	Procedimento Sistêmico	Referência nº: SED-PS-TI-005	
		Estabelecido em: 14/07/2022 Válido até: 14/07/2024	
		Página 1 de 5	
Atividade: Códigos Maliciosos  Responsável: Coordenador de T.I.		Classificação: Interno	I

Controle Histórico				
Revisão	Data	Elaboração	Verificação	Aprovação
0	31/01/2020	Edmilson Braz Filho	Comitê de Segurança da Informação	Dr. José Renato C. Schmidt e Edemilson Antonio Donola
1	14/07/2022	Edmilson Braz Filho	Comitê de Segurança da Informação	Dra. Maura Aparecida da Silva e Edemilson A. Donola

Síglas e Definições

**Ameaça:** Causa potencial de um incidente, que pode vir a prejudicar 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.

**Segurança da informação:** A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO.

Materiais


Computador com acesso a rede interna.

Abrangência

Aplica-se a todos colaboradores da Unimed Pindamonhangaba.

Diretrizes

1. Introdução

	Procedimento Sistêmico	Referência nº: SED-PS-TI-005	
		Estabelecido em: 14/07/2022 Válido até: 14/07/2024	
		Página 2 de 5	
Atividade: Códigos Maliciosos  Responsável: Coordenador de T.I.		Classificação: Interno	I

Esta norma complementa a Política Geral de Segurança da Informação (SED-POL-TI-002), definindo as diretrizes para proteção dos ativos/serviços de informação UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO contra ameaças e códigos maliciosos de qualquer natureza.

2. Propósito

Estabelecer diretrizes para a proteção dos ativos/serviços de informação UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO contra ameaças e códigos maliciosos de qualquer natureza.


3. Escopo

Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação (SED-POL-TI-002).

4. Diretrizes

4.1 Ferramenta de proteção contra códigos maliciosos:

- A UNIMED PINDAMONHANGABA disponibiliza ferramentas para proteção dos seus ativos/serviços de informação e recursos computacionais, incluindo estações de usuários, dispositivos móveis e servidores corporativos, contra ameaças e códigos maliciosos tais como vírus, cavalos de Tróia, ferramentas de captura de tela e dados digitados, softwares de propaganda e similares;
- Apenas a ferramenta disponibilizada pela UNIMED PINDAMONHANGABA deve ser utilizada na proteção contra códigos maliciosos;
- A ferramenta de proteção contra códigos maliciosos da UNIMED PINDAMONHANGABA adota as seguintes regras de uso:

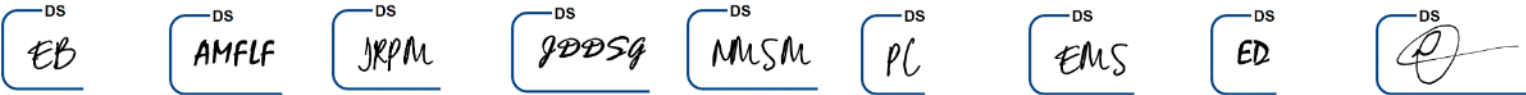
	Procedimento Sistêmico	Referência nº: SED-PS-TI-005	
		Estabelecido em: 14/07/2022 Válido até: 14/07/2024	
		Página 3 de 5	
Atividade: Códigos Maliciosos  Responsável: Coordenador de T.I.		Classificação: Interno	I


- Atualização em tempo real do arquivo de assinaturas de códigos maliciosos e varredura diária em estações de usuários e servidores corporativos;
- *As varreduras completas devem analisar todos os arquivos em cada uma das unidades de armazenamento locais das estações de usuários semanalmente;*
- As varreduras diárias em servidores corporativos podem ser limitadas a pastas ou arquivos específicos, de modo a evitar o comprometimento do desempenho de recursos computacionais críticos;
- As funções de proteção em tempo real e detecção com base no comportamento devem estar habilitadas para todas as estações de usuários e dispositivos móveis;
- Sites, serviços e arquivos baixados da internet detectados como possíveis ameaças serão automaticamente bloqueados em estações de usuários, dispositivos móveis e servidores corporativos;
- Caso uma estação de usuário ou dispositivo móvel esteja infectado ou com suspeita de infecção de código malicioso, a mesma deverá ser imediatamente isolada da rede corporativa da UNIMED PINDAMONHANGABA e de qualquer comunicação com a internet;
- Caso um servidor corporativo esteja infectado ou com suspeita de infecção de código malicioso, deverão ser adotadas medidas para garantir o isolamento do mesmo da rede corporativa e da internet, levando em consideração o impacto da desativação dos serviços publicados no referido servidor.

4.2 Prevenção dos usuários contra códigos maliciosos

Mesmo com a existência de ferramentas para proteção contra códigos maliciosos, os usuários da UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO devem adotar um comportamento seguro, reduzindo a probabilidade de infecção ou propagação de códigos maliciosos.

Os usuários da UNIMED PINDAMONHANGABA devem seguir as seguintes regras para proteção contra códigos maliciosos:



	Procedimento Sistêmico	Referência nº: SED-PS-TI-005	
		Estabelecido em: 14/07/2022 Válido até: 14/07/2024	
		Página 4 de 5	
Atividade: Códigos Maliciosos  Responsável: Coordenador de T.I.		Classificação: Interno	I

- Não tentar efetuar o tratamento e correção de códigos maliciosos por iniciativa própria;
- Reportar imediatamente a área de tecnologias da informação qualquer infecção ou suspeita de infecção por código malicioso;
- Não desenvolver, testar ou armazenar qualquer parte de um código malicioso de qualquer tipo, a menos que expressamente autorizado;
- Efetuar uma varredura com a ferramenta de proteção contra códigos maliciosos fornecida pela UNIMED PINDAMONHANGABA antes de utilizar arquivos armazenados em mídias removíveis, baixados da internet ou recebidos nos serviços de e-mail ou comunicadores instantâneos;
- Não habilitar MACROS para arquivos recebidos de fontes suspeitas, baixados da internet ou recebidos nos serviços de e-mail ou comunicadores instantâneos. Caso necessário, poderá ser solicitado o apoio da equipe de segurança da informação para validar se o arquivo representa ou não uma ameaça.

5 Papéis e responsabilidades

5.1 Setor de Tecnologia da Informação

É responsabilidade do setor de tecnologia da informação:

- Tratar casos de infecção ou suspeita de infecção por códigos maliciosos.

6 Sanções e punições

Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

Registros

Não se aplica.

DS

EB

DS

AMFLF

DS

JRPM

DS

JDDSG

DS

MUSM

DS

PL


DS

EMS

DS

ED

DS

	Procedimento Sistêmico	Referência nº: SED-PS-TI-005	
		Estabelecido em: 14/07/2022	
		Válido até: 14/07/2024	
		Página 5 de 5	
Atividade: Códigos Maliciosos		Classificação: Interno	I
Responsável: Coordenador de T.I.			

Anexos

Não se aplica.

Referências

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 1.5.1. 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/rn/RN\\_507\\_-\\_ANEXO\\_I\\_-\\_TAMANHO\\_CORRETO\\_Conferir\\_se\\_houve\\_altera%C3%A7%C3%A3o.pdf](https://www.ans.gov.br/images/stories/Legislacao/rn/RN_507_-_ANEXO_I_-_TAMANHO_CORRETO_Conferir_se_houve_altera%C3%A7%C3%A3o.pdf)  
SED-POL-TI-002 Política Geral da Segurança da Informação. Disponível no Sistema Sigquali.

Controle de Alterações

- Revisão “0” – Emissão Inicial.
- Revisão “1” – Emissão Inicial.
- Revisão “2” – Alteração no item 4.1, referencias e exclusão do item 7.

Comitê de Segurança da Informação

- Ana Maria Farias Leal Freire
- Dr. Eduardo Mayer Schmidt
- Drª Maura Aparecida da Silva
- Edmilson Braz Filho
- Jacqueline Romão Prado Morais
- João Diego dos Santos Guimarães
- Nathallia Matta S. Moreira
- Pablo da Silva Camargo