1. OBJETIVO

O objetivo desta política é definir normas e diretrizes para proteção dos dados da Santa Casa BH, contra ameaças internas e externas, reduzindo riscos operacionais, paradas sistêmicas, problemas de jurisdição e possíveis impactos financeiros em decorrência.

2. ABRANGÊNCIA

Santa Casa BH e partes interessadas.

Esta política se aplica a todos os colaboradores, prestadores de serviço e qualquer pessoa que tenha acesso aos sistemas, à rede, às informações ou aos equipamentos da Santa Casa BH. A abrangência se estende a todos os ambientes tecnológicos da instituição, incluindo infraestrutura física (datacenters, unidades de saúde), ambientes virtuais (nuvem pública/privada) e dispositivos móveis autorizados. Cobre especialmente os sistemas críticos para assistência à saúde, como prontuário eletrônico, sistemas de imagens médicas (PACS/RIS) e plataformas de gestão hospitalar, que demandam proteção adicional devido à sua sensibilidade e impacto operacional.

A política também regulamenta o acesso e uso de dados pessoais de pacientes e colaboradores, aplicando-se a qualquer forma de processamento, seja por meios digitais ou físicos. As obrigações permanecem válidas mesmo após o término de vínculos contratuais, até a completa eliminação ou devolução dos ativos informacionais, conforme exigido pela LGPD e normas internas de governança.

3. SIGLAS E DEFINIÇÕES

Agenda 2030: Corresponde a um conjunto de programas, ações e diretrizes que orientam os trabalhos das Nações Unidas e de seus países membros rumo ao desenvolvimento sustentável, atribuindo responsabilidade a todos os componentes da sociedade para cumprimento dos 17 ODS e suas metas.

Comitê de Compliance e Integridade (CCI): órgão colegiado composto por membros indicados pelo NDS (Núcleo de Direção Superior) da Santa Casa BH, responsável por garantir o atendimento às normas da instituição e acompanhar os pilares de trabalho da área de *Compliance* da Santa Casa BH e promover a cultura de integridade; avaliar, apoiar e disseminar as estratégias para a conformidade com a proteção de dados pessoais, privacidade das pessoas, segurança da informação e temas correlatos.

CEAO: Comitê Estratégico e de Aprimoramento Organizacional é um órgão executivo exercido por meio de um fórum colegiado de planejamento, administração, governança corporativa e assistencial, gestão de riscos,

controle, orçamento, finanças, elaboração de políticas, programas e projetos subordinados ao NDS (Núcleo de Direção Superior) e a Provedoria.

ERP: É a abreviação de Enterprise Resource Planning, é um sistema integrado de gestão empresarial que ajuda a centralizar e automatizar processos como finanças, estoque, vendas, RH e muito mais.

GPO: É a abreviação de Group Policy Object, é o conjunto de regras utilizado para aplicar, de forma centralizada, configurações de segurança e restrições em computadores da rede.

HSL: Hospital São Lucas Particular e Convênios.

IA: Inteligência Artificial.

ISO/IEC 27001:2013: Norma de padrão internacional que estabelece diretrizes para a gestão de segurança da informação.

ISO/IEC 27002:2013: Norma de padrão internacional que fornece orientações para a gestão de segurança da informação.

LGPD: Lei Geral de Proteção de Dados Pessoais.

ODS: Objetivos do Desenvolvimento Sustentável, são um apelo global à ação para acabar com a pobreza, proteger o meio ambiente e o clima e garantir que as pessoas, em todos os lugares, possam desfrutar de paz e de prosperidade. Estes são os objetivos para os quais a Organização das Nações Unidas está contribuindo a fim de que seja possível atingir a Agenda 2030 no Brasil.

Partes interessadas (*Stakeholders*): Pessoa ou instituição que pode afetar ser afetada ou se perceber afetada por uma decisão ou atividade (Provedor, Irmãos Associados, conselheiros, diretores, superintendentes, gerentes, coordenadores, colaboradores, corpo clínico, docentes, residentes, especializando, pesquisadores, estagiários, bolsistas, jovens aprendizes, voluntários, cooperados, prestadores de serviços, fornecedores, órgãos fiscalizadores e normativos, doadores, políticos, pacientes/clientes, acompanhantes, familiares, voluntários e visitantes, dentre outros).

PRS (Procedimento Sistêmico): Documento que descreve uma atividade ou interação sistêmica da instituição. Esse documento é aplicável a partir da interação das ações entre um conjunto de processos. A abrangência que consta no PRS deverá citar o (s) processo (s) envolvido (s) na atividade/tarefa e quem executa. É importante salientar que quando a abrangência do documento envolver somente um processo deverá ser descrito um POP - Procedimento Operacional Padrão e quando envolver dois ou mais processos

será considerado PRS.

Santa Casa BH: Santa Casa de Belo Horizonte.

TI: É a abreviação de Tecnologia da Informação, é um termo comum para definir todos os recursos de tecnologia para o processamento de informações, incluindo softwares, hardwares, tecnologias de comunicação e serviços relacionados.

USB: Padrão de conexão que permite a comunicação entre dispositivos eletrônicos móveis (pen drives, teclados, mouses e HDs externos).

VPN: É uma sigla, em inglês, para "Rede Virtual Privada", funciona criando uma rede de comunicações entre computadores e outros dispositivos que têm acesso restrito a quem tem as credenciais necessárias.

4. DIRETRIZES

O Sistema de Tecnologia da Santa Casa BH, está estruturado com o compromisso de salvaguardar os dados e informações da instituição, garantindo a governança eficaz dos ativos tecnológicos. Sua atuação visa mitigar riscos de segurança cibernética, assegurar a conformidade regulatória e promover um ambiente digital robusto, escalável e confiável para todas as operações assistenciais e administrativas.

Esta política estabelece um framework de segurança da informação baseado em três pilares essenciais: prevenção, detecção e resposta. Os controles técnicos alinhados aos padrões do setor para proteger ativos críticos, incluindo sistemas clínicos e dados de pacientes. A Santa Casa BH adota uma abordagem de segurança em camadas, com monitoramento contínuo, gestão de vulnerabilidades e planos de resposta a incidentes documentados.

O modelo incorpora os princípios de least privilege e zero trust, garantindo que cada acesso seja autenticado, autorizado e auditado. Além da proteção tecnológica, a política visa promover uma cultura organizacional de segurança através de treinamentos regulares e conscientização, assegurando que todos os colaboradores compreendam seu papel na proteção dos ativos de informação da instituição.

Para o uso adequado dos ativos de TI, gestão de acessos, proteção de dados e tratamento de incidentes de segurança, a Santa Casa BH adota as seguintes diretrizes:

- **Gestão segura de ativos de TI**, incluindo sistemas críticos para a operação hospitalar;
- **Controle de acessos** com governança rígida, especialmente a dados sensíveis de pacientes;
- **Proteção contra ameaças cibernéticas**, alinhada aos riscos institucionais;
- **Resposta a incidentes** com agilidade e minimização de impactos operacionais;

- **Backups de servidores e sistemas** garantindo a periodicidade de cópias seguras dos dados e configurações críticas armazenadas nos servidores da instituição.
- **Cadastro de ativos de TI** garantindo a gestão na usabilidade e rastreabilidade.

Desenvolvida em colaboração entre a área de TI e as lideranças da Santa Casa BH, esta política reflete tanto os requisitos técnicos de segurança quanto as necessidades estratégicas da organização, garantindo que a proteção da informação apoie nossa missão de excelência em saúde.

Para garantir a segurança da informação, é importante que todos sigam estes princípios:

- **Confidencialidade:** Garantia de que a informação seja acessível apenas por pessoas autorizadas;
- **Integridade:** Garantia de que a informação não será alterada indevidamente;
- **Disponibilidade:** Acesso à informação sempre que necessário, garantindo a continuidade dos serviços;
- **Autenticidade:** Refere-se à garantia de que um usuário, dispositivo ou dado é, de fato, quem ou o que afirma ser. Esse princípio é fundamental para reduzir riscos de acesso não autorizado e fortalecer a segurança da informação.
- **Conformidade:** Atendimento às normas e leis vigentes.

A adesão a estes princípios é obrigatória para todos os colaboradores, prestadores de serviço e parceiros que interajam com os sistemas ou dados do SCBH, constituindo elemento fundamental para nossa estratégia de transformação digital segura no setor de saúde.

4.1 Aspectos da Segurança da Informação:

Os aspetos da segurança da informação, baseados nas diretrizes de confidencialidade, integridade, disponibilidade e conformidade, visam garantir a proteção dos dados e sistemas de uma organização contra ameaças internas e externas (Cabrice, 2015), (Martin & Khazanchi, 2006), (Tyagi et al., 2012) [3]. Estas diretrizes formam a base para a implementação de políticas de segurança eficazes e controles que protegem os ativos de informação e asseguram o cumprimento das normas e regulamentos aplicáveis conforme (Galatenko et al., 2021), e (Correia et al., 2017).

> [...]". À *medida que as organizações adotam cada vez mais ambientes de nuvem híbrida, a complexidade de gerenciar e proteger essas infraestruturas aumentam. Integrações entre nuvem híbrida e on-premise apresentam desafios únicos em termos de segurança de dados, controle de acesso e conformidade, exigindo uma abordagem mais avançada e unificada para a segurança de*

*redes em nuvem (*Oladosu et al., 2021). "[...]

Aspecto da Segurança	Descrição	Exemplo
Confidencialidade	Garantir que informações pessoais ou confidenciais sejam acessadas apenas por usuários autorizados.	Acesso restrito ao prontuário eletrônico de pacientes (PEP), Restrição de acesso a documentos, sistemas institucionais, etc, por meio de Gestão de Acessos.
Integridade	Assegurar que os dados sejam consistentes, íntegros e confiáveis durante todo o seu ciclo de vida.	Controle de versão documental/sistêmica. Trilha de auditorias regulares em prescrições médicas.
Disponibilidade	Garantia de acesso legítimo e contínuo às informações por usuários autorizados, exceto em manutenção planejada.	Garantia de funcionamento do sistema de gestão hospitalar de forma ininterrupta garantindo o acesso do corpo clínico, mantendo os softwares atualizados.
Autenticidade	Validar a autenticidade dos usuários, garantindo que os perfis sejam personalizados e rastreáveis através de Gestão de logins e senhas.	Acesso individual por biometria ou senha no ingresso a sistemas institucionais, como registro de evoluções e prescrições médicas no prontuário eletrônico do paciente (PEP).
Conformidade	Garantir que a autoria da informação esteja em conformidade com as normas e leis vigentes.	Assinatura do PEP no modo digital efetuado pelos médicos em laudos e prescrições eletrônicas, garantidos conforme Conselho Federal de Medicina (CFM) e pela Sociedade Brasileira de Informática em Saúde (SBIS).

4.2 Utilização da Inteligência Artificial (IA) na Santa Casa BH

Comprometida com a transparência e a segurança no uso de novas tecnologias, a Santa Casa BH estabelece preceitos para a implementação responsável da Inteligência Artificial (IA), conforme a seguir:

4.2.1 Boas Práticas e Transparência

- **Protocolos de Informação:** A instituição manterá protocolos claros para informar pacientes e colaboradores sobre o uso da IA, seus benefícios, riscos e limitações.
- **Supervisão Humana:** Todo conteúdo gerado por IA passará por rigorosa supervisão humana para garantir a qualidade, precisão e alinhamento com os valores da instituição.
- **Garantia de Qualidade:** A qualidade do material gerado automaticamente será assegurada por "supervisão de processos", leituras por amostragem e outras formas de checagem, combinando celeridade e exatidão.

4.2.2 Diretrizes para o Uso da IA

- **Transparência:** Informar claramente quando a IA for utilizada na produção de documentos ou materiais.
- **Segurança:** Implementar medidas robustas de segurança para proteger dados sensíveis e garantir a privacidade dos pacientes e colaboradores.
- **Treinamento:** Capacitar a equipe para utilizar a IA de forma ética, responsável e eficiente.
- **Auditoria:** Realizar auditorias, quando devido, para identificar e corrigir possíveis problemas relacionados ao uso da IA. Será de responsabilidade da área pertinente o monitoramento contínuo do uso da IA, incluindo a análise de indicadores de eficácia e eficiência da sua aplicação, de forma a garantir benefícios alinhados aos objetivos institucionais.

4.2.3 Aplicações Permitidas da IA

- **Geração de Conteúdo:** Utilizar a IA para auxiliar na produção de imagens, textos, vídeos, áudios, infográficos e outros formatos de conteúdo.
- **Revisão e Correção:** Empregar a IA para revisões gramaticais, correções factuais e ajustes de estilo em documentos e materiais.

4.2.4 Restrições ao Uso da IA

Para a utilização de novas tecnologias de Inteligência Artificial (IA) na Instituição, será necessário apresentar um **Parecer Técnico** das áreas pertinentes, conforme detalhado abaixo:

- **Tecnologia da Informação:** titular e obrigatório;
- **Jurídico/LGPD:** titular e obrigatório;
- **Compliance:** auxiliar e/ou outras áreas afins.

Caso necessário, os comitês e comissões institucionais aplicáveis deverão ser previamente informados e a respectiva deliberação deverá ser submetida ao CEAO, com direito de impugnação.

Uso da IA

- **Decisões Médicas:** A IA não substituirá o julgamento clínico e a tomada de decisões por profissionais de saúde qualificados; utilização de IA com regulamentação no segmento de saúde seguindo os princípios do Projeto de Lei 2338/2023.
- **Contato Humano:** A IA não substitui o contato humano essencial entre médicos e pacientes.
- **Discriminação:** A IA não será utilizada para discriminar pacientes com base em raça, gênero, religião ou qualquer outra característica pessoal.
- **Conteúdo Opinativo:** A IA não será utilizada para redigir textos opinativos ou editoriais.
- **Tratamento da IA na Saúde:** Considerar a IA no segmento saúde como risco alto em função do potencial de causar danos significativos ao indivíduo, carecendo de validação e monitoramento ativo.

4.2.5 Inovação e Aprimoramento

A Santa Casa BH reconhece o potencial disruptivo da IA e busca ativamente a inovação e a adoção de tecnologias avançadas para aprimorar a qualidade do trabalho e o atendimento aos pacientes. A IA será utilizada como ferramenta para ampliar a capacidade de processamento e geração de informações, sempre em consonância com os valores éticos e profissionais da instituição.

4.3 Gerenciamento de Ativos de TI

Os ativos de tecnologia (computadores, notebooks, Smartphone, Tablet, redes, softwares, servidores etc.) são de propriedade da SCBH e devem ser usados exclusivamente para fins institucionais, de acordo com a política de segurança da instituição.

Além disso, é responsabilidade de todos os colaboradores zelar pela integridade e uso adequado desses recursos, reportando eventuais falhas, perdas ou desvios ao setor responsável. A SCBH reserva-se o direito de monitorar o uso dos ativos de TI, assegurando conformidade com as normas internas e a proteção dos dados institucionais.

4.4 Uso e Manutenção de Equipamentos

- É proibido o consumo de alimentos e bebidas nas proximidades de equipamentos de TI, a fim de evitar danos por derramamento ou contaminação.
- Apenas a equipe de Tecnologia da Informação (TI) está autorizada a realizar movimentações, manutenções, instalações ou qualquer tipo de intervenção técnica nos equipamentos.
- Ativos de TI não devem ser utilizados para fins pessoais ou para atividades que não estejam diretamente relacionadas às funções profissionais do colaborador.
- Cada colaborador é responsável pelo uso adequado, conservação e integridade dos equipamentos que lhe forem disponibilizados.
- É proibida a instalação de softwares, dispositivos externos ou alterações nas configurações dos equipamentos, salvo quando previamente autorizados pela equipe de TI.
- Em caso de avarias, falhas ou comportamentos anômalos dos dispositivos, o usuário deve reportar imediatamente ao suporte técnico para avaliação e providências via sistema de chamados gestão X.
- A retirada de qualquer equipamento da empresa (Desktop – Impressoras - Monitores) deve ser previamente autorizada e registrada junto à equipe de TI. Exceto quando se trata de notebook e equipamentos moveis onde o responsável já assinou o termo de responsabilidade pela guarda e uso do ativo de trabalho, conforme PRS INST GER TI 002 – Controle de Segurança da Informação.

4.5 Uso de Softwares e Sistemas

- A instalação e o uso de softwares nos equipamentos corporativos devem ser previamente autorizados pela equipe de Tecnologia da Informação (TI). É expressamente proibida a instalação de programas não homologados, piratas ou sem licença, mesmo que utilizados para fins profissionais.
- A utilização dos sistemas institucionais deve seguir estritamente a finalidade operacional definida pela SCBH. É proibida a extração, manipulação, compartilhamento ou uso de dados para fins pessoais, comerciais ou externos à instituição, salvo em casos autorizados formalmente.
- Tentativas de modificar, copiar, clonar ou distribuir softwares institucionais sem autorização da TI serão consideradas infrações graves, podendo acarretar sanções administrativas, civis e/ou criminais, conforme a legislação vigente e as normas internas da organização.

- É responsabilidade de cada colaborador zelar pela confidencialidade das credenciais de acesso aos sistemas corporativos, não sendo permitido o compartilhamento de senhas ou o uso de logins de terceiros.

- O uso inadequado de softwares, como acessos indevidos, instalação de extensões não autorizadas ou exploração de vulnerabilidades, será monitorado e auditado periodicamente pela equipe de TI, em conformidade com as diretrizes de segurança da informação citados PRS INST GER TI 002 – Controle de Segurança da Informação.

4.6 Gerenciamento de Acessos

4.6.1 Controle de Acesso

- O acesso à rede, sistemas e demais recursos tecnológicos da instituição devem ser realizados exclusivamente por meio de login e senha pessoal e intransferível, sendo vedado o compartilhamento de credenciais entre usuários.
- As senhas devem atender aos critérios de complexidade definidos pela equipe de TI, incluindo: uso de letras maiúsculas e minúsculas, números, caracteres especiais e um comprimento mínimo de 8 caracteres. Recomenda-se a troca periódica das senhas a cada 45 dias, sendo vedada a reutilização das três últimas senhas, conforme estabelecido na política interna de segurança da informação.
- A concessão de acessos será feita somente mediante solicitação formal do gestor responsável, com justificativa clara e detalhamento dos níveis de permissão necessários ao desempenho da função.
- Todo acesso indevido, suspeito ou fora do padrão operacional deve ser reportado imediatamente à equipe de TI, para investigação e mitigação de possíveis riscos.
- A equipe de TI está autorizada a suspender, restringir ou revogar acessos a sistemas, serviços ou equipamentos sempre que for identificado risco iminente à segurança da informação, ou em caso de não conformidades com as diretrizes institucionais.
- O acesso de colaboradores desligados, afastados ou transferidos de setor deve ser revogado imediatamente após a formalização do status no RH, em alinhamento com o gestor direto.
- A criação de acessos temporários como no caso de terceiros ou prestadores de serviço - deverá seguir procedimento específico, com registro do prazo de validade, monitoramento de uso e assinatura de termo de responsabilidade, quando aplicável. Esses acessos seguirão o fluxo de solicitação via sistema Gestão X e serão configurados com expiração automática em até 90 dias, conforme o procedimento padrão da instituição.
- Todos os acessos são registrados e monitorados, e podem ser auditados a qualquer momento, conforme as normas da instituição PRS INST GER TI 002 – Controle de Segurança da Informação.

- Toda e qualquer solicitação de alteração ou redefinição de senha deve ser realizada por meio da abertura de uma OS no portal Gestão X ou, em casos de senha de rede, pelo telefone corporativo do Service Desk – (31) 98726-3513. Cada usuário tem autonomia para solicitar o reset apenas da senha de seu próprio usuário, sendo vedada a solicitação de redefinição de senha de contas de outros colaboradores do setor. Exceção: Apenas o gestor imediato poderá solicitar o reset de senha de um subordinado, devendo, obrigatoriamente, justificar o motivo na própria solicitação.

4.6.2 Acesso Remoto

- O acesso remoto aos recursos da instituição será permitido exclusivamente via VPN corporativa, mediante autorização prévia da equipe de TI e com credenciais individuais e intransferíveis. Exceções serão aplicadas apenas em casos de suporte imediato, nos quais o acesso poderá ser concedido por meio de ferramentas como AnyDesk ou TeamViewer, sendo obrigatório o acompanhamento de um técnico, analista ou solicitante durante toda a sessão.
- Fornecedores e terceiros só poderão acessar os sistemas institucionais mediante contrato formalizado, contendo cláusulas de confidencialidade e segurança da informação, além da definição clara do escopo de atuação.
- Em casos de acesso remoto a servidores ou sistemas críticos, será obrigatório o acompanhamento da equipe de infraestrutura ou suporte de TI, garantindo rastreabilidade, controle e mitigação de riscos.
- Todo acesso remoto será registrado, monitorado e auditado periodicamente, visando prevenir acessos indevidos, vazamentos de dados e violações de integridade.
- A duração dos acessos remotos temporários deverá ser limitada, com expiração automática ao término do período autorizado.
- A violação das regras de acesso remoto está sujeita a bloqueio imediato das credenciais e apuração conforme as normas internas citadas no PRS INST GER TI 002 – Controle de Segurança da Informação.

5. PROTEÇÃO DE DADOS E CONFIDENCIALIDADE

As diretrizes sobre o tratamento de dados pessoais são abordadas na Política de Proteção de Dados Pessoais e Privacidade (POL INST SCBH 023), sendo esta Política de Segurança da Informação complementar no que se refere aos requisitos de segurança.

5.1Armazenamento e Compartilhamento

Todas as informações relativos aos controles de armazenamento e compartilhamento estão referenciados no Controle de Segurança da Informação - PRS INST GER TI 002.

- Todas as informações institucionais devem ser armazenadas exclusivamente nos repositórios oficiais da instituição, como o servidor de arquivos, sistemas corporativos (ERP) ou soluções de armazenamento em

nuvem autorizadas pela equipe de TI.

- É terminantemente proibido armazenar dados institucionais em dispositivos externos removíveis, como pen drives, HDs externos, cartões de memória ou similares, exceto em situações excepcionais previamente autorizadas pela equipe de TI, mediante avaliação da real necessidade de uso e análise dos riscos à segurança da informação.
- O compartilhamento de informações deve obedecer aos princípios constantes no item 4.1, garantindo que apenas pessoas autorizadas tenham acesso aos dados. É vedado o envio de informações institucionais para e-mails pessoais ou quaisquer plataformas não autorizadas, a fim de evitar riscos de vazamento, perda ou uso indevido de dados.
- Sempre que possível, o compartilhamento de documentos sensíveis deve ser realizado com proteção por senha e restrição de edição e/ou visualização, utilizando canais seguros definidos pela área de tecnologia.
- Por padrão, nas USB, todas as portas de dispositivos externos dos equipamentos institucionais são bloqueadas automaticamente por meio da solução de antivírus homologada, a qual aplica as diretrizes de segurança definidas pela GPO (Group Policy Object). Eventuais exceções a este bloqueio são autorizadas exclusivamente mediante avaliação da equipe de TI e são gerenciadas por grupo de controle específico, conforme critérios de necessidade e análise de risco à segurança da informação.
- O descumprimento dessas diretrizes poderá resultar em sanções administrativas, responsabilização disciplinar e, quando cabível, encaminhamento às instâncias legais competentes conforme - Política de Proteção de Dados Pessoais e de Privacidade (POL INST SCBH 023).

5.2 Proteção de Dados Pessoais e Sensíveis

- Todas as informações relativas a pacientes e colaboradores são consideradas confidenciais e devem ser protegidas em conformidade com a Lei Geral de Proteção de Dados (LGPD).
- O acesso e uso dessas informações pessoais devem ser restritos exclusivamente a pessoas autorizadas e que possuam necessidade operacional para tal, conforme Política de Proteção de Dados Pessoais e Privacidade (POL INST SCBH 023).

5.3 - Tipos de Informações Geradas e Tratamento

As informações pessoais geradas pela instituição de saúde durante a estadia dos pacientes e usuários operadores são cruciais para garantir a continuidade do cuidado, avaliar a eficácia dos tratamentos e prevenir complicações. Nesse sentido, a natureza dos dados pessoais coletados, as medidas de segurança aplicáveis e a forma de coleta dessas informações devem estar descritos no Aviso de Privacidade, conforme item 4.3 da Política de Proteção de Dados Pessoais e Privacidade.

6. MONITORAMENTO E AUDITORIA

- A Santa Casa BH realiza o monitoramento contínuo do tráfego de e-mails, dos acessos à rede e dos sistemas com o objetivo de assegurar a integridade e a segurança das informações.
- A equipe de Tecnologia da Informação (TI) está autorizada a realizar o monitoramento ativo de colaboradores internos e prestadores de serviço, sem a necessidade de aviso prévio, com o objetivo de identificar potenciais ameaças ou irregularidades. Em situações suspeitas, o acesso a sistemas e equipamentos poderá ser bloqueado imediatamente, até a conclusão de uma apuração detalhada. Ressalta-se que é expressamente necessária a existência de registro na ferramenta de Service Desk - Gestão X do possível acesso realizado.
- Além disso, a equipe de TI poderá conduzir auditorias internas para verificar a conformidade com esta política de segurança da informação.
- O descumprimento das normas estabelecidas poderá acarretar a aplicação de medidas disciplinares e sanções administrativas, conforme previsto nas diretrizes institucionais.

7. GERENCIAMENTO DE INCIDENTES DE SEGURANÇA

- Todo incidente de segurança como tentativas de invasão, vazamento de dados ou acessos não autorizados deve ser reportado imediatamente ao setor de Tecnologia da Informação (TI) para avaliação.
- Em casos que envolvam o comprometimento de dados pessoais e sensíveis, a autoridade competente será notificada conforme as exigências da Lei Geral de Proteção de Dados (LGPD) pelo setor responsável.
- Nos casos de incidentes críticos de segurança, a equipe de TI está autorizada a adotar todas as medidas necessárias para restaurar a normalidade dos serviços, mesmo que essas ações impliquem impacto significativo nas operações. Tais medidas poderão ser executadas de forma imediata e sem aviso prévio.

8. PLANOS DE CONTINGÊNCIA

Com o objetivo de mitigar riscos e assegurar a continuidade das operações, a TI adota as seguintes medidas preventivas e corretivas:

- **Backups Periódicos** realização de cópias de segurança regulares, acompanhadas de testes de restauração para garantir a integridade e disponibilidade dos dados. O processo inclui:
- **Backup incremental**: Executado diariamente em horários distintos, registrando apenas as alterações desde o último backup.
- **Backup completo (full)**: Em geral, os backups são realizados semanalmente em horários distintos,

garantindo uma cópia integral de todos os dados.

- **Proteção contra-ataques cibernéticos:** Implementação de firewalls, soluções antivírus e sistemas de monitoramento contínuo de ameaças.
- **Gerenciamento de acessos:** Monitoramento constante e bloqueio imediato de credenciais suspeitas ou não autorizadas.
- **Redundância de serviços:** A infraestrutura conta com servidores, links de internet e sistemas críticos duplicados para garantir a continuidade das operações em caso de falhas. Além disso, os dados são mantidos com redundância em servidores distintos e plataformas diversas, assegurando maior resiliência e disponibilidade.

9. OS MECANISMOS DE CONTROLE E DOS DESDOBRAMENTOS

Esta política será avaliada periodicamente, por meio de relatórios de resultados, incluindo indicadores, auditorias, pesquisas de satisfação, análise crítica, relatórios de sustentabilidade, conforme mecanismo de controle a ser estabelecido por cada área, visando avaliar a adesão, aplicabilidade e eficácia da diretriz, além de fornecer uma visão abrangente do impacto institucional.

Os processos relativos a esta política serão desdobrados de forma transversalizada, sendo que seu fluxo de aplicação operacional deverá ser detalhado por meio de PRS - Procedimento Sistêmico específico. O monitoramento dos resultados da respectiva política serão mensurados e analisados por meio de instrumento (s) acima referenciado (s), de forma contínua.

Esta política apresenta seus principais desdobramentos por meio dos seguintes documentos:

- PRS INST GER TI 002 - Controle de Segurança das Informações TI;
- PRS INT INF DEC 001 - Solicitação dos serviços prestados pela equipe do setor de Coordenação de Informações Estratégicas;
- POP INFRA SEG INF 001- Backup de Servidores e Sistemas Santa Casa;
- POP INFRA SEG INF 008 - Inventário, Mapeamento e Gestão de Ativos.

10. DESCUMPRIMENTO DA POLÍTICA

Na Santa Casa BH, valorizamos a colaboração para um ambiente íntegro. Caso presencie ou tenha conhecimento de qualquer irregularidade, reúna o máximo de informações e evidências possíveis e denuncie de forma segura pelo site www.ouvidordigital.com.br/santacasabh ou pelo telefone 0800 892 5020. A denúncia pode ser feita anonimamente ou com identificação, de acordo com sua escolha. Sua identidade será

preservada, e a Santa Casa BH não permitirá qualquer tipo de retaliação.

Os envolvidos nos fatos, após o processo de apuração, se comprovada a violação a essa ou a outras Políticas e normas correlatas estarão sujeitos às medidas disciplinares, administrativas e legais cabíveis, conforme previsto: (i) nas regras internas da Santa Casa BH, como no PRS INST CONF CULT 001 – Procedimentos sobre Aplicação de Regras de Consequências; (ii) na legislação aplicável (LGPD, CLT, etc.); e (iii) nos instrumentos contratuais pertinentes, sem prejuízo de eventual responsabilização civil, penal ou administrativa perante as autoridades competentes.

11. DOCUMENTOS DE REFERÊNCIA

ABRADMIN. Regulamentação da Inteligência Artificial no Brasil: desafios e perspectivas na saúde - Abramed. Disponível em: <https://abramed.org.br/5435/regulamentacao-da-inteligencia-artificial-no-brasil-desafios-e-perspectivas-na-saude/>. Acesso em: 20 janeiro 2025.

BRASIL. Autoridade Nacional de Proteção de Dados.Guia de Elaboração de Termo de Uso e Políticas de Privacidade para Serviços Públicos: Lei Geral de Proteção de Dados Pessoais (LGPD). Versão 1.3. Brasília, junho de 2022.

BRASIL. Autoridade Nacional de Proteção de Dados.Guia Orientativo de Cookies e Proteção de Dados Pessoais. Versão 1.0. Brasília, outubro de 2022.

BRASIL. Autoridade Nacional de Proteção de Dados. Modelo com Orientações para Elaboração do Termo de Uso e Políticas de Privacidade. Brasília, 10 de junho de 2022.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011, Lei de Acesso a Informações. Brasília, DF: Presidência da República, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/12527.htm. Acesso em: 27 de janeiro, 2023.

BRASIL, Lei nº 13.709, de 14 de Agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF. Presidência da República, 2018. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/13709.htm Acesso em: 27 de janeiro, 2023.

Cabric M. Confidentiality, Integrity, and Availability. In: Corporate Security Management [Internet]. Elsevier; 2015. p. 185–200. Available from: http://dx.doi.org/10.1016/b978-0-12-802934-3.00011-1.

Código de Ética Médica: Conselho Federal de Medicina (CFM).

Correia A, Gonçalves A, Teodoro MF. A model-driven approach to information security compliance. In: AIP Conference Proceedings [Internet]. Author(s); 2017. p. 020082. Available from: http://dx.doi.org/10.1063/1.4982022.

Galatenko VA, Kostyukhin KA, Levchenkova GL. Integrity as an Aspect of Information Security: an Overview of Modern Approaches. PRIN [Internet]. 2021 Nov 19;12(8):420–4. Available from: http://dx.doi.org/10.17587/prin.12.420-424

ISO/IEC 27001:2013 – Sistemas de Gestão de Segurança da Informação.

ISO/IEC 27002:2013 – Código de boas práticas para segurança da informação.

Lei Geral de Proteção de Dados (LGPD): Lei nº 13.709, de 14 de agosto de 2018.

Martin A, Khazanchi D. Information availability and security policy. 2006.

ONU - Organização das Nações Unidas. Declaração Universal dos Direitos Humanos da ONU. Disponível em: https://www.unicef.org/brazil/declaração-universal-dos.direitos-humanos. Acesso em: 27 de fevereiro, 2023.

Projeto de Lei nº 2338, de 2023: Dispõe sobre o uso da Inteligência Artificial.

PROGRAMA DAS NAÇÕES UNIDAS PARA O DESENVOLVIMENTO (PNUD). Acompanhando a agenda 2030 para o desenvolvimento sustentável: subsídios iniciais do Sistema Nações Unidas no Brasil sobre a identificação de indicadores nacionais referentes aos objetivos de desenvolvimento sustentável/ Programa das Nações Unidas para o Desenvolvimento. Brasília: PNUD, 2015. Disponível em https://brasil.un.org/pt-br/sdgs/10 Acesso em 27 de fevereiro, 2023.

SANTA CASA BH. Estatuto da Santa Casa de Belo Horizonte. Belo Horizonte, 2024. Disponível em: https://santacasabh.org.br/organizacao/. Acesso em: 29 maio 2025.

SANTA CASA BH. Regras Institucionais de Conduta da Santa Casa de Belo Horizonte. Belo Horizonte, 2023. Disponível em: https://santacasabh.org.br/politicas/. Acesso em: 29 maio 2025.

Sunday Adeola Oladosu, Christian Chukwuemeka Ike, Peter Adeyemo Adepoju, Adeoye Idowu Afolabi, Adebimpe Bolatito Ige, Olukunle Oladipupo Amoo. Advancing cloud networking security models: Conceptualizing a unified framework for hybrid cloud and on-premise integrations. Magna Sci Adv Res Rev

[Internet]. 2021 Oct 30;3(1):079–90. Available from: http://dx.doi.org/10.30574/msarr.2021.3.1.0076

Tyagi S, Sirohi P, Khan MY, Darwish A. Industrial Information Security, Safety, and Trust. In: Advances in Civil and Industrial Engineering [Internet]. IGI Global; 2012. p. 20–31. Available from: http://dx.doi.org/10.4018/978-1-4666-0294-6.ch002

12. ANEXOS

Não se aplica.

Elaboração / Revisão	Análise Crítica	Aprovação
Governança Corporativa, demais Gerências e Superintendentes responsáveis Data: 23/10/2025	Comitê Estratégico de Aprimoramento Organizacional - CEAO Data: 28/10/2025	Núcleo de Direção Superior- NDS Data: 12/11/2025