

	<div>POLÍTICA INSTITUCIONAL</div>	Referência nº: SED-POL-TI-002	
		Estabelecido em: 12/07/2022	
		Válido até: 12/07/2024	
TÍTULO: POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO		Classificação: Público	P
		Página 1 de 12	

Controle Histórico				
Revisão	Data	Elaboração	Verificação	Aprovação
0	20/07/2006	Tecnologia da Informação	Diretoria	Diretoria
1	15/06/2010	Edmilson Braz Filho	Diretoria	Diretoria
2	25/05/2017	Caio Humberto G. Júnior	Edmilson Braz Filho	Dr. José Renato C. Schmidt e Edemilson A. Donola
3	30/01/2020	Edmilson Braz Filho	Comitê de Segurança da Informação	Dr. José Renato C. Schmidt e Edemilson A. Donola
4	01/12/2020	Edmilson Braz Filho	Comitê de Segurança da Informação	Dra. Maura Ap. da Silva e Edemilson A. Donola
5	12/07/2022	Edmilson Braz Filho	Comitê de Segurança da Informação e Edemilson Antonio Donola	Dra. Maura Ap. da Silva, Dr. Roberto Rezende Machado e Dr. José Renato C. Schmidt

1. OBJETIVO

A UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO tem como missão cuidar da saúde das pessoas.

A UNIMED PINDAMONHANGABA entende que a informação corporativa é um bem essencial para sustentar suas atividades e garantir a qualidade dos atendimentos de seus beneficiários e cooperados.

A UNIMED PINDAMONHANGABA compreende que a manipulação e armazenamento de suas informações físicas e digitais são vulneráveis a fatores externos e internos que podem comprometer a segurança das informações corporativas.

DS

AMFLF

DS

ED

DS

EB

DS

EMS

DS

JRPM


DS

DJRLS

DS

JDDSG

DS



DS


MMSM

DS

RRM

DS

PC

	<div>POLÍTICA</div> <div>INSTITUCIONAL</div>	Referência nº: SED-POL-TI-002	
		Estabelecido em: 12/07/2022	
		Válido até: 12/07/2024	
TÍTULO: POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO		Classificação: Público	P
		Página 2 de 12	

Desta forma, a UNIMED PINDAMONHANGABA estabelece sua Política Geral de Segurança da Informação, como parte integrante do seu sistema de gestão corporativo, *planejamento estratégico*, alinhada às boas práticas e normativas de agências reguladoras, preconizando níveis adequados de proteção das informações sob sua responsabilidade.

2. ÂMBITO DE APLICAÇÃO

Esta política se aplica a todos os usuários da informação da UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO, tais como *Diretores, Conselheiros, Cooperados, Colaboradores, terceiros contratados e, onde pertinente*, que possuíram, possuem ou virão a possuir acesso às informações e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura UNIMED PINDAMONHANGABA. *Se aplica a Operadora e seus recursos próprios.*

O objetivo da Gestão de Segurança da Informação da UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte as operações críticas do negócio e minimizando riscos e seus eventuais impactos.

A Diretoria e o Comitê Gestor de Segurança da Informação estão comprometidos com uma gestão efetiva de Segurança da Informação. Desta forma, adotam todas medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização.

É política da UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO:

- Elaborar, implantar e seguir por completo políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação da UNIMED PINDAMONHANGABA sejam atingidos através da adoção de controles contra ameaças externas e internas;
- Disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas, tais como: *Diretores, Conselheiros, Cooperados, Colaboradores, terceiros contratados e, onde pertinente.*

DS

AMFLF

DS

ED

DS

EB

DS

EMS

DS

JRPM


DS

DJRLS

DS

JDDSG

DS



DS

MMSM

DS

RRM

DS

PC

	POLÍTICA INSTITUCIONAL	Referência nº: SED-POL-TI-002	
		Estabelecido em: 12/07/2022	
		Válido até: 12/07/2024	
TÍTULO: POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO		Classificação: Público	P
		Página 3 de 12	

- Garantir a educação e conscientização sobre as práticas adotadas pela UNIMED PINDAMONHANGABA de segurança da informação para *Diretores, Conselheiros, Cooperados, Colaboradores, terceiros contratados e, onde pertinente.*
- Atender integralmente requisitos de segurança da informação aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais;
- Tratar integralmente incidentes de segurança da informação, garantindo que os mesmos sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicando as autoridades apropriadas e os titulares das informações;
- Garantir a continuidade do negócio através da implantação de planos de continuidade e recuperação de desastres;
- Melhorar continuamente a Gestão de Segurança da Informação através da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização.
- *As conexões de redes externas ao ambiente da Operadora e seus Recursos Próprios devem ser realizadas por VPN (conforme documento SED-PS-TI-003);*
- *Arquivos confidenciais transmitidos por meios eletrônicos devem ser criptografados (conforme documento SED-PS-TI-017), para preservar a integridade da informação.*

3. SIGLAS E DEFINIÇÕES

Administradores: Todas as pessoas naturais, eleitas, nomeadas ou designadas para os cargos de diretor, administrador ou conselheiro do conselho de administração, ou órgão assemelhado, independentemente da nomenclatura e do tipo societário da qual façam parte.

Ameaça: Causa potencial de um incidente, que pode vir a prejudicar a UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO.

Ativo de informação: Patrimônio intangível da UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, legal natureza,

DS

AMFLF

DS

ED

DS

EB

DS

EMS

DS

JRPM


DS

DJRLS

DS

JDDSG

DS



DS

MMSM

DS

RRM

DS

PC

	<div>POLÍTICA</div> <div>INSTITUCIONAL</div>	Referência nº: SED-POL-TI-002	
		Estabelecido em: 12/07/2022	
		Válido até: 12/07/2024	
TÍTULO: POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO		Classificação: Público	P
		Página 4 de 12	

bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas a UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO por parceiros, clientes, empregados e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional da UNIMED PINDAMONHANGABA ou por infraestrutura externa contratada pela organização, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física.

Ativo: Tudo aquilo que possui valor para a UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO.

COMITÊ DE SEGURANÇA DA INFORMAÇÃO – CSI: Grupo de trabalho multidisciplinar permanente, efetivado pela diretoria da UNIMED PINDAMONHANGABA, que tem por finalidade tratar questões ligadas à Segurança da Informação.

Confidencialidade: Propriedade dos ativos da informação da UNIMED PINDAMONHANGABA, de não serem disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas.

Confidencialidade: Propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizada e credenciada. É a garantia do resguardo das informações dadas pessoalmente em confiança e proteção contra a sua revelação não autorizada.

Controle: Medida de segurança adotada pela UNIMED PINDAMONHANGABA para o tratamento de um risco específico.

Disponibilidade: Propriedade dos ativos da informação da UNIMED PINDAMONHANGABA, de serem acessíveis e utilizáveis sob demanda, por partes autorizadas.

Gestor: É o responsável por administrar e coordenar as atividades de uma determinada área ou departamento. Também é o responsável pela articulação entre equipes e gerência, trabalhando junto aos colaboradores para garantir que as metas sejam cumpridas e que as necessidades da equipe sejam atendidas. Enquanto o Gerente possui um papel mais administrativo, focado no desenvolvimento de estratégias da organização, o gestor atua com maior proximidade da equipe agindo como um facilitador para que as metas estabelecidas possam ser alcançadas.

Incidente de segurança da informação: Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações da UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO.

Integridade: Propriedade dos ativos da informação da UNIMED PINDAMONHANGABA, de serem exatos e completos.

	POLÍTICA INSTITUCIONAL	Referência nº: SED-POL-TI-002	
		Estabelecido em: 12/07/2022 Válido até: 12/07/2024	
		Classificação: Público	P
TÍTULO: POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO		Página 5 de 12	

Integridade das Informações/Dados: Corresponde à preservação da precisão, consistência e confiabilidade das informações e sistemas pela organização ao longo dos processos ou de seu ciclo de vida.

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, impondo mais proteção e penalidades para o não cumprimento.

Monitoramento: Observação e registro regular das atividades de um projeto ou programa, com o objetivo identificar tanto não conformidades reais como potenciais, e ainda, apontar pontos de melhoria.

Nível de Acesso: Ferramenta de segurança da informação que permite determinar quais áreas do sistema cada usuário tem permissão de acessar de acordo com sua categoria. Funciona de forma hierárquica: usuários não podem excluir e/ou editar informações de usuários de hierarquias iguais ou superiores aos dele.

PGSI: Política Geral de Segurança da Informação.

Política de Segurança da Informação: Documento que deve conter um conjunto de normas, métodos e procedimentos, de diretrizes e melhores práticas em gestão da segurança da informação, os quais devem ser comunicados a todos os funcionários, bem como analisado e revisado criticamente, em intervalos regulares ou quando mudanças se fizerem necessárias.

Usuário da informação: Cooperados e colaboradores com vínculo empregatício de qualquer área da UNIMED PINDAMONHANGABA ou terceiros alocados na prestação de serviços a UNIMED PINDAMONHANGABA, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar ou manipular qualquer ativo de informação da UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO para o desempenho de suas atividades profissionais.

VPN: “Virtual Private Network” (Rede Privada Virtual).

4. DIRETRIZES

4.1 Atribuições e responsabilidades

DS

AMFLF

DS

ED

DS

EB

DS

EMS

DS

JRPM


DS

DJRLS

DS

JDDSG

DS



DS


MMSM

DS

RRM

DS

PC

	<div>POLÍTICA INSTITUCIONAL</div>	Referência nº: SED-POL-TI-002	
		Estabelecido em: 12/07/2022	
		Válido até: 12/07/2024	
TÍTULO: POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO		Classificação: Público	P
		Página 6 de 12	

Comitê de Segurança da Informação - CSI	<p>Fica constituído o COMITÊ DE SEGURANÇA DA INFORMAÇÃO, contando com a participação de, pelo menos, um representante da diretoria e um membro sênior das seguintes áreas: Tecnologia da Informação, Recursos Humanos, Jurídico.</p> <p>É responsabilidade do CSI:</p> <ul style="list-style-type: none">- Analisar, revisar e propor a aprovação de políticas e normas relacionadas à segurança da informação;- Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação;- Garantir que as atividades de segurança da informação sejam executadas em conformidade com a PGSI;- Promover a divulgação da PGSI e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente da UNIMED PINDAMONHANGABA;- Conduzir a Gestão e Operação da segurança da informação;- Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;- Tomar as ações cabíveis para se fazer cumprir os termos desta política;- Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado.
Gestores da informação (coordenadores dos setores)	<p>É responsabilidade dos Gestores da Informação:</p> <ul style="list-style-type: none">- Gerenciar as informações geradas ou sob a responsabilidade da sua área de negócio durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte conforme as normas estabelecidas pela UNIMED PINDAMONHANGABA;- Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de negócio conforme normas, critérios e

	<div>POLÍTICA</div> <div>INSTITUCIONAL</div>	Referência nº: SED-POL-TI-002	
		Estabelecido em: 12/07/2022	
		Válido até: 12/07/2024	
TÍTULO: POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO		Classificação: Público	P
		Página 7 de 12	

	<p>procedimentos adotados pela UNIMED PINDAMONHANGABA;</p> <ul style="list-style-type: none">- Periodicamente revisar as informações geradas ou sob a responsabilidade da sua área de negócio, ajustando a classificação e rotulagem das mesmas conforme necessário;- Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;- Solicitar a concessão ou revogação de acesso a informação ou sistemas de informação de acordo com os procedimentos adotados pela UNIMED PINDAMONHANGABA.
Usuários da informação	<p>É responsabilidade dos Usuários da Informação:</p> <ul style="list-style-type: none">- Ler, compreender e cumprir integralmente os termos da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;- Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política Geral de Segurança da Informação, suas normas ou procedimentos ao Comitê de Segurança da Informação;- Comunicar ao Comitê de Segurança da Informação qualquer evento que viole esta Política ou gere riscos à segurança das informações ou dos recursos computacionais da UNIMED PINDAMONHANGABA;- Assinar o Termo de Confidencialidade e uso dos Sistemas de Informação (impresso SED-I-TI-004) da UNIMED PINDAMONHANGABA, formalizando a ciência e o aceite integral das disposições da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;- Responder pela inobservância da Política Geral de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item sanções e punições.

4.2 Propósito

DS

AMFLF

DS

ED

DS

EB

DS

EMS

DS

JRPM

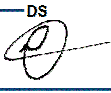
DS

DJRS

DS

JDDSG

DS



DS


MMSM

DS

KRM

DS

PL

	<p style="text-align: center;">POLÍTICA INSTITUCIONAL</p>		Referência nº: SED-POL-TI-002
			Estabelecido em: 12/07/2022 Válido até: 12/07/2024
TÍTULO: POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO		Classificação: Público	P
		Página 8 de 12	

Esta política normatiza a manipulação, integridade e confidencialidade das informações e permite aos colaboradores e cooperados da UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO adotar padrões comportamentais seguros e adequados às metas e necessidades da UNIMED PINDAMONHANGABA;


- Orientar quanto à adoção de controles e processos para atendimento dos requisitos para Segurança da Informação;
- Resguardar as informações da UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO, garantindo requisitos básicos de confidencialidade, integridade e disponibilidade;
- Prevenir possíveis causas de incidentes e a responsabilidade legal da instituição e seus colaboradores, cooperados, beneficiários e parceiros;
- Minimizar os riscos de perdas financeiras, da confiança de beneficiários e contratantes ou de qualquer outro impacto negativo no negócio da UNIMED PINDAMONHANGABA como resultado de falhas de segurança.

4.3 Escopo

Esta Política de Segurança da Informação é composta por:

- **Termo de confidencialidade e uso dos sistemas (documento SED-I-TI-004)**, que normatiza os direitos e deveres dos funcionários, cooperados, terceiros e parceiros sobre o uso seguro dos ativos da informação da Unimed Pindamonhangaba. A Política e seu acesso são citados no documento.
- **Acesso Remoto (documento SED-PS-TI-003)**, norteia as melhores práticas para acessos remotos aos ativos da informação. Todo acesso deve ser solicitado pelo Coordenador (Gestor da Informação) via GLPI (Sistema de Chamados).
- **Classificação da Informação (documento SED-PS-TI-004)**, que orienta como as informações devem ser classificadas e manipuladas. Em seu anexo 1, normatiza a manipulação, distribuição e destruição, além de destacar a necessidade de criptografar arquivos confidenciais quando transmitidos por e-mail.
- **Códigos Maliciosos (documento SED-PS-TI-005)**, estabelece diretrizes para a proteção dos ativos/serviços de informação UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO contra ameaças e códigos maliciosos de qualquer natureza.

DS AMFLF DS ED DS EB DS EMS DS JRPM DS DJRCS DS JDDSG DS [Signature] DS MMSM DS KRM DS PC

	POLÍTICA INSTITUCIONAL	Referência nº: SED-POL-TI-002	
		Estabelecido em: 12/07/2022 Válido até: 12/07/2024	
TÍTULO: POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO		Classificação: Público	P
		Página 9 de 12	

- **E-mail e Mensageiros instantâneos (documento SED-PS-TI-006)**, institui regras sobre o uso do e-mail corporativo e mensageiros eletrônicos.
- **Gestão de Identidade controle de acesso (documento SED-PS-TI-007)**, apresenta a responsabilidade dos Usuários da Informação sobre suas credenciais de acesso, lógica de criação de senhas e periodicidade de troca. A senha de acesso é individual e de total responsabilidade do Usuário da Informação.
- **Internet e Mídias Sociais (documento SED-PS-TI-008)**, estabelece regras sobre o uso de redes sociais e diretrizes éticas a serem respeitadas.
- **Monitoramento (documento SED-PS-TI-009)**, destaca a existência do monitoramento de todos ativos da informação e físico (Câmeras de Monitoramento).
- **Resposta a incidentes (documento SED-PS-TI-010)**, apresenta as diretrizes em caso de incidentes.
- **Uso Aceitável de Ativos de Informação (documento SED-PS-TI-013)**, estabelece diretrizes para o uso aceitável, entendido como seguro, dos ativos de informação da UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO por seus usuários autorizados.


As documentações estão disponíveis nos sistemas Sigquali, Tasy e “Área do Cooperado” para consulta.

4.4 Sanções e punições

As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa;

A aplicação de sanções e punições será realizada conforme a análise do CSI - Comitê de Segurança da Informação, devendo-se considerar a gravidade da infração, o descumprimento da Lei Geral de Proteção de Dados – Lei 13.709/18, efeito alcançado, recorrência e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, podendo o CSI, no uso do poder disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave;

No caso de terceiros contratados ou prestadores de serviço, o CSI deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato;

	<p style="text-align: center;">POLÍTICA INSTITUCIONAL</p>	Referência nº: SED-POL-TI-002	
TÍTULO: POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO		Estabelecido em: 12/07/2022 Válido até: 12/07/2024	
		Classificação: Público	P
		Página 10 de 12	

Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano a UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo aos termos descritos nesta política.

4.5 Casos omissos

Os casos omissos serão avaliados pelo Comitê de Segurança da Informação para posterior deliberação. As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação da UNIMED PINDAMONHANGABA adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção as informações da UNIMED PINDAMONHANGABA.

5. VALIDAÇÃO E APROVAÇÃO PELO CONSELHO DE ADMINISTRAÇÃO


Esta Política foi validada e aprovada pelo Conselho de Administração, conforme ata de reunião do dia 11/07/2022.

6. REGRAS DE CONSEQUÊNCIA

As consequências em caso de descumprimento destas diretrizes serão tratadas em conformidade com o Estatuto Social da Unimed Pindamonhangaba - disponível na Área do Cooperado (site www.unimedpinda.com.br), tópico de Infrações e Penalidades (artigos 37º e 38º) – quando se tratar de cooperados, ou Código de Conduta e Ética Institucional, tópico de penalidades e ações disciplinares, quando for relacionado a colaboradores. Situações excepcionais serão encaminhadas para a Diretoria Executiva e/ou demais órgãos de governança.

7. REFERÊNCIAS

DS AMFLF DS ED DS EB DS EMS DS JRPM DS DJRCS DS JDDSG DS [Assinatura] DS MUSA DS RRM DS PC

	<p style="text-align: center;">POLÍTICA INSTITUCIONAL</p>		Referência nº:
			SED-POL-TI-002
		Estabelecido em: 12/07/2022	
		Válido até: 12/07/2024	
TÍTULO: POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO		Classificação:	P
		Público	
		Página 11 de 12	

RESOLUÇÃO NORMATIVA - RN Nº 507, DE 30 DE MARÇO DE 2022. Dispõe sobre o Programa de Acreditação de Operadoras de Planos Privados de Assistência à Saúde. Anexo I. Item 1.3.1 e 1.3.10. Disponível em:

https://www.ans.gov.br/component/legislacao/?view=legislacao&task=pdfAtualizado&format=raw&id=ND_E5Ng== e [https://www.ans.gov.br/images/stories/Legislacao/n/RN_507 - ANEXO I - TAMANHO CORRETO Conferir se houve altera%C3%A7%C3%A3o.pdf](https://www.ans.gov.br/images/stories/Legislacao/n/RN_507_-_ANEXO_I_-_TAMANHO_CORRETO_Conferir_se_houve_altera%C3%A7%C3%A3o.pdf)

Lei nº 13.709 de 14/08/2018. Esta Lei dispõe sobre o 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 e o livre desenvolvimento da personalidade da pessoa natural. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm

Lei nº 13.853 de 08/07/2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispõe sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1

SED-I-TI-004 Termo de confidencialidade e uso dos sistemas

SED-PS-TI-003 Acesso Remoto

SED-PS-TI-004 Classificação da Informação

SED-PS-TI-005 Códigos Maliciosos

SED-PS-TI-006 E-mail e Mensageiros instantâneos

SED-PS-TI-007 Gestão de Identidade e controle de acesso

SED-PS-TI-008 Internet e Mídias Sociais

SED-PS-TI-009 Monitoramento de ativos/serviços de informação e recursos computacionais

SED-PS-TI-010 Resposta a incidentes

SED-PS-TI-013 Uso aceitável de Ativos de Informação

SED-PS-TI-014 Uso de equipamentos pessoais

8. CONTROLE DE ALTERAÇÕES

Revisão 0 - Emissão Inicial.

Revisão 1 - Alterados itens 2.2, 4.2, 4.3, 4.4, 4.5 4.6, 4.7 e 4.8. Incluído os itens 4.9 e subitem 4.4.1.

DS AMFLF DS ED DS EB DS EMS DS JKPM DS DJRCS DS JDDSG DS [Signature] DS MMSM DS RRAM DS PC

	POLÍTICA INSTITUCIONAL	Referência nº: SED-POL-TI-002	
		Estabelecido em: 12/07/2022 Válido até: 12/07/2024	
TÍTULO: POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO	Classificação: Público	P	
	Página 12 de 12		

Revisão 2 - Alterado a referência de T.I/001 para SED-POP-TI-001 e itens 1.1, 1.2, 2.1, 2.2, 4.2, 4.3, 4.4, 4.5 e 4.9. Inclusão dos itens 4.11, 4.11.1, 4.12, 4.13 e anexos.

Revisão 3 - Alterada a referência de SED-POP-TI-001 para SED-PS-TI-002. Alteração em todos os itens do documento.

Revisão 4 – Alteração correta na revisão 3 - referência de SED-POP-TI-001 para SED-POL-TI-002, “Abrangência” e “Documentos de referência para atendimento às Diretrizes”.

Revisão 5 – Alteração nos itens: 1, 2, 3, 4.1, 4.3, 4.4 e 7. Alteração em “Referências”.

CÓPIA NÃO CONTROLADA