Sumário

1. OBJETIVO

Trazer princípios, orientações e diretrizes relacionadas a Segurança da Informação da Elosaúde a fim de reforçar e garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a realização do negócio da Organização.

O conteúdo desta Política deve ser interpretado e cumprido em conjunto com as diretrizes presentes no Estatuto, Código de Ética e Conduta, Políticas, Regulamentos e demais normativos internos aplicáveis.

2. ABRANGÊNCIA

Esta política aplica-se a todos os administradores (Diretores, membros do Conselho Deliberativo e Conselho Fiscal), colaboradores da Elosaúde, bem como, por todos os seus respectivos participantes e prepostos a eles vinculados, considerando suas necessidades específicas e os aspectos legais e regulamentares a que estão sujeitas. O cumprimento desta Política também é obrigatório a todos os terceiros e prestadores de serviços.

3. DEFINIÇÕES

Backup: Cópia de segurança. O termo em inglês é muito utilizado por empresas e pessoas que guardam documentos, imagens, vídeos e outros arquivos no computador ou na nuvem.

Compliance: Estar em conformidade com a legislação, as regulamentações, as normas e procedimentos, externos e internos, e com os princípios de nossa Instituição que garantem as melhores práticas de mercado e de Governança Corporativa.

Integridade: Característica da pessoa que é íntegra, incorruptível. Refere-se àquele cujos comportamentos ou ações demonstram honestidade, imparcialidade, que atua de forma correta e justa, honra os seus compromissos e que tem nobreza moral. A integridade deve ser demonstrada em ações que venham coibir, prevenir e auxiliar na detecção de atos ilícitos, fraude, lavagem de dinheiro, suborno, corrupção, desvios de conduta ou qualquer comportamento considerado inadequado envolvendo as partes com as quais a ELOSAUDE se relaciona.

Informação: Resultado do processamento, manipulação e organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (pessoa, máquina) que a recebe. Genericamente, o conceito de informação está intimamente ligado às noções de restrição, comunicação, controle, dados, forma, instrução, conhecimento, significado, estímulo, padrão, percepção e representação de conhecimento.

GNI: Sigla para a gerência Gestão de Negócio, Inteligência e Inovação que compõe a hierarquia da ELOSAUDE.

Governança Corporativa e Compliance: Estrutura que compõe, mas não se limite a Governança, Risco e Compliance.

Hardware: Palavra de origem inglesa que, no âmbito da informática, é utilizada para designar a parte física de um computador. São todos os componentes palpáveis de um dispositivo eletrônico, como placas, memória, processador, teclado, monitor, etc. Não se limita apenas ao computador, referindo-se também a itens físicos que compõem celulares, tablets, televisores entre outros aparelhos.

LGPD – Lei Geral de Proteção de Dados: A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, dispõe sobre qualquer tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade, estabelecendo regras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, cobrando mais proteção sobre os dados e impondo penalidades em caso de descumprimento.

Segurança da Informação: Está relacionada com proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade (não repúdio), não estando esta segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento. O conceito se aplica a todos os aspectos de proteção de informações e dados.

Software: Conjunto de componentes lógicos de um computador ou sistema de processamento de dados; programa, rotina ou conjunto de instruções que controlam o funcionamento de um computador; suporte lógico.

TI: A Tecnologia da Informação (ou, em inglês, Information Technology — IT) pode ser definida como o conjunto de todas as atividades e soluções providas por recursos computacionais que visam permitir a obtenção, o armazenamento, a proteção, o processamento, o acesso, o gerenciamento e o uso dos dados e das informações.

VPN (Virtual Private Network): Sigla, em inglês, para “Rede Virtual Privada” e que, como o nome diz, funciona criando uma rede de comunicações entre computadores e outros dispositivos que têm acesso restrito a quem tem as credenciais necessárias.

4. DIRETRIZES

Considera-se como Segurança da Informação a preservação de sua autenticidade, confidencialidade, integridade, disponibilidade, irretratabilidade e legalidade da Elosaúde, a violação desta política de segurança é qualquer ato que:

- Exponha a Instituição a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados /ou de informações ou ainda da perda de equipamento;
- Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos;
- Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental ou mesmo interno.

5. GOVERNANÇA DE TECNOLOGIA

Todas as áreas da Elosaúde devem inteirar-se das melhores práticas de gestão de TI e dar suporte à área de GNI, com recursos e informações necessárias ao bom desempenho dos processos de gestão. A área de GNI deve garantir que recursos de hardware e software, para suportar serviços críticos, tenham características básicas de contingência e redundância, tais como:

- Fontes redundantes de energia, interfaces de rede múltiplas e conectadas em portas de rede alternativas;
- Processo de cópia de segurança (backup) estruturado, implantado e monitorado;

- Processo de gestão de incidentes e desempenho estruturado, implantado e monitorado. Manter e disponibilizar contingência de recursos críticos para a continuidade do negócio, bem como aqueles necessários à continuidade da gestão da GNI na ocorrência de eventos adversos. Servidores, equipamentos de rede e segurança críticos ao negócio devem ser adquiridos e implementados com capacidades próprias de contingência, tais como fontes redundantes, placas de rede alternativas, memória com correção de erros, processadores duplos, placas controladoras e sistemas em alta disponibilidade, sempre considerando a relação custo/benefício. No caso da contratação de serviços de infraestrutura de TI em nuvem, os mesmos requisitos são aplicáveis. A arquitetura de processamento para serviços críticos deve ser analisada e validada quanto aos requisitos de contingência e continuidade. Garantir que toda documentação dos sistemas, topologia e inventário, esteja atualizada e divulgada.

6. CONTROLE DE ACESSO LÓGICO E FÍSICO

O acesso às informações e sistemas da Elosaúde deve ser autorizado de acordo com as atividades atribuídas ao cargo ou função exercida, designados como perfil de usuário – Gestão de Perfis. Os privilégios de acesso, determinado por estes perfis, atribuídos para os usuários devem ser revistos periodicamente pelos gestores das áreas. Ficará também a cargo dos gestor de cada área a definição de acessos físicos às áreas da Elosaúde, devendo as liberações serem autorizadas conforme procedimento interno. Todos os entes vinculados à Elosaúde, devem possuir uma única identificação de usuário relacionada às suas atribuições ou funções em exercício no contrato de trabalho ou de prestação de serviço. Os privilégios e direitos de acesso devem ser atribuídos de acordo com as atribuições ou funções em exercício no contrato de trabalho ou de prestação de serviço. A Elosaúde dispõe de procedimentos pré-estabelecidos para os níveis de acessos que cada usuário poderá ser incluído, sejam eles físicos ou eletrônicos. É responsabilidade da GNI validar e aplicar mecanismos de autenticação atrelados ao domínio de rede, bem como delimitar o desenvolvimento e aquisição de sistemas considerando os requisitos mínimos de autenticação definidos nesta política.

Todos os compartilhamentos de rede serão autorizados no ato da execução de criação de usuário de acordo com o setor de cada usuário, no entanto, se houver necessidade de que sejam ainda adicionadas outras pastas de arquivos no compartilhamento de rede, estas deverão ser especificadas na solicitação de acesso.

Acesso às pastas não pertinentes à função e área do colaborador serão passíveis de verificação e remoção de autorização prévia pela área de GNI.

7. CLASSIFICAÇÃO DA INFORMAÇÃO

É de responsabilidade do gestor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com a tabela abaixo:

1 – Pública

2 – Interna

3 – Confidencial

4 – Restrita

Conceitos:

Informação Pública: É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral;

Informação Interna: É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização;

Informação Confidencial: É toda informação que pode ser acessada por usuários da Organização e por parceiros da organização. A divulgação não autorizada desta informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da Organização ou ao negócio do parceiro;

Informação Restrita: É toda informação que pode ser acessada somente por usuários da Organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada desta informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

Todo gestor deve orientar seus colaboradores a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

8. DADOS PESSOAIS DE FUNCIONÁRIOS

A Elosaúde se compromete em não acumular ou manter intencionalmente dados pessoais de funcionários além daqueles relevantes na condução do seu negócio. Todos os dados pessoais de funcionários são considerados dados confidenciais e sob a responsabilidade da Instituição não serão usados para fins diferentes daqueles para os quais foram coletados.

Os dados pessoais de funcionários não serão transferidos para terceiros, exceto quando exigido pelo negócio, e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, neste caso a lista de endereços eletrônicos (e-mails) usados pelos funcionários da Elosaúde.

9. SENHAS

É proibido o empréstimo e o compartilhamento de identificação de usuários e senhas associadas a qualquer tipo acesso às informações, sistemas e equipamentos da Elosaúde, sujeito às sanções.

Os colaboradores, clientes, fornecedores e terceiros devem escolher sempre um mínimo de 8 (oito) caracteres alfanuméricos para formação da sua senha. É responsabilidade da área de TI garantir configurações no(s) domínio(s) de controle para assegurar a construção de senhas fortes, aplicação de histórico e expiração automática das senhas.

Quando o usuário suspeitar de utilização indevida de sua(s) senha(s), deverá alterá-la(s) imediatamente e tratar a situação como um incidente de segurança, reportando ao seu superior imediato, o qual deverá comunicar à área de GNI. As senhas não devem ser armazenadas de forma compreensível (leitura) em código fonte, scripts, macros e papel para evitar a divulgação e uso indevido destas.

Todas as estações de trabalho da Elosaúde devem utilizar proteção de tela (screensaver) previamente homologada pela área de GNI e com ação automática de execução da proteção a partir de 10 (dez) minutos de inatividade destas, devendo o usuário digitar o login e senha para acessar novamente seu computador.
É responsabilidade da área de GNI configurar padrões nos diversos domínios para assegurar a utilização de proteção de tela. É vedado a qualquer usuário a remoção das configurações de proteção de tela da estação de trabalho. Deve-se, ao fim de sua jornada desligar a sua estação de trabalho.

Os colaboradores da Elosaúde devem evitar o uso de mecanismos e software para salvar automaticamente senhas de acesso a sistemas e sites, salvo se devidamente homologados e aprovados pela área de GNI.

10. CÓPIAS DE SEGURANÇA E CONTINGÊNCIA

Todas as informações críticas de negócio da Elosaúde devem possuir cópia de segurança *(backup)* realizada de acordo com planejamento associado à criticidade da informação para o negócio. É responsabilidade da área de GNI providenciar os recursos físicos e lógicos para armazenamento e restauração das cópias de segurança. Também deve assegurar que cópias estejam presentes em locais físicos diferentes do local de origem da informação e devidamente acondicionadas.

É responsabilidade do proprietário da informação definir os requisitos mínimos de salvaguarda da informação, tais como periodicidade da cópia. As cópias de segurança devem ser verificadas sistemicamente para assegurar o processo de restauração.

É responsabilidade da área de GNI prover os recursos necessários e realizar a restauração das cópias de segurança regularmente. O processo de restauração das informações críticas armazenadas em cópias de segurança é responsabilidade exclusiva da área de GNI. A restauração da informação deverá ser solicitada formalmente a esta área pelo proprietário da informação.

11. DESENVOLVIMENTO DE SOFTWARE

O processo de desenvolvimento e aquisição de novos sistemas deve considerar as melhores práticas de segurança da informação. Estas práticas devem ser atualizadas, discutidas e disseminadas na Elosaúde. É responsabilidade da área de GNI garantir a disseminação e aplicação de melhores práticas para desenvolvimento seguro.

Aquisição e implantação de novos sistemas devem considerar a verificação de requisitos mínimos de segurança da informação e seguir o procedimento de segurança desde a concepção. A definição destes requisitos e a atualização do procedimento é de responsabilidade da área de GNI e Compliance, a verificação do emprego e uso adequado destes requisitos é da área de GNI. A Política de Segurança da Informação deve fazer parte como anexo de qualquer contrato envolvendo a aquisição e uso de novos sistemas. O fornecedor proponente deverá atender as condições estabelecidas neste documento para garantir a integridade, disponibilidade e confidencialidade das informações. É mandatória a comprovação de melhores práticas de desenvolvimento seguro, realização de análise de vulnerabilidades e mapa de riscos de Segurança da Informação, para as soluções e sistemas a serem adquiridos ou desenvolvidos externamente. Os sistemas devem apresentar recursos para controle de acesso lógico segregado e robusto, logs de acessos, bem como capacidade para a execução e verificação de trilhas de auditoria. É responsabilidade da GNI, classificar os fornecedores e apresentar ao setor de Compliance a matriz de decisão técnica com aspectos, requisitos de Segurança da Informação e classificação de risco para ele.

12. GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E CONTINUIDADE

A área GNI é responsável pela gestão de Incidentes de Segurança da Informação, pelo gerenciamento e manutenção de seus registros, bem como aplicar melhores práticas para contenção e resolução de causa raiz. É responsabilidade também gerenciar os riscos relacionados à Política de Segurança e Informação, comunicar possíveis alterações no cenário e impactos imediatos. A realização de análise de vulnerabilidades e testes de invasão periódicos deve ser prática de responsabilidade da GNI, informada e acompanhada pela área de Compliance.

O gerenciamento do(s) banco(s) de dados é responsabilidade exclusiva da GNI, assim como a manutenção, alteração e atualização de equipamentos e programas.

13. CONFORMIDADE

A aderência e o cumprimento desta Política está diretamente associada aos requisitos da Resolução Normativa da ANS no 452 de 2020 de 09 de março de 2020.

Os requisitos da Lei Geral de Proteção de Dados (LGPD) no 13.709 de 2018 e a Política de Proteção de Dados devem ser observados por todos os colaboradores visando preservar a privacidade do titular de dados pessoais. Em nenhum caso, o colaborador poderá vender ou transferir informações da Elosaúde ou de responsabilidade desta a terceiros, ou fornecer acesso a elas sem a autorização formal e prévia [DE QUEM]. A confidencialidade e sigilo de dados pessoais devem ser observados, preservados e garantidos por todos os colaboradores, prestadores e terceiros da Elosaúde.

14. USO DE E-MAIL

O correio eletrônico é um recurso de comunicação institucional da Elosaúde e as regras de acesso e utilização do e-mail devem atender a todas as orientações desta Política, além das demais diretrizes da Política de Proteção de Dados. Portanto fica proibido o uso de compartilhamento de informações da Elosaúde com e-mail pessoal.

As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem da organização, não podem ser contrárias à legislação vigente e nem aos princípios éticos da organização.

O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço.

É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias ou linguagem ofensiva;
- Possam trazer prejuízos a outras pessoas;
- Sejam hostis ou inúteis;
- Sejam relativas a “correntes”, de conteúdos pornográficos ou equivalentes;
- Possam prejudicar a imagem da organização;

- Possam prejudicar a imagem de outras organizações;
- Sejam incoerentes com as políticas da organização.

A utilização do e-mail deve ser criteriosa, evitando que o sistema fique congestionado, em caso de congestionamento no sistema de correio eletrônico o setor de GNI fará auditorias no servidor de correio e/ou nas estações de trabalho dos usuários, visando identificar o motivo que ocasionou o mesmo.

15. USO DE INTERNET

A Internet é uma ferramenta de trabalho para o desenvolvimento de atividades, processos, pesquisas, tecnologias e competências. A Elosaúde mantém regras de utilização e bloqueio de acesso a determinados sites que não contenham informações que agreguem conhecimento profissional e/ou para o negócio não devem ser acessados.

A Instituição não autoriza a utilização dos meios de comunicação para divulgar mensagens com conteúdo ilegal, pornográfico, com qualquer sentido discriminatório, de cunho religioso, político-partidário, ideológico ou em desacordo com os princípios éticos e morais da Elosaúde.

O uso da Internet será monitorado pelo setor da GNI, inclusive através de “logs” (arquivos gerados no servidor) que informam qual usuário está conectado, o tempo que usou a Internet e qual página acessou. A definição dos colaboradores que terão permissão para uso (navegação) da Internet é atribuição do gestor de cada área.

Não é permitido instalar programas provenientes da Internet nos computadores da organização, sem expressa anuência da GNI.

16. USO DAS REDES SOCIAIS

A utilização de perfis institucionais mantidos em redes sociais com o objetivo de prestar atendimento e serviços, divulgando ou compartilhando informações da Elosaúde, com autorização previamente constituída pelas áreas de gestão, deve ser regida pelo Código de Ética e Conduta e deve estar em consonância tanto com esta política quanto com os objetivos estratégicos da Instituição.

A Elosaúde não permite a divulgação de imagens da Instituição, de suas instalações e de colaboradores identificados com crachás e/ou uniformizados, bem como o compartilhamento de informações confidenciais e restritas, pessoais ou sensíveis em sites pessoais, redes sociais, aplicativos ou qualquer meio de comunicação sem o consentimento da Elosaúde. Não é autorizada a exposição de imagem dos nossos clientes, a não ser que seja necessário e aprovado por escrito pela pessoa e pela Elosaúde. Também não é permitida a divulgação de informações inverídicas de qualquer natureza em qualquer meio de comunicação. Ao cadastrar no perfil das redes sociais, que é um colaborador da Elosaúde, o profissional não deve realizar qualquer ação que impacte a marca ou contrarie os valores de nossa Instituição.

17. 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 atender as determinações desta Política, e a Política de Proteção de Dados, com vista a garantir a disponibilidade, integridade, confidencialidade, irretratabilidade e autenticidade das informações armazenadas na nuvem.

18. USO DE DISPOSITIVOS MÓVEIS

As diretrizes gerais de uso de dispositivos móveis para acesso às informações, sistemas, aplicações e e-mail devem considerar, prioritariamente, os requisitos legais e a estrutura da Instituição, atendendo a esta Política de Segurança da Informação e a Política de Proteção de Dados.

19. USO DE COMPUTADORES DE PROPRIEDADE DA ORGANIZAÇÃO

Os usuários que tiverem direito ao uso de computadores pessoais (laptop ou notebook), ou qualquer outro equipamento computacional, de propriedade da organização, devem estar cientes de que:

- Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais;
- A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário;

- É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo;
- O usuário não deve alterar a configuração do equipamento recebido.

Alguns cuidados que devem ser observados fora do trabalho:

- Mantenha o equipamento sempre com você;
- Atenção em hall de hotéis, aeroportos, aviões, táxi e etc.
- Quando transportar o equipamento em automóvel utilize sempre o porta malas ou lugar não visível;
- Atenção ao transportar o equipamento na rua.

Em caso de furto:

- Registre a ocorrência em uma delegacia de polícia;
- Comunique ao seu superior imediato e GNI, enviando uma cópia da ocorrência registrada.

20. SISTEMA DE TELECOMUNICAÇÕES

O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos da organização, assim como, o uso de eventuais ramais virtuais instalados nos computadores, é responsabilidade do setor de GNI, de acordo com as definições do gestor de cada área.

21. PASTA DE REDE

Informações relacionadas ao negócio da Elosaúde não devem estar armazenadas em estações de trabalho e equipamentos móveis, tais como laptops, celulares e tablets, devem ser armazenadas em diretórios de rede para que o processo de cópia de segurança seja assegurado. É responsabilidade dos colaboradores garantir que estas informações estejam em diretórios de rede.

22. ANTIVIRUS

Toda estação de trabalho e servidor deve possuir antivírus (software) instalado e atualizado automaticamente. É responsabilidade da área da GNI assegurar o processo de controle de malware na Elosaúde.

É responsabilidade do colaborador comunicar à área de GNI a correta atualização da ferramenta bem como comportamentos associados a malwares em suas estações de trabalho.

O uso de dispositivos do tipo “mídia removível” (pendrives, discos externos e smartphones) é expressamente proibido e as exceções devem ser autorizadas formalmente pela GNI.

Os controles de segurança da informação devem ser empregados pela TI coibindo o uso não autorizado, garantindo o bloqueio de malwares, e utilização de dispositivos removíveis.

O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

23. AUDITORIA E PENALIDADES

A Elosaúde reserva o direito para si de monitorar e manter registros de todos os tipos de acesso aos seus sistemas, redes e informações. Incluindo-se o uso particular (pessoal) através destes recursos, quando da existência de informações e/ou evidências de atos ilícitos ou conduta inadequada. Estes registros também podem ser utilizados para análises estatísticas visando a boa prestação de serviços e para verificação em casos relacionados a incidentes de segurança.

Auditorias internas e investigações podem ser executadas sem aviso prévio, para a verificação do atendimento das considerações que compõe e suportam esta política. Ações disciplinares resultantes da violação dos requisitos e diretrizes de Segurança da Informação serão tratadas conforme Política de Compliance e Integridade, bem como normativos internos, Política de Privacidade e Política de Proteção de dados, após realização de parecer elaborado pela GNI e Compliance.

24. DISPOSIÇÕES GERAIS

É competência da estrutura de GRC e GNI, em conjunto com a Superintendência da Elosaúde, alterar esta Política, sempre que necessário.

Esta Política entra em vigor na data de sua aprovação pela Diretoria Executiva e Conselho Deliberativo e revoga quaisquer normas e procedimentos em contrário.

25. REFERÊNCIAS

- ABNT NBR ISO/IEC 27001 –tecnologia da informação –técnicas de segurança – sistema de gestão de segurança da informação -requisitos.
- ABNT NBR ISO /IEC 31001 –gestão de riscos –técnicas para o processo de avaliação de riscos. • ABNTNBR ISO /IEC 27002 –tecnologia da informação – técnicas de segurança –código de prática para a gestão da segurança da informação.
- ABNT NBR ISO /IEC 27005 –tecnologia da informação –técnicas de segurança – gestão de riscos de segurança da informação.
- ABNT NBR 15999-1:2007 -gestão da continuidade de negócios –parte 1: código de prática. Resolução Normativa da ANS no 452/2020 de 09 de março de 2020, em especial ao Anexo I – Seção 1.5 Política de Segurança e Privacidade das Informações.
- LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Lei Geral de Proteção de Dados.
- Lei nº 12.965, de 23 de abril de 2014.Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

26. ANEXOS

Não aplicável.

27. HISTÓRICO DE REVISÕES

Identificação das Alterações		
Revisão	**Data da revisão**	**Alterações efetuadas**
00	01/12/2022	Implementação

Áreas envolvidas	Validação	Data
Conselho Deliberativo	Política aprovada em reunião pela Conselho Deliberativo	19/12/2022