1- INTRODUÇÃO

A segurança e sigilo da informação é um conceito que se relaciona com o ideal de privacidade das informações, isto é, da restrição do acesso. A segurança da informação, nesse ponto, é pensada e implantada para garantir o total sigilo de dados sensíveis, evitando que ações maliciosas possam expor o seu conteúdo e causando prejuízos para as organizações e pessoas.

A lei, que está em vigor no Brasil, tem impacto nas instituições públicas e privadas nacionais, bem como as entidades estrangeiras com sede no país que manipulam dados pessoais, com o objetivo de regulamentar seus processos.

O marco na regulamentação sobre dados pessoais no Brasil é a Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei n. 13.709, de 14 de agosto de 2018, entrando a legislação em vigor em 18 de setembro de 2020. A lei representa um marco histórico na regulamentação sobre o tratamento de dados pessoais no Brasil, tanto em meios físicos quanto em plataformas digitais. Além de mudar a maneira como instituições privadas coletam, armazenam e disponibilizam informações de usuários, a LGPD deve ser seguida por União, Estados, Distrito Federal e Municípios.

Os pontos mais importantes da LGPD é aplicável a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país no qual estejam localizados os dados, desde que a operação de tratamento de dados seja realizada no Brasil; a atividade de tratamento tenha por objetivo a oferta de bens ou serviços ou o manejo de dados de indivíduos localizados no país; ou, ainda, que os dados pessoais objeto do tratamento tenham sido coletados em território nacional.

Entretanto, estão excluídos da aplicação da lei alguns meios de tratamentos de dados, a exemplo daqueles realizados para fins exclusivamente jornalísticos, artísticos e acadêmicos, além de informações relacionadas exclusivamente à segurança pública, defesa nacional, segurança do Estado e a atividades de investigação e repressão de infrações penais.

Segundo a LGPD as empresas devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

A LGPD disciplina que a governança dos dados e a estrutura do armazenamento dos dados quando referente ao poder público, deverão sempre ser pensados e estruturados da melhor forma a execução das políticas públicas e a persecução do interesse público.

Logo, não se trata apenas do nome, mas de uma gama de informações como endereço e até mesmo emprego podem ser considerados como tal quando combinados a cruzamentos de dados arquivados em outros registros.

Existe uma subcategoria nomeada "dados sensíveis", informações que podem gerar formas de discriminação como etnia, convicções religiosas, posicionamentos políticos, orientação sexual e condições de saúde. Esses registros têm maior nível de proteção e não poderão ser considerados relevantes para direcionamentos publicitários, por exemplo, sem o usuário consentir anteriormente. As informações médicas terão acesso ainda mais restritos, e não poderão ser divulgadas por qualquer meio sem o prévio consentimento para pessoa. De modo geral, a ideia é proteger o cidadão do uso abusivo e indiscriminado de seus próprios dados.

Elaborado por:	Misleine Fagundes Jaco	Assinatura:	Data: 13/03/23
Revisado por:	Samuel Silva do Rosário	Assinatura:	Data: 21/03/23
Aprovado por:	Gracio Tomaz saturno	Assinatura:	Data: 29/03/23
Padronizado Por:	Elen Regiane Soares Lopes	Assinatura:	Data: 15/03/23

Esta POLÍTICA DE SEGURANÇA E SIGILO DAS INFORMAÇÕES descreve a informação coletada e como ela será usada.

2- OBJETIVO

A Política de Segurança e Sigilo das Informações tem por objetivo a instituição de diretrizes estratégicas que visam garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações, 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 HABM (Hospital Dr. Adolfo Bezerra de Menezes) contra ameaças e vulnerabilidades. Desse modo, a Política busca preservar os seus ativos de informação, assim como a sua imagem institucional. O propósito da Política é orientar o HABM no que diz respeito à gestão de riscos e ao tratamento de incidentes de Segurança e sigilo das Informações, em conformidade com as disposições constitucionais, legais e regimentais vigentes. Estabelece o comprometimento da alta direção organizacional do hospital, com vistas a prover apoio para a implantação da Gestão dos Riscos de Segurança e sigilo das Informações.

3- APLICABILIDADE

Esta política se aplica a todos os serviços e colaboradores do hospital, sejam aqueles em regime CLT, PJ ou autônomo.

Elaborado por:	Misleine Fagundes Jaco	Assinatura:	Data: 13/03/23
Revisado por:	Samuel Silva do Rosário	Assinatura:	Data: 21/03/23
Aprovado por:	Gracio Tomaz saturno	Assinatura:	Data: 29/03/23
Padronizado Por:	Elen Regiane Soares Lopes	Assinatura:	Data: 15/03/23

Se o titular de dados possuir dúvidas em relação a esta **política**, ele deverá primeiramente entrar em contato com o hospital, utilizando-se do seguinte *e-mail* aux.qualidade@bezerra.org.br .

4- DIRETRIZES

As diretrizes de segurança da informação estabelecidas nesta política aplicam-se às informações armazenadas, acessadas, produzidas e transmitidas pelo HABM, e que devem ser seguidas pelos usuários, incumbindo a todos a responsabilidade e o comprometimento com sua aplicação. Independentemente da forma ou do meio pelo qual a informação seja apresentada ou compartilhada, deverá ser sempre protegida adequadamente, de acordo com esta política. Os recursos de Tecnologia das Informações disponibilizados pelo HABM serão utilizados estritamente para propósito institucional. É vedado a qualquer usuário deste hospital o uso dos recursos de Tecnologia das Informações 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 política constituem os principais pilares da Gestão de Segurança da Informação do HABM, sendo norteadoras da elaboração das normas.

4.1 DIRETRIZES ESPECÍFICAS

a) Gestão da Segurança e Sigilo das Informações

Elaborado por:	Misleine Fagundes Jaco	Assinatura:	Data: 13/09/23
Revisado por:	Samuel Silva do Rosário	Assinatura:	Data: 21/03/23
Aprovado por:	Gracio Tomaz saturno	Assinatura:	Data: 29/03/23
Padronizado Por:	Elen Regiane Soares Lopes	Assinatura:	Data: 15/03/23

Todos os mecanismos de proteção utilizados para a segurança das informações deverão ser mantidos com o objetivo de garantir a continuidade dos serviços do HABM. As medidas de proteção deverão ser planejadas e os gastos da aplicação de controles deverão ser compatíveis com o valor do ativo protegido. Os requisitos de segurança das informações do HABM deverão ser explicitamente citados em todos os termos de compromisso celebrados entre a instituição e terceiros, por meio de cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta política, devendo também ser exigido termo de confidencialidade.

b) Gestão de Tratamento de Incidentes de Segurança em Rede Computacional

A Tecnologia da Informação deverá criar e manter equipe de tratamento e resposta a incidentes em redes computacionais, 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 segurança das informações deverão ser comunicados, registrados e tratados de acordo com um Plano de Gerenciamento de Incidentes específico.

c) Gestão de Riscos, Segurança e Sigilo das Informações

A GRSSI será um conjunto de processos que permitirá identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação do HABM, 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 GRSSI. A GRSSI deverá ser implementada no âmbito do HABM, visando identificar os ativos relevantes e determinar ações de gestão apropriadas, devendo ser atualizada periodicamente, no mínimo 01 (uma) vez a cada 2 anos, ou oportunamente, em função de inventários de ativos, mudanças, ameaças ou vulnerabilidades. Trata-se

de instrumento do programa de Gestão de Riscos que deve incluir um Plano de Continuidade de Serviços (PCS) e um Plano de Gerenciamento de Incidentes (PGI). O Plano de Continuidade de serviços deverá complementar a análise de riscos, visando limitar os impactos do incidente e garantir que as informações requeridas para os processos do negócio estejam prontamente disponíveis. O Plano de Gerenciamento de Incidentes definirá responsabilidades e procedimentos para assegurar respostas rápidas, efetivas e ordenadas perante incidentes de SSI.

d) Gestão de Continuidade dos Serviços

Será um processo abrangente de gestão que identificará ameaças potenciais aos ativos de informação do HABM, assim como possíveis impactos nas operações, caso essas ameaças se concretizem. Portanto, prevê a definição de uma estrutura para que se aprimore a resiliência organizacional, com vistas a responder efetivamente aos incidentes de SSI e minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do hospital, além de recuperar perdas de ativos de informações. As áreas deverão manter processo bem definidos, de modo a não permitir que os serviços 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 na capacidade de atingir os principais objetivos institucionais deve ser prática proativa de todos os titulares das unidades administrativas e assistenciais, de forma a proteger a reputação, a assistência ao paciente e imagem institucional. Todas as áreas do HABM que dependam de recursos de Tecnologia da Informação deverão elaborar, com o apoio da CGSSI, Planos de Gerenciamento de Incidentes, de acordo com o grau de probabilidade de ocorrência de eventos ou sinistros, bem como estabelecer um conjunto de estratégias e procedimentos que deverão ser adotados 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 a disponibilidade dos ativos de informação e a recuperação de atividades críticas à normalidade, com o objetivo de minimizar o impacto de situações inesperadas, desastres, falhas de segurança, entre outras, até que se retorne à normalidade.

e) 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 informações do hospital deverão ser inventariados, com a classificação em termos de valor, requisitos legais, sensibilidade e criticidade da informação para o HABM, e serão atribuídos aos respectivos responsáveis. Seu uso deverá estar em conformidade com os princípios e normas operacionais de SSI, sendo destinados exclusivamente ao uso institucional, vedada a utilização para fins em desconformidade com os interesses do hospital. O usuário deve ter acesso apenas aos ativos necessários e indispensáveis ao seu trabalho, respeitando as recomendações de sigilo, conforme disposto em 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 HABM.

f) Tratamento da Informação

A informação deve ser protegida de forma preventiva, com o objetivo de minimizar riscos às atividades e serviços. Essa proteção deve ser de acordo com o valor, sensibilidade e criticidade da informação, devendo ser desenvolvido, para este fim, sistema de classificação da informação. Os dados, as informações e os sistemas de informação do HABM devem ser protegidos contra ameaças e ações não autorizadas, acidentais

Elaborado por:	Misleine Fagundes Jaco	Assinatura:	Data: 13/03/23
Revisado por:	Samuel Silva do Rosário	Assinatura:	Data: 21/03/23
Aprovado por:	Gracio Tomaz saturno	Assinatura:	Data: 29/03/23
Padronizado Por:	Elen Regiane Soares Lopes	Assinatura:	Data: 15/03/23

ou não, de modo a reduzir riscos e garantir a disponibilidade, integridade, confidencialidade e autenticidade desses bens.

g) Classificação da Informação

Toda informação criada, manuseada, armazenada, transportada ou descartada 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 HABM e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas. As informações sob gestão do hospital devem dispor de segurança, de maneira a serem adequadamente protegidas quanto ao acesso e uso. Para aquelas consideradas de alta criticidade, serão necessárias medidas especiais de tratamento, com o objetivo de limitar a exploração de informações exclusivas da instituição.

h) Monitoramento, Auditoria e Conformidade

O monitoramento, auditoria e conformidade de ativos de informações observarão o seguinte:

- O uso dos recursos de tecnologia da informação disponibilizados pelo HABM é passível de monitoramento e auditoria, devendo ser implementados e mantidos, à medida do possível, mecanismos que permitam a sua rastreabilidade;
- A entrada e saída de ativos de informação do HABM deverá ser registrada e autorizada por autoridade competente mediante procedimento formal;
- A Comissão LGPD manterá registros e procedimentos específicos, tais como trilhas de auditoria e outros que assegurem o rastreamento, acompanhamento, controle e verificação de acessos a todos os sistemas institucionais, à rede interna e à internet;
- A Ouvidoria do HABM será responsável por manter canal de comunicação para recebimento de denúncias de infração a qualquer parte desta política.

Elaborado por:	Misleine Fagundes Jaco	Assinatura:	Data: 13/03/23
Revisado por:	Samuel Silva do Rosário	Assinatura:	Data: 21/03/23
Aprovado por:	Gracio Tomaz saturno	Assinatura:	Data: 29/03/23
Padronizado Por:	Elen Regiane Soares Lopes	Assinatura:	Data: 15/03/23

i) Controle de Acesso e Uso de Senhas

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

j) uso de e-mail

O correio eletrônico é um recurso de comunicação institucional do HABM e as regras de acesso e utilização do e-mail devem atender a todas as orientações desta política e das normas específicas.

l) 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 política, e demais orientações governamentais e legislação em vigor.

m) 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 HABM, deve ser regida por normas internas especificas e deve estar em consonância tanto com a política quanto com os objetivos estratégicos da instituição.

n) Propriedade Intelectual

As informações produzidas por usuários internos e colaboradores, no exercício de suas funções, são patrimônio intelectual do HABM e não cabe a seus criadores qualquer forma de direito autoral, ressalvado o direito de autoria, quando for o caso. É vedada a utilização de patrimônio intelectual do HABM em quaisquer projetos ou atividades de uso diverso do estabelecido pela instituição, salvo autorização específica.

Elaborado por:	Misleine Fagundes Jaco	Assinatura:	Data: 13/03/23
Revisado por:	Samuel Silva do Rosário	Assinatura:	Data: 21/03/23
Aprovado por:	Gracio Tomaz saturno	Assinatura:	Data: 21/03/23
Padronizado Por:	Elen Regiane Soares Lopes	Assinatura:	Data: 15/03/23

o) Contratos, Convênios, Acordos e Instrumentos Congêneres

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

p) 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 política, e demais orientações governamentais e legislação em vigor, com vistas a garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações armazenadas na nuvem, em especial aquelas sob custódia e gerenciamento de prestador de serviço.

q) Uso de Dispositivos Móveis

As diretrizes gerais de uso de dispositivos móveis para acesso às informações, sistemas, aplicações e e-mail do HABM devem considerar, prioritariamente, os requisitos legais e a estrutura da instituição, atendendo a esta política, e deverão ser regidas por normas específicas, as quais contemplarão recomendações sobre o uso desses dispositivos.

r) Informações de prontuário médico

As informações contidas em prontuário médico são de propriedade do paciente, sendo somente ele o autorizado a solicitar impresso. Durante a internação o responsável pela internação, o familiar que assina a responsabilidade pela internação em termo de internação, poderá receber informações sobre as condições do paciente, devendo

vir pessoalmente e receber todas as informações pelo médico assistente. Nenhuma pessoa poderá receber informações por telefone sem identificação ou que não seja responsável pelo paciente. Em algumas situações onde o paciente é curatelado ou menor de idade, o responsável, por ele, poderá requerer prontuário impresso com a identificação da responsabilidade, conforme lei vigentes.

5- NOTIFICAÇÃO DE ALTERAÇÕES

Em caso de alteração na política, quando novos serviços são adicionados ou incorporados por algum motivo justificável. Caso o hospital queira utilizar ou divulgar a informação pessoais sensível do titular de dados em situação materialmente diferente daquela que se iniciou ao tempo que foi coletada a informação, o titular dos dados terá uma escolha a fazer, se permite ou não a utilizar ou divulgar sua informação nesta nova situação. Qualquer mudança material será somente efetivada após o fornecimento por *e-mail* com, no mínimo, 30 dias de antecedência e autorização expressa do titular dos dados.

O hospital disponibilizará a emenda da política no site, para que o titular de dados possa sempre acessar a informação nova e como ela será usada e divulgada. Deverão acessar e conferir o site do hospital no endereço www.bezerra.org.br , a qualquer tempo para versões mais atualizadas.

6- POLÍTICA DE USO

Elaborado por:	Misleine Fagundes Jaco	Assinatura:	Data: 13/03/23
Revisado por:	Samuel Silva do Rosário	Assinatura:	Data: 21/03/23
Aprovado por:	Gracio Tomaz saturno	Assinatura:	Data: 29/03/23
Padronizado Por:	Elen Regiane Soares Lopes	Assinatura:	Data: 15/03/23

O Hospital pode emendar esta política a qualquer tempo, o que será disponibilizado os termos emendados em seu site, que passam a vigorar após 30 (trinta) dias de sua postagem.

Qualquer pessoa poderá acessar o site do hospital e ler a política disponível e atualizada.;

7- VIOLAÇÕES DA POLÍTICA

Constitui violações a política, às normas ou aos procedimentos de segurança da informação as seguintes situações:

- Quaisquer ações ou situações que exponha o hospital, incluindo imagem, ou seus parceiros e pacientes à perda financeira e de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação;
- Utilização indevida de dados do hospital, divulgação não autorizada de informações médicas, segredos comerciais ou outras informações sem a permissão expressa do hospital;
- Uso de dados, informações, equipamentos, *software,* sistemas ou outros recursos tecnológicos, para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, da ética ou de exigências de organismos reguladores da área de atuação do hospital ou de seus parceiros e clientes;

Os colaboradores e usuários dos serviços hospitalares compreende que, se usar os dados do hospital de maneira que viole esta política, poderá incorrer em substancial responsabilidade e/ou sofrer danos significativos, incluindo-se (sem limitação) multas e outras despesas relacionadas a procedimentos e serviços. Em ocorrendo tais fatos, o

infrator concorda em reembolsar ao hospital por quaisquer custos, despesas e multas a ela atribuídas pelas suas ações e omissões cometidas em detrimento desta política.

O hospital, pessoa jurídica, é responsável pelo cadastramento dos seus colaboradores no sistema, bem como as atividades desenvolvidas por todos eles no uso dos serviços.

O hospital é responsável por todos os atos cometidos pelos demais colaboradores, cadastrados no sistema do DGP (departamento de gestão de pessoas), e quaisquer violações à política será notificado pelo titular dos dados, através do e-mail cadastrados nesta política, e não resolvendo os problemas de violações em até 7 (sete) dias da notificação, o problema será encaminhado ao jurídico e administração para medidas cabíveis.

8- TÉRMINO E FECHAMENTO DE ACESSO

O colaborador do hospital não poderá utilizar o fechamento de seu acesso como meio para evitar uma investigação, caso esteja pendente no momento do fechamento da conta. O hospital poderá continuar a manter ativo seu acesso e arquivos por até 180 (cento e oitenta) dias, a fim de proteger os demais usuários e o sistema de riscos e contratempos.

O colaborador permanecerá responsável por todas as obrigações relacionadas seus acessos, mesmo após sua demissão. Se o titular dos acessos (colaborador) não acessar a sua conta num período de 6 meses, ela será encerrada.

Ao fim do contrato de trabalho o DGP deverá desativar as senhas dos usuários colaboradores do hospital, a fim de não fornecer acessos aos desligados.

Elaborado por:	Misleine Fagundes Jaco	Assinatura:	Data: 13/03/23
Revisado por:	Samuel Silva do Rosário	Assinatura:	Data: 21/03/23
Aprovado por:	Gracio Tomaz saturno	Assinatura:	Data: 29/03/23
Padronizado Por:	Elen Regiane Soares Lopes	Assinatura:	Data: 15/03/23

9. DEVER LEGAL

O hospital deverá cumprir com todas as leis aplicáveis, estatutos, ordenamentos, regulamentos, contratos e licenças relacionadas com o uso dos serviços.

a) Informações Coletadas

- Informações requeridas

Para abrir um atendimento, os titulares de dados, bem como os colaboradores do hospital, poderão fornecer nome, CPF, número de telefone e *e-mail*, dentre outras informações, desde que o hospital requeira estas informações por requisitos legais. Para realizar pagamentos, se for o caso, o titular de dados deverá fornecer o seu cartão de crédito ou cartão de débito, em caso de pacientes após o uso dos serviços particulares, que não serão registrados em nossos servidores. Já os colaboradores deverão fornecer dados bancários para recebimentos de salários, que serão registrados em nossos servidores.

Visando garantir a segurança da senha de acesso ao perfil, em uso dos sistemas do hospital, os colaboradores que estarão registrando informações deverão ter sua senha de acesso individual, intransferível e só de conhecimento do próprio. Estas informações requisitadas serão necessárias para prosseguir os atendimentos ou cadastros, também deverá contatar no termo inicial sobre a necessidade das informações. Tais medidas visam protege-lo contra fraude.

b) Segurança da Informação

O HABM está empenhado em resguardar a informação pública e sigilosa do titular de dados com altos padrões de segurança. O HABM autoriza o acesso à sua informação pública para as empresas parceiras, empregados e outros que necessitam saber dela, a fim de providenciar produtos e serviços. O HABM mantém salvaguardas

físicas, eletrônicas e procedimentais que estão de acordo com as regulamentações constitucionais e legais para guarda de dados pessoais. O HABM testa os sistemas de segurança regularmente e também contrata outras companhias para auditar nossos sistemas de segurança e processos.

A segurança do acesso dos colaboradores do HABM também assenta na proteção de sua senha. O titular não pode dividir sua senha com outros.

Qualquer *e-mail* ou outra comunicação solicitando o fornecimento de informação pessoal via *e-mail* ou *linking* a um sítio com uma URL, deve ser tratada como não autorizada e suspeita, devendo ser notificada o HABM imediatamente no setor de tecnologia da informação. Se o titular dos acessos compartilhar sua (s) senha (s) dos sistemas do HABM com terceiros poderá ser responsabilizado por ações tomadas no uso de sua senha. Se o titular acreditar que alguém obteve acesso à sua senha, deverá mudar imediatamente, e comunicar o setor de tecnologia da informação.

c) Mudança das Informações do Titular de Acessos

O titular pode revisar a informação pessoal por ele fornecida e fazer quaisquer mudanças desejadas sobre ela, a qualquer tempo ao acessá-la. para tanto, deverá solicitar via DGP ou T.I., se o titular de dados fechar seu acesso no HABM todas as informações fornecidas nos sistemas do HABM permanecerão conforme legislação.

10. PENALIDADES

Ações que violem esta política ou quaisquer de suas diretrizes, normas ou procedimentos, ou que infrinjam os controles de Segurança e Sigilo das Informações serão devidamente apuradas, sendo aplicadas aos responsáveis as sanções penais, administrativas e civis cabíveis. O usuário responderá disciplinarmente e/ou civilmente pelo

Elaborado por:	Misleine Fagundes Jaco	Assinatura:	Data: 13/03/23
Revisado por:	Samuel Silva do Rosário	Assinatura:	Data: 21/03/23
Aprovado por:	Gracio Tomaz saturno	Assinatura:	Data: 20/03/23
Padronizado Por:	Elen Regiane Soares Lopes	Assinatura:	Data: 15/03/23

prejuízo que vier a ocasionar à instituição, podendo culminar com o seu desligamento e, se aplicáveis eventuais processos criminais.

11. PROCEDIMENTOS OPERACIONAIS PADRÃO

a) Utilização de dados em cadastros e termos;
b) Compartilhamento de informações com rede de atenção psicossocial;
c) Compartilhamento de dados pessoais de colaboradores aos convênios de benefícios;
d) Utilização de imagens de colaboradores e pacientes;
e) Compartilhamento de informações de prontuário médico;
f) Fornecimentos e descredenciamentos de senhas de acessos aos sistemas operacionais do hospital;
g) Utilização de e-mail, redes sociais e internet de propriedade institucional;
h) Tratamento das informações;
i) Classificação das informações do hospital;
j) Monitoramento, auditoria e conformidade de ativos de informações;
k) Computação em nuvem;
l) Sistema de segurança das informações.

Elaborado por:	Misleine Fagundes Jaco	Assinatura:	Data: 13/03/23
Revisado por:	Samuel Silva do Rosário	Assinatura:	Data: 21/03/23
Aprovado por:	Gracio Tomaz saturno	Assinatura:	Data: 29/03/23
Padronizado Por:	Elen Regiane Soares Lopes	Assinatura:	Data: 15/03/23