

 GESTÃO EM SAÚDE	POLÍTICA INSTITUCIONAL		
	SEGURANÇA DA INFORMAÇÃO		
	Setor/Área:	Código:	Versão:
	Presidência	PL-06	02

1 OBJETIVO

Estabelecer diretrizes para a gestão, proteção e uso seguro das informações da organização, assegurando sua confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade, de forma a apoiar os processos administrativos, assistenciais e estratégicos, promover a continuidade das operações, reduzir riscos relacionados à informação e garantir a conformidade com a legislação vigente e demais requisitos regulatórios.

2 APLICAÇÃO

Esta Política compõe o Programa de Integridade da S3 Gestão em Saúde, sendo aplicável a todos os integrantes, colaboradores, terceiros e parceiros, dirigentes e gestores, sendo extensivo, no que couber, a doadores e patrocinadores.

Devem cumpri-la obrigatoriamente:

- Colaboradores da S3, independentemente do tipo de vínculo (efetivos, temporários, estagiários, aprendizes ou voluntários);
- Fornecedores, prestadores de serviço, consultores e terceiros, cujas atividades envolvam o acesso, uso, armazenamento ou qualquer forma de tratamento de dados pessoais em nome da instituição;
- Profissionais de saúde, educadores, técnicos, gestores e equipes multiprofissionais que atuem nas unidades sob responsabilidade da S3;
- Parceiros institucionais e organizações associadas, no âmbito das relações contratuais ou de cooperação técnica que envolvam o compartilhamento de dados;
- Usuários, pacientes, estudantes e participantes de programas, projetos ou serviços oferecidos ou executados pela S3, no que se refere ao tratamento de seus próprios dados e ao exercício de seus direitos como titulares.

3 BASE LEGAL

Esta Política fundamenta-se na legislação brasileira, nas boas práticas de governança da informação e nas normas técnicas aplicáveis à segurança da informação, observando, dentre outras:

- Constituição Federal de 1988, especialmente quanto aos direitos fundamentais à intimidade, à vida privada e ao sigilo das comunicações;
- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);
- Lei nº 12.965/2014 – Marco Civil da Internet;
- Lei nº 12.527/2011 – Lei de Acesso à Informação, quando aplicável;
- Código de Ética das categorias profissionais envolvidas;
- Normas e regulamentos expedidos pela Autoridade Nacional de Proteção de Dados (ANPD);

Elaborado por:	Revisado por:	Autorizado por:	Data:	Página
Paula Amorim	NQSP	Dr. Yurgan Targe	23/07/2026	Página 1 de 8

 GESTÃO EM SAÚDE	POLÍTICA INSTITUCIONAL		
	SEGURANÇA DA INFORMAÇÃO		
	Setor/Área:	Código:	Versão:
	Presidência	PL-06	02

- g) Normas técnicas da família ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002, bem como demais normas correlatas relativas à gestão da segurança da informação;
- h) Requisitos regulatórios e de acreditação aplicáveis às organizações de saúde.

A aplicação desta Política deverá observar ainda os demais normativos internos da organização relacionados à governança, tecnologia da informação, gestão de riscos, continuidade de negócios e proteção de dados pessoais.

4 DEFINIÇÕES

- a) **Ativo de informação:** qualquer informação, sistema, equipamento, documento, software, serviço ou recurso tecnológico que possua valor para a organização.
- b) **Disponibilidade:** garantia de que a informação estará acessível aos usuários autorizados sempre que necessária.
- c) **Confidencialidade:** garantia de que a informação será acessada apenas por pessoas autorizadas.
- d) **Integridade:** garantia de que a informação permanecerá íntegra, completa, exata e protegida contra alterações não autorizadas.
- e) **Autenticidade:** capacidade de assegurar que a informação, documento ou usuário é genuíno e proveniente da fonte declarada.
- f) **Rastreabilidade:** capacidade de identificar quem acessou, alterou, transmitiu ou eliminou determinada informação.
- g) **Classificação da informação:** processo de categorização das informações conforme seu nível de criticidade, sensibilidade e necessidade de proteção.
- h) **Incidente de Segurança da Informação:** qualquer evento que comprometa ou possa comprometer a confidencialidade, integridade, disponibilidade ou autenticidade das informações ou dos ativos tecnológicos.
- i) **Backup:** cópia de segurança realizada para permitir a recuperação de informações em caso de perda, corrupção ou indisponibilidade.
- j) **Recuperação de Desastres:** conjunto de procedimentos destinados ao restabelecimento da infraestrutura tecnológica e das informações críticas após eventos que comprometam a continuidade das operações.
- k) **Segurança Cibernética:** conjunto de medidas destinadas à prevenção, detecção, resposta e recuperação frente a ameaças provenientes do ambiente digital.

5 DIRETRIZES

5.1 Governança da Informação

A S3 reconhece a informação como um ativo estratégico essencial ao desempenho de suas atividades assistenciais, administrativas, financeiras, acadêmicas e institucionais. A adequada gestão da informação é indispensável para garantir a continuidade dos serviços, a qualidade da assistência, a segurança dos pacientes, a tomada de decisão baseada em evidências, a

Elaborado por:	Revisado por:	Autorizado por:	Data:	Página
Paula Amorim	NQSP	Dr. Yurgan Targe	23/07/2026	Página 2 de 8

 GESTÃO EM SAÚDE	POLÍTICA INSTITUCIONAL		
	SEGURANÇA DA INFORMAÇÃO		
	Setor/Área:	Código:	Versão:
	Presidência	PL-06	02

conformidade legal e a sustentabilidade organizacional.

Nesse contexto, a gestão da informação deverá assegurar que todas as informações produzidas, recebidas, armazenadas, utilizadas, compartilhadas e descartadas sejam administradas de forma padronizada, segura, íntegra e alinhada aos objetivos institucionais.

Constituem diretrizes da governança da informação:

- reconhecer a informação como patrimônio institucional e ativo estratégico da organização;
- assegurar que todas as informações possuam responsável definido durante todo o seu ciclo de vida;
- estabelecer controles que garantam a qualidade, confiabilidade, integridade e disponibilidade das informações;
- promover a padronização dos processos relacionados à gestão documental e à gestão das informações eletrônicas;
- assegurar que a utilização das informações ocorra exclusivamente para finalidades institucionais legítimas e autorizadas;
- manter mecanismos de rastreabilidade das informações críticas, possibilitando identificar sua origem, utilização, alterações e destinação.

5.2 Organização e Gestão das Informações

As informações institucionais deverão ser organizadas de forma estruturada, permitindo sua recuperação, utilização, compartilhamento e preservação de maneira eficiente e segura.

A S3 adota critérios padronizados para criação, armazenamento, atualização, retenção, arquivamento e descarte das informações, observando requisitos legais, regulatórios, assistenciais e administrativos.

São diretrizes para organização das informações:

- manter informações completas, atualizadas, consistentes e confiáveis;
- utilizar sistemas informatizados e mecanismos de controle compatíveis com a criticidade das informações;
- preservar a integridade dos registros físicos e eletrônicos;
- definir prazos de guarda e descarte conforme legislação vigente e normas internas;
- assegurar a disponibilidade das informações necessárias à continuidade das atividades institucionais.

5.3 Classificação da Informação

A classificação da informação constitui mecanismo essencial para definição dos níveis de proteção aplicáveis aos ativos informacionais da organização. A informação deverá ser classificada considerando sua sensibilidade, criticidade, requisitos legais, impacto institucional e necessidade de restrição de acesso.

A classificação deverá orientar os controles relativos ao acesso, armazenamento,

Elaborado por:	Revisado por:	Autorizado por:	Data:	Página
Paula Amorim	NQSP	Dr. Yurgan Targe	23/07/2026	Página 3 de 8

 GESTÃO EM SAÚDE	POLÍTICA INSTITUCIONAL		
	SEGURANÇA DA INFORMAÇÃO		
	Setor/Área:	Código:	Versão:
	Presidência	PL-06	02

transmissão, compartilhamento, retenção e descarte das informações.

5.4 Confidencialidade da Informação

Todos os colaboradores, prestadores de serviços e terceiros devem assinar o Termo de Confidencialidade ao estabelecer o contrato de trabalho. As diretrizes organizacionais de segurança das informações do paciente estão descritas em procedimentos específicos por perfil da unidade.

5.5 Obtenção, Validação e Utilização das Informações

As informações utilizadas pela organização deverão ser provenientes de fontes confiáveis, obtidas por meios lícitos e submetidas, sempre que necessário, a processos de validação que assegurem sua qualidade e confiabilidade.

A utilização das informações deverá apoiar os processos de gestão, assistência, planejamento, avaliação de desempenho, monitoramento de indicadores, gestão de riscos e melhoria contínua.

Constituem diretrizes:

- utilizar fontes confiáveis para obtenção das informações;
- validar informações críticas antes de sua utilização;
- preservar a integridade dos registros institucionais;
- utilizar indicadores e dados confiáveis para subsidiar decisões;
- assegurar que as informações sejam utilizadas apenas para finalidades institucionais legítimas.

5.6 Gestão dos Ativos de Informação

Todos os ativos de informação deverão ser identificados, inventariados, protegidos e gerenciados de acordo com sua importância para a organização.

São considerados ativos de informação, entre outros:

- documentos físicos;
- prontuários;
- bancos de dados;
- sistemas de informação;
- equipamentos computacionais;
- dispositivos móveis;
- servidores;
- mídias de armazenamento;
- serviços em nuvem;

Elaborado por:	Revisado por:	Autorizado por:	Data:	Página
Paula Amorim	NQSP	Dr. Yurgan Targe	23/07/2026	Página 4 de 8

 GESTÃO EM SAÚDE	POLÍTICA INSTITUCIONAL		
	SEGURANÇA DA INFORMAÇÃO		
	Setor/Área:	Código:	Versão:
	Presidência	PL-06	02

j) redes de comunicação.

5.7 Controle de Acesso

O acesso às informações institucionais deverá observar os princípios da necessidade de conhecimento e do menor privilégio, garantindo que cada usuário tenha acesso apenas às informações necessárias ao desempenho de suas atribuições. A S3 mantém mecanismos formais de concessão, revisão, alteração e revogação de acessos.

Constituem diretrizes:

- a) autenticação individual dos usuários;
- b) utilização de credenciais pessoais e intransferíveis;
- c) revisão periódica dos perfis de acesso;
- d) revogação imediata dos acessos quando houver desligamento ou alteração de função;
- e) registro e monitoramento dos acessos aos sistemas críticos.

5.8 Segurança da Informação

A organização adotará medidas técnicas, administrativas e organizacionais destinadas à proteção das informações contra acessos não autorizados, perda, destruição, alteração, indisponibilidade ou qualquer forma de tratamento inadequado.

Os controles de segurança deverão ser proporcionais aos riscos identificados e revisados periodicamente.

Para esse fim deverão ser implementados, entre outros:

- a) controles de acesso físico e lógico;
- b) mecanismos de autenticação;
- c) criptografia, quando aplicável;
- d) proteção contra códigos maliciosos;
- e) atualização de softwares e sistemas;
- f) monitoramento da infraestrutura tecnológica;
- g) gestão de vulnerabilidades;
- h) registro e tratamento de incidentes.

5.9 Segurança Cibernética

A organização manterá programa contínuo de segurança cibernética voltado à prevenção, identificação, resposta e recuperação frente a ameaças que possam comprometer seus ativos tecnológicos e informacionais.

As medidas de proteção deverão considerar a evolução constante dos riscos cibernéticos e contemplar mecanismos preventivos, detectivos e corretivos.

Elaborado por:	Revisado por:	Autorizado por:	Data:	Página
Paula Amorim	NQSP	Dr. Yurgan Targe	23/07/2026	Página 5 de 8

 GESTÃO EM SAÚDE	POLÍTICA INSTITUCIONAL		
	SEGURANÇA DA INFORMAÇÃO		
	Setor/Área:	Código:	Versão:
	Presidência	PL-06	02

Constituem diretrizes:

- a) monitoramento contínuo dos ambientes tecnológicos;
- b) atualização permanente dos sistemas;
- c) utilização de soluções de proteção de redes;
- d) gerenciamento de vulnerabilidades;
- e) realização de avaliações periódicas de riscos;
- f) resposta estruturada aos incidentes de segurança.

5.10 Informação dos Pacientes

Toda a informação relativa ao atendimento aos pacientes deve ser guardada por meio do prontuário do paciente (seja ele físico, eletrônico ou misto). O acesso ao prontuário dos pacientes é regulamentado em procedimentos operacionais locais conforme perfil de cada unidade, porém, em todos os casos, a S3 responsabiliza-se pela segurança de tais informações, compartilhando essa responsabilidade com o time assistencial que tem acesso a tais registros.

Dados dos pacientes são informações sigilosas, sendo proibido a qualquer pessoa que tenha acesso a essas informações, durante o exercício das atividades profissionais ou de forma acidental, fornecer à terceiros os dados neles contidos, a não ser entre as pessoas incumbidas do diagnóstico dos pacientes, ou quando autorizado, por escrito, pelo paciente ou seu representante legal, ou para atender a ordem judicial.

5.11 Backup e Recuperação das Informações

A organização manterá procedimentos formais de backup destinados à preservação das informações críticas e à continuidade das operações institucionais.

As cópias de segurança deverão ser protegidas contra perda, acesso não autorizado, alteração ou destruição. Procedimentos operacionais da equipe de Tecnologia da Informação, descrevem periodicidade, fluxos e controles do processo de backup realizados na S3.

5.12 Proteção de Equipamentos

A proteção de equipamentos utilizados em qualquer processo, que manipulam informações é garantida pela área específica onde o processo ocorre através do cumprimento dos requisitos de utilização do equipamento conforme manual do fabricante ou instrução interna. Em todos os casos Planos de Manutenção e/ou Segurança são acompanhados pelo Gestor e/ou pela equipe de TI quando aplicável. As soluções de segurança oferecidas pela S3 como antivírus e/ou programas de proteção de tela não devem ser desinstaladas.

É importante lembrar que todo o uso de recursos de tecnologia da informação disponibilizados pela S3 tais como e-mail, sistemas, Internet, bem como fornecidos por terceiros, no uso e atribuições da S3, devem ser utilizados estritamente para fins profissionais e no interesse da S3.

Elaborado por:	Revisado por:	Autorizado por:	Data:	Página
Paula Amorim	NQSP	Dr. Yurgan Targe	23/07/2026	Página 6 de 8

 GESTÃO EM SAÚDE	POLÍTICA INSTITUCIONAL		
	SEGURANÇA DA INFORMAÇÃO		
	Setor/Área:	Código:	Versão:
	Presidência	PL-06	02

Serão considerados fins indevidos: fraudes, invasão, jogos, uso de proxys, acesso não autorizado, personificação, falsa identidade, obtenção de senhas e dados privativos, perseguição, ameaças, downloads não autorizados, distribuição de códigos maliciosos, vírus, acesso e disseminação de materiais pornográficos, ofensivos, difamatório, discriminatório, preconceituoso e atentatórios à moral e aos bons costumes, instalação de softwares piratas, veiculação de opiniões político-partidárias ou religiosas, conteúdo ilegal, de incitação à violência, que não respeitem os direitos autorais ou objetivos comerciais particulares; SPAM; distribuição de correntes de mensagens eletrônicas, ações que comprometam a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pela S3, cometimento de crimes ou que venham a prejudicar, mesmo de forma não intencional, outros colaboradores, pessoas e instituições vinculadas à prestação de serviços ou recursos da S3.

5.13 Continuidade de Negócios e Recuperação de Desastres

A S3 mantém Plano de Contingência documentados, atualizados e periodicamente testados, visando minimizar impactos decorrentes de falhas tecnológicas, eventos naturais, ataques cibernéticos ou outras situações que comprometam a disponibilidade das informações.

Os planos deverão contemplar procedimentos para recuperação dos serviços críticos, definição de responsabilidades, prioridades de restabelecimento, testes periódicos e avaliação dos resultados obtidos.

5.14 Capacitação e Conscientização

A efetividade da segurança da informação depende da participação ativa de todos os profissionais da organização.

A organização promoverá programas permanentes de capacitação, treinamento e conscientização destinados ao desenvolvimento da cultura de segurança da informação, abordando boas práticas de utilização dos recursos tecnológicos, prevenção de incidentes, proteção das informações institucionais, segurança cibernética, engenharia social, uso seguro de dispositivos móveis e responsabilidades individuais.

Todos os colaboradores deverão participar das ações educativas compatíveis com suas atribuições.

6 INVESTIGAÇÃO E SANÇÕES APLICÁVEIS

Qualquer dirigente, colaborador, terceiro ou parceiro que viole disposições desta Política estará sujeito às sanções disciplinares previstas no Código de Ética e Conduta da S3 Gestão em Saúde, listadas abaixo:

- Advertência verbal;
- Advertência por escrito;
- Suspensão;
- Demissão sem justa causa;

Elaborado por:	Revisado por:	Autorizado por:	Data:	Página
Paula Amorim	NQSP	Dr. Yurgan Targe	23/07/2026	Página 7 de 8

 GESTÃO EM SAÚDE	POLÍTICA INSTITUCIONAL		
	SEGURANÇA DA INFORMAÇÃO		
	Setor/Área:	Código:	Versão:
	Presidência	PL-06	02

- e) Demissão por justa causa;
- f) Exclusão do fornecedor, parceiro ou agente intermediário da instituição;
- g) Ação judicial cabível.

7 RESPONSABILIDADES

A proteção das informações é responsabilidade de todos. Independentemente do cargo, função ou vínculo com a organização, toda pessoa que tenha acesso a informações, ativos informacionais ou recursos utilizados para seu tratamento deve atuar de forma diligente para preservar sua confidencialidade, integridade e disponibilidade. Isso inclui cumprir as diretrizes estabelecidas nesta Política, utilizar as informações apenas para fins autorizados, comunicar imediatamente quaisquer incidentes, vulnerabilidades ou suspeitas de violação de segurança e adotar boas práticas de proteção das informações em qualquer meio, seja físico, digital, verbal ou qualquer outra forma de armazenamento, processamento ou compartilhamento.

8 COMUNICAÇÃO

A S3 Gestão em Saúde incentiva a todos que comuniquem imediatamente ao Comitê de Ética quando suspeitarem ou detectarem violações a esta Política ou as legislações correlatas, cuja análise e investigação serão tratadas confidencialmente. Não serão admitidas retaliações e intimidações aos denunciante.

Essa Política deverá ser amplamente comunicada através do Sistema de Gestão de Qualidade e iniciativas realizadas pelo setor de TI e NEPH em todas as unidades.

9 HISTÓRICO DE REVISÃO

VERSÃO	DATA	DESCRIÇÃO DAS ALTERAÇÕES	RESPONSÁVEL
1	04/11/2012	Criação do Documento	Nailton Cazumbá
2	23/07/2026	Atualização dos requisitos orientados pela versão 2026 da norma ONA.	Paula Amorim

Elaborado por:	Revisado por:	Autorizado por:	Data:	Página
Paula Amorim	NQSP	Dr. Yurgan Targe	23/07/2026	Página 8 de 8