o objetivo de prestar atendimento e serviços públicos, divulgando ou compartilhando informações do Hospital da Criança, deve ser regida por normas internas especificas e deve estar alinhada tanto à POSIC quanto aos objetivos estratégicos da instituição.

### 6.13. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO

As atividades de aquisição, manutenção e desenvolvimento de sistemas de informação devem observar critérios e controles de segurança para garantir o respeito aos atributos básicos de segurança da informação.

### 6.14. CONSCIENTIZAÇÃO, SENSIBILIZAÇÃO E CAPACITAÇÃO EM SIC

O Hospital da Criança deverá promover continuamente a capacitação, reciclagem e o aperfeiçoamento de todos os usuários da instituição por meio de programas de divulgação, sensibilização, conscientização e capacitação em segurança

da informação e comunicações, com o propósito de criar uma cultura de segurança dentro da instituição.

### 6.15. PLANO DE INVESTIMENTOS EM SIC

Os investimentos em segurança da informação e comunicações serão realizados de forma planejada e consolidados em um Plano de Investimentos em SIC e, no que couber, no Plano Diretor de Tecnologia da Informação e Comunicações (PDTIC).

O Plano de Investimentos em SIC deverá ser reavaliado quando houver revisão orçamentária ou revisão de prioridades das ações de SIC.

### 6.16. PROPRIEDADE INTELECTUAL

As informações produzidas por usuários internos e colaboradores, no exercício de suas funções, são patrimônio intelectual do Hospital da Criança e não cabe a seus criadores qualquer forma de direito autoral, ressalvando o direito de autoria, se for o caso.

É vedada a utilização de patrimônio intelectual do Hospital da Criança em quaisquer projetos ou atividades de uso diverso do estabelecido pela instituição, salvo autorização específica.

### 6.17. 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.

O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar esta política e suas normas complementares aos empregados, prepostos e todos os envolvidos em atividades vinculadas ao Hospital da Criança.

### 6.18. USO DE COMPUTAÇÃO EM NUVEM

O uso de recursos de Computação em Nuvem para suprir demandas de transferência e armazenamento de documentos, processamento de dados, aplicações, sistemas e demais tecnologias da informação, deve ser regido por normas específicas, atendendo a determinações desta POSIC e demais orientações governamentais e legislação em vigor, visando garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento de um prestador de serviço.

### 6.19. USO DE DISPOSITIVOS MÓVEIS

As diretrizes gerais de uso de dispositivos móveis para acesso às informações, sistemas, aplicações e e-mail do Hospital da Criança devem considerar, prioritariamente, os requisitos legais e a estrutura da Instituição, atendendo a esta Política de Segurança da Informação e Comunicações e regidas por normas específicas, as quais contemplarão recomendações sobre o uso desses dispositivos.

## 7. PENALIDADES

Ações que violem esta política ou quaisquer de suas diretrizes, normas ou procedimentos ou que quebrem os controles de Segurança da Informação e Comunicações, serão devidamente apuradas e aos responsáveis serão aplicadas as sanções penais, administrativas e civis em vigor.

O usuário responderá disciplinarmente e/ou civilmente pelo prejuízo que vier a ocasionar à instituição, podendo culminar com o seu desligamento e eventuais processos criminais, se aplicáveis.

## 8. COMPETÊNCIAS E RESPONSABILIDADES

### 8.1. DIRETORIA EXECUTIVA DO HOSPITAL DA CRIANÇA

a) Promover a cultura de segurança da informação e comunicações;

b) Aprovar a Política de Segurança da Informação e Comunicações (POSIC);

c) Nomear o Gestor de Segurança da Informação e Comunicações;

d) Propor programa orçamentário específico para as ações de SIC;

e) Aplicar ações corretivas e disciplinares cabíveis nos casos de quebra de segurança.

### 8.2. GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

a) Promover e disseminar a cultura de segurança da informação e comunicações;

b) Coordenar a elaboração da Política de Segurança da Informação e Comunicações;

c) Instituir e coordenar o Comitê Gestor de Segurança da Informação e Comunicações (CGSIC) e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR);

d) Coordenar as ações de segurança da informação e comunicações;

e) Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança e submeter à Presidência do Hospital da Criança os resultados consolidados de tais investigações e avaliações;

f) Propor recursos necessários às ações de Segurança da Informação e Comunicações;

g) Realizar e acompanhar estudos de novas tecnologias, quanto aos possíveis impactos na segurança da informação e comunicações;

h) Propor normas e procedimentos relativos à Segurança da Informação e Comunicações;

i) Prover os meios necessários para capacitação, o aperfeiçoamento técnico dos membros da ETIR, bem como prover a infraestrutura necessária para o seu funcionamento;

j) Providenciar a divulgação interna desta POSIC.

## 8.3. COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

a) Promover a cultura de segurança da informação e comunicações;

b) Implementar, acompanhar, avaliar e propor alterações desta POSIC e de suas normas;

c) Definir diretrizes estratégicas para aplicação da POSIC no Hospital da Criança;

d) Propor normas e procedimentos relativos à SIC em conformidade com as legislações existentes sobre o tema;

e) Assessorar na implementação das ações de SIC do Hospital da Criança;

f) Propor à Presidência do Hospital da Criança penalidades em caso de violação desta POSIC;

g) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;

h) Solicitar apurações quando da suspeita de ocorrências de quebras de SIC;

i) Avaliar, revisar e analisar criticamente a POSIC e suas normas complementares, visando a sua aderência aos objetivos institucionais do Hospital da Criança e às legislações vigentes;

j) Dirimir eventuais dúvidas e deliberar sobre assuntos relativos à POSIC;

k) Aprovar Plano de Investimentos em Segurança da Informação e Comunicações;

l) Definir e atualizar seu regimento interno.

## 8.4. EQUIPE DE TRATAMENTO DE INCIDENTES EM REDES DE COMPUTADORES

a) Facilitar e coordenar as atividades de tratamento e resposta a incidentes de SIC;

b) Promover a recuperação de sistemas;

c) Agir proativamente com o objetivo de tratar incidentes de segurança, divulgando práticas e recomendações de SIC e avaliando condições de segurança de redes por meio de verificações de conformidade;

d) Realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos, buscando causas, danos e responsáveis;

e) Analisar ataques e intrusões da rede do Hospital da Criança;

f) Executar as ações necessárias para tratar quebras de segurança;

g) Obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causa, data da ocorrência, frequência e custos resultantes;

h) Cooperar com outras equipes de tratamento e resposta a incidentes;

i) Participar de fóruns, redes nacionais e internacionais relativas à SIC.

## 8.5. PROPRIETÁRIO DE ATIVOS DE INFORMAÇÃO

a) Descrever o ativo de informação;

b) Definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade em conformidade com esta POSIC;

c) Garantir a segurança dos ativos de informação sob sua

responsabilidade através de monitoramento contínuo;

d) Comunicar as exigências de SIC do ativo de informação a todos os custodiantes e usuários;

e) Conceder e revogar acessos aos ativos de informação;

f) Comunicar à ETIR os riscos e a ocorrência de incidentes de SIC;

g) Designar custodiante dos ativos de informação, quando aplicável.

### 8.6. CUSTODIANTE DOS ATIVOS DE INFORMAÇÃO

a) Proteger e manter os ativos de informação;

b) Controlar o acesso, conforme requisitos definidos pelo proprietário da informação e em conformidade com esta POSIC;

c) Definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade em conformidade com esta POSIC.

### 8.7. TERCEIROS E FORNECEDORES

a) Tomar conhecimento desta POSIC;

b) Fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato;

c) Fornecer toda a documentação dos sistemas, produtos e serviços relacionados às suas atividades.

### 8.8. USUÁRIOS

a) Conhecer e cumprir todos os princípios, diretrizes e responsabilidades desta POSIC, bem como os demais normativos e resoluções relacionados à Segurança da Informação e Comunicações;

b) Obedecer aos requisitos de controle especificados pelos gestores e

custodiantes da informação; e

c) Comunicar os incidentes que afetam à segurança dos ativos de informação e comunicações à ouvidoria ou à ETIR.

## 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 na Intranet, seminários de conscientização e quaisquer outros meios, como forma de ser criada uma cultura de segurança dentro do Hospital da Criança.

Cabe ao Gestor de Segurança da Informação e Comunicações providenciar a divulgação interna desta POSIC e das normas, inclusive com publicação permanente na página da intranet do Hospital da Criança, 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 E VALIDADE

A SIC, 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.

Os instrumentos normativos gerados a partir desta POSIC deverão ser revisados sempre que se fizer necessário, em função de alterações na legislação pertinente ou de diretrizes políticas do Governo Federal, ou conforme os seguintes critérios:

### 10.1. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (POSIC):

a) Nível de Aprovação: Diretoria Executiva

b) Periodicidade de Revisão: Anual

### 10.2. NORMAS DE SEGURANÇA DA INFORMAÇÃO:

a) Nível de Aprovação: Comitê de Segurança da Informação e Comunicações (CGSIC)

b) Periodicidade de Revisão: Semestral

### 10.3. PROCEDIMENTOS OPERACIONAIS:

a) Nível de Aprovação: Área Técnica

b) Periodicidade de Revisão: Semestral

### 10.4. VALIDADE

Esta POSIC tem prazo de validade indeterminado, portanto, sua vigência se estenderá até a edição de outro marco normativo que a atualize ou a revogue.

## 11. PRINCIPAIS SIGLAS

ABNT Associação Brasileira de Normas Técnicas

CGSIC Comitê Gestor de Segurança da Informação e Comunicações

EBSERH Empresa Brasileira de Serviços Hospitalares

ETIR Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais

GETIR Gestão de Tratamento de Incidentes de Segurança em Rede Computacional

GECON Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações

GESIC Gestão de Segurança da Informação e Comunicações

GRSIC Gestão de Riscos de Segurança da Informação e Comunicações

IEC International Electrotechnical Commission

| | |
|---|---|
| ISO | International Organization for Standardization |
| POSIC | Política de Segurança da Informação e Comunicações |
| SIC | Segurança da Informação e Comunicações |
| SISP | Sistema de Administração dos Recursos de Informação e Informática |
| TI | Tecnologia da Informação |
| TIC | Tecnologia da Informação e Comunicação |
| PDTIC | Plano Diretor de Tecnologia da Informação e Comunicações |