1. INTRODUÇÃO

A gestão da segurança da informação do HCI será orientada por um conjunto de normas e procedimentos interligados. A Política e Segurança da Informação (PSI) define os princípios e diretrizes estratégicas, enquanto as normas operacionais estabelecem os controles específicos a serem implementados. Os procedimentos operacionais, por sua vez, detalham as ações a serem realizadas para garantir a conformidade com as normas e procedimentos, proporcionando um guia prático para as atividades diárias.

2. OBJETIVO

Esta política tem como objetivo primordial proteger os dados, informações e sistemas do Hospital de Clínicas de Itajubá (HCI) contra ameaças e vulnerabilidades. Ao estabelecer diretrizes estratégicas para garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações, a PSI visa assegurar a continuidade dos serviços, a proteção da reputação institucional e o cumprimento da legislação, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD). A PSI também direciona as ações do HCI para a gestão de riscos e o tratamento de incidentes de segurança da informação, promovendo uma cultura de segurança e garantindo a proteção dos ativos de informação da instituição.

3. APLICAÇÃO

A garantia da segurança das informações no HCI é uma responsabilidade compartilhada por todos os membros da instituição, incluindo colaboradores, parceiros e quaisquer usuários. Esta política aplica-se a todos os colaboradores, prestadores de serviços, parceiros, pacientes e demais indivíduos que tenham acesso aos sistemas, redes e informações do HCI, independentemente do seu vínculo com a instituição.

4. BASE LEGAL

A presente PSI foi elaborada em conformidade com a legislação vigente e está alinhada com os documentos institucionais, incluindo, mas não se limitando:

- Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018): Estabelece normas sobre o tratamento de dados pessoais, incluindo dados sensíveis, e os direitos dos titulares.
- Normas da ANVISA: Regulamentam a segurança e a privacidade de informações em sistemas de saúde.
- Decreto nº 7.724, de 16 de maio de 2012: regulamenta a Lei de Acesso à Informação (LAI)
- ABNT NBR ISO/IEC 27001: Norma Internacional de Sistemas de Gestão de Segurança da Informação
- Norma ABNT NBR ISO/IEC 27002:2013: institui o código de melhores práticas para Gestão de Segurança da Informação e da Comunicação

5. PRINCÍPIOS

Atuamos de forma célere, ética, clara e transparente, garantindo a segurança da informação e o respeito aos direitos dos usuários. Todas as ações serão conduzidas em conformidade com as leis, normas e políticas institucionais, assegurando a publicidade e a transparência nas informações. As ações serão norteadas pelos seguintes princípios, assim definidos:

- Celeridade: A instituição deve 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 PSI;
- 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;
- Publicidade: Transparência no trato da informação, observados os critérios legais.

6. METAS INSTITUCIONAIS

Assegurar a proteção dos dados da organização através da institucionalização de uma Política de Segurança da Informação, que será amplamente divulgada e compreendida por todos os colaboradores. Além disso, serão implementadas ações de conscientização contínuas e protocolos específicos para prevenir, detectar, conter e corrigir incidentes de segurança, como ataques cibernéticos e vazamentos de informações confidenciais.

7. MEDIDAS DE SEGURANÇA

- Controle de acesso: Implementar mecanismos de autenticação e autorização para acesso aos sistemas e informações.
- Criptografia: Utilizar criptografia para proteger dados em trânsito e em repouso.
- Gestão de dispositivos: Controlar o acesso e o uso de dispositivos móveis e outros equipamentos.
- Backup e recuperação: Realizar backups regularmente e testar os procedimentos de recuperação.
- Sensibilização e treinamento: Oferecer treinamentos periódicos aos colaboradores sobre segurança da informação.
- Gestão de incidentes: Estabelecer procedimentos para identificar, responder e investigar incidentes de segurança.
- Contingência: Desenvolver planos de contingência para garantir a continuidade dos serviços em caso de incidentes.

8. COMPETÊNCIAS DE RESPONSABILIDADES:

Diretoria Executiva

- Monitorar o desempenho do Sistema de Gestão de Segurança da Informação e garantir a sua conformidade com as normas e regulamentações, incluindo a LGPD.

- Investigar e tomar as medidas cabíveis em caso de incidentes de segurança que possam comprometer a privacidade dos pacientes ou a integridade dos dados.
- Receber relatórios periódicos sobre o estado da segurança da informação e tomar as decisões necessárias para garantir a proteção dos dados dos pacientes.
- Comunicar aos colaboradores, médicos, pacientes e demais partes interessadas as decisões e ações relacionadas à segurança da informação, enfatizando a importância da proteção dos dados dos pacientes.
- Assegurar a alocação dos recursos necessários para a implementação da estratégia de segurança da informação;

Comitê de Segurança da Informação

- Assessoria à Diretoria Executiva;
- Definição de políticas e procedimentos;
- Implementação de projetos;
- Monitoramento e avaliação do sistema de gestão de segurança da informação;
- Investigação de incidentes;
- Promoção da conscientização e treinamento;
- Elaboração de relatórios. O CSI se reunirá periodicamente para discutir as questões relacionadas à segurança da informação e tomar as decisões necessárias.

Responsável pela Privacidade de Dados

O Encarregado de Dados (DPO) é a pessoa designada para atuar como elo de comunicação com a Autoridade Nacional de Privacidade de Dados (ANPD), com os titulares de dados, monitorar a adequação a Lei Geral de Proteção de Dados (LGPD) bem como aplicação e desempenho das políticas regimentais. Em caso de incidentes, dúvidas, sugestões ou orientações quanto à privacidade de dados pessoais ou dados pessoais sensíveis, acionar o DPO: Mariana Rodrigues de Castro | E-mail: dpo@hcitajuba.org.br

Recursos Humanos

É obrigatório comunicar à TI, de forma imediata, qualquer alteração relacionada a usuários dos sistemas, como contratações, desligamentos e mudanças de função. Todos os novos colaboradores e prestadores de serviços deverão assinar termos de confidencialidade e participar de treinamentos sobre segurança da informação e boas práticas de uso dos sistemas.

Tecnologia da Informação

Implementar um framework de segurança da informação abrangente, incluindo controles de acesso lógico e físico, gestão de vulnerabilidades, planos de investigação e de gestão de incidentes. Garantir a conformidade com os padrões de segurança da informação e realizar auditorias regulares.

9. DIRETRIZES GERAIS

É fundamental garantir a segurança da rede e prevenir atividades ilícitas. Portanto, a segurança da informação é responsabilidade de todos no HCI. Todas as informações, independentemente do formato ou meio, devem

ser protegidas de acordo com esta política. Os recursos de Tecnologia da Informação e Comunicação devem ser utilizados exclusivamente para fins institucionais e de acordo com as normas estabelecidas.

A proteção da informação é fundamental para garantir a integridade, confidencialidade e disponibilidade dos dados do HCI. Os casos omissos e as dúvidas surgidas na aplicação do disposto nesta PSI, devem ser direcionados ao Comitê Gestor de Proteção de Dados do HCI.

10. DIRETRIZES ESPECÍFICAS

O usuário deve ter acesso apenas aos ativos necessários e indispensáveis ao seu trabalho ou atividade, respeitando as recomendações técnicas, comportamentais e de sigilo específicas aplicáveis. A aplicação de cada uma das diretrizes constantes na relação abaixo deverá ser seguida rigorosamente.

Correio eletrônico (e-mail), sistemas de mensageria e de correspondências

- O uso do e-mail corporativo é de responsabilidade individual de cada usuário. As mensagens devem ser redigidas em linguagem profissional e respeitosa, evitando conteúdo difamatório, ofensivo, discriminatório ou que viole a legislação vigente, especialmente a LGPD. O HCI reserva-se o direito de monitorar e auditar todo o tráfego de e-mail corporativo, incluindo o conteúdo das mensagens.
  Contratos, convênios, acordos e instrumentos congêneres: Todos os contratos, convênios, acordos e instrumentos congêneres deverão conter cláusulas que estabeleçam a obrigatoriedade de observância desta PSI e da LGPD. O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar essa PSI e suas normas complementares aos empregados, prepostos e todos os envolvidos em atividades vinculadas ao HCI.
- As mensagens de correio eletrônico sempre deverão incluir assinatura conforme o padrão estabelecido pela instituição.
- É obrigatória a manutenção da caixa de e-mails pelo respectivo usuário, evitando acúmulo de e-mails e arquivos desnecessários.

Dispositivos de impressão, cópia e digitalização

- O uso de impressoras e scanners é monitorado para garantir a segurança da informação. Os equipamentos devem ser utilizados apenas para fins profissionais. A cópia de materiais protegidos por direitos autorais é proibida. Ao imprimir, verifique o destino e a segurança do documento.
- Os usuários devem recolher imediatamente suas impressões, sejam elas corretas ou impressões com falhas. No caso de impressões com falhas, deverão ser descartadas de forma adequada.

Acessos e recursos de internet (Rede Mundial)

- O acesso aos sistemas de informação é gerenciado pela TI, sendo concedido de forma individualizada e com base na necessidade de cada função. As credenciais de acesso são únicas e os privilégios são mínimos e estritamente necessários para o desempenho das atividades. A auditoria regular dos acessos garante a conformidade com as políticas de segurança.
- O acesso à rede Wi-Fi corporativa é exclusivo para equipamentos do HCI que possuam licenças válidas de software, antivírus atualizados. A chave de acesso é fornecida individualmente pela TI e deve ser mantida em sigilo. O compartilhamento da chave é proibido e a TI realizará trocas periódicas.

- É terminantemente proibido a conexão de equipamentos de terceiros à rede do HCI sem a prévia autorização do Departamento de T.I e mediante assinatura do Termo de Confidencialidade e Política de Segurança da Informação. Se houver a necessidade de conectar os equipamentos de terceiros à rede de computadores, o mesmo deverá ter seu sistema operacional e antivírus licenciado e atualizado.
- A fim de preservar a segurança da informação, todas as informações e documentos gerados ou utilizados na rede interna do HCI são considerados propriedade institucional e devem ser protegidos.

Instalação de programas (softwares) e antivírus

- Todos os softwares utilizados no hospital devem possuir licença válida. A instalação de softwares sem autorização é proibida e sujeita a sanções disciplinares. O Departamento de TI realiza acompanhamento periódico para garantir a conformidade legal e a remoção de softwares não licenciados.
- É obrigatória a instalação e manutenção de softwares antivírus atualizados em todos os sistemas do HCI, sendo esta tarefa de responsabilidade exclusiva da área técnica.
- É obrigatório verificar todos os arquivos provenientes de fontes externas (internet, e-mail, dispositivos removíveis, etc.) utilizando o software antivírus antes de abri-los.

Dispositivos de acesso móveis e mídias removíveis

- O uso de aplicativos de mensagens como o WhatsApp na rotina profissional exige cuidados com a segurança da informação. O uso de dispositivos pessoais para tratar de dados corporativos ou sensíveis é desaconselhado devido à falta de controle do HCI sobre esses dispositivos.
- Evite o uso de aplicativos de mensagens para compartilhar dados pessoais, laudos, imagens ou informações estratégicas sem haja relevante necessidade ou finalidade. Caso seja imprescindível, utilize a função de mensagens temporárias e apague as informações do seu dispositivo após inserir os dados nos sistemas do hospital.
- O uso de mídias removíveis (cartões de memória, disquetes, pen drive, pen USB e similares) não é recomendado, pois trata-se de uma das maiores fontes de ameaças a vulnerabilidades, tanto no sentido de injetar ataques cibernéticos na Rede Corporativa, bem como fontes de vazamento de informações. Contudo, caso seja imprescindível sua utilização, atuar com toda a cautela possível e, quando estas não forem mais necessárias, deverão ser descartadas de forma segura e protegida.

Guarda de informações digitais (backup)

- A execução de rotinas sistemáticas de backup e guarda de informações é de responsabilidade exclusiva da equipe técnica da instituição;
- A fim de garantir a preservação e o acesso aos documentos essenciais para as atividades da Entidade, estes devem ser armazenados em drives de rede corporativa, permitindo a realização de backups regulares;

Estação de trabalho e controle de acesso físico

- Todos os computadores de uso individual deverão ter senhas para restringir o acesso de colaboradores não autorizados. Tais senhas serão definidas pela unidade setorial e TI, que terá acesso a elas para manutenção dos equipamentos.
- A guarda e o arquivamento de documentos físicos devem ser realizados em locais seguros, tanto internamente quanto externamente, e de acordo com os prazos estabelecidos pela legislação vigente

- Para garantir a confidencialidade das informações, evite deixá-las à vista. Documentos e dispositivos eletrônicos devem ser guardados em locais seguros e trancados.
- Todos que transitem por ambientes do HCI devem possuir identificação pessoal visível por crachás e registrados em sistema de controle de acessos.
- Ao término do contrato ou de suas atividades na instituição, os usuários devem devolver todos os materiais e equipamentos da organização que estiverem em sua posse.
- Em caso de desligamento, o funcionário deve garantir que todas as informações relevantes sejam transferidas para a organização e apagadas de seus dispositivos pessoais.

11. INCIDENTES DE SEGURANÇA

É obrigatório que os usuários reportem ao Departamento de Tecnologia da Informação qualquer incidente que comprometa a segurança dos sistemas ou dados do HCI. O não cumprimento desta obrigação poderá acarretar sanções disciplinares. A colaboração dos usuários é fundamental para garantir a segurança da informação do HCI.

A perda ou roubo de dispositivos com dados do HCI pode resultar em vazamento de informações sensíveis. Notifique imediatamente a DPO (dpo@hcitajuba.org.br) especificando os dados comprometidos para que as medidas cabíveis sejam tomadas. Ao reportar incidentes, você contribui para a proteção dos nossos sistemas e dados.

12. VIOLAÇÕES E SANÇÕES

O descumprimento desta política poderá acarretar sanções disciplinares e administrativas, conforme a gravidade da infração. Alguns exemplos de sanções incluem:

- Advertência formal: Uma advertência por escrito, registrada no prontuário do funcionário, serve como um alerta e pode ser utilizada como base para sanções mais severas em caso de reincidência.
- Suspensão: A suspensão temporária das atividades do funcionário pode ser aplicada em casos de violações mais graves.
- Demissão: Em casos de violações graves e intencionais, a demissão pode ser a sanção mais adequada.
- Treinamento obrigatório: O funcionário pode ser obrigado a participar de treinamentos adicionais sobre segurança da informação.
- Restrição de acesso: O acesso do funcionário a determinados sistemas ou informações pode ser restringido.

13. DIVULGAÇÃO E CONSCIENTIZAÇÃO

Para fomentar uma cultura de segurança da informação, o HCI promoverá campanhas contínuas de conscientização, disponibilizando as regras e orientações. É obrigatória a divulgação e atualização constante das informações, inclusive com publicação permanente na página do HCI, para que seu conteúdo possa ser consultado a qualquer momento. É importante desenvolver processo permanente de divulgação, sensibilização, conscientização e capacitação dos usuários sobre os cuidados e deveres relacionados.

14. REVISÃO E ATUALIZAÇÃO

A PSI será objeto de revisão periódica, visando garantir sua adequação às novas tecnologias, às melhores práticas de segurança e mudanças na legislação. Alterações na PSI ou nos instrumentos normativos dela decorrentes serão submetidas à aprovação do Comitê Gestor de Proteção de Dados.

15. CONSIDERAÇÕES FINAIS

A cultura de compliance é um processo contínuo que exige dedicação e esforço de todos os envolvidos. Ao implementar uma estrutura robusta e abrangente, a instituição estará devidamente preparada para enfrentar os desafios do mercado e garantir a sua sustentabilidade a longo prazo. Esta política entra em vigor a partir de sua publicação e substitui qualquer outra norma anterior que lhe seja contrária.

SITUAÇÃO	NOME	ÁREA DE ATUAÇÃO	DATA DE APROVAÇÃO
Elaboração	Paulo Henrique C. Teixeira	Juridico/ E	02/06/2023
Revisão	Mariana Rodrigues de Castro	Encarregada de Dados (DPO)	15/10/2024
Consenso	Comitê Gestor de Privacidade	Proteção de Dados	21/10/2024
Aprovador final	Seleno Glauber de Jesus Silva	Diretor Geral	25/10/2024