	Procedimento Sistêmico	Referência nº: SED-PS-TI-007	
		Estabelecido em: 26/10/2022 Válido até: 26/10/2024	
		Página 1 de 9	
Atividade: Gestão de Identidade e controle de acesso 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 Edemilson Antonio Donola
1	26/10/2022	Edmilson Braz Filho	Comitê de Segurança da Informação e Edemilson Antonio Donola	Dra. Maura Aparecida da Silva

Siglas e Definições

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

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

CSI - Comitê de segurança da informação – Grupo de trabalho multidisciplinar permanente, efetivado pela diretoria da UNIMED PINDAMONHANGABA, que tem por finalidade tratar questões ligadas à Segurança da Informação.


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

ERP - sigla para Enterprise Resource Planning e trata-se de um software integrado de gestão empresarial que reúne numa única solução as informações gerenciais.

GLPI - Gestão Livre de Parque de Informática - É uma solução web Open-source completa para gestão de ativos e Help Desk. Gerencia todos os problemas de inventário de ativos/hardwares e softwares e suporte ao usuário (Help Desk).

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.

Vulnerabilidade - Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações da UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO.

DS


DS
EMS

DS
EAD

DS
EB


DS
PL

DS
JDDSG

DS
JRPM

DS
AMFLF

DS
MMSM

	Procedimento Sistêmico	Referência nº: SED-PS-TI-007	
		Estabelecido em: 26/10/2022 Válido até: 26/10/2024	
		Página 2 de 9	
		Atividade: Gestão de Identidade e controle de acesso Responsável: Coordenador de T.I.	Classificação: Interno

Materiais

Computador com acesso a rede interna.

Abrangência

Aplica-se a todos Diretores, conselheiros, cooperados, colaboradores, terceiros contratados da Unimed Pindamonhangaba e seus recursos próprios.

Diretrizes

1. Introdução

A Norma de segurança da informação SED-PS-TI-007 complementa Política de Segurança da Informação (documento SED-POL-TI-002), definindo as diretrizes para garantir que o acesso aos ativos de informação ou sistemas de informação da UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO garanta níveis adequados de proteção.

2. Propósito


Estabelecer diretrizes para gestão de identidade e acesso aos ativos e sistemas de informação da UNIMED PINDAMONHANGABA.

3. Escopo

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

4. Diretrizes

4.1 Acesso a ativos e sistemas de informação

DS


DS
EMS

DS
EAD

DS
EB


DS
PL

DS
JDDSG

DS
JRPM

DS
AMFLF

DS
MUSM

	Procedimento Sistêmico	Referência nº: SED-PS-TI-007	
		Estabelecido em: 26/10/2022 Válido até: 26/10/2024	
		Página 3 de 9	
		Atividade: Gestão de Identidade e controle de acesso Responsável: Coordenador de T.I.	Classificação: Interno


A UNIMED PINDAMONHANGABA fornece a seus usuários autorizados contas de acesso que permitem o uso de ativos de informação, sistemas de informação e recursos computacionais como, por exemplo, rede corporativa ou sistema ERP.

As referidas contas de acesso são fornecidas exclusivamente para que os usuários possam executar suas atividades laborais.

Toda conta de acesso é **pessoal do usuário** a qual foi delegada e intransferível. Desta forma, o usuário é integralmente responsável por sua utilização, respondendo por qualquer violação ou ato irregular/ilícito, mesmo que exercido por outro indivíduo e/ou organização de posse de sua conta de acesso.

Os usuários devem adotar medidas de prevenção para garantir o acesso seguro a ativos e serviços de informação, incluindo:

- Não anotar ou registrar senhas de acesso em qualquer local, exceto nas ferramentas oficialmente fornecidas pela UNIMED PINDAMONHANGABA;
- Não utilizar sua conta, ou tentar utilizar qualquer outra conta, para violar controles de segurança estabelecidos pela UNIMED PINDAMONHANGABA;
- Não compartilhar a conta de acesso e senha com outro usuário, colaborador e/ou terceiro;
- Informar imediatamente a equipe de tecnologia da informação caso identifique qualquer falha ou vulnerabilidade que permita a utilização não autorizada de ativos de informação, sistemas e/ou recursos computacionais da UNIMED PINDAMONHANGABA;
- Usuários que tem acesso autorizado a privilégios administrativos em sistemas de informação devem possuir uma credencial específica para este propósito. A credencial privilegiada deve ser utilizada somente para a execução de atividades administrativas que requeiram esse nível de acesso, enquanto a conta de acesso comum deve ser utilizada em atividades do dia a dia;

DS


DS
EMS

DS
EAD

DS
EB


DS
PL

DS
JDDSG

DS
JRPM

DS
AMFLF

DS
MUSM

	Procedimento Sistêmico	Referência nº: SED-PS-TI-007	
		Estabelecido em: 26/10/2022 Válido até: 26/10/2024	
		Página 4 de 9	
		Classificação: Interno	I
Atividade: Gestão de Identidade e controle de acesso Responsável: Coordenador de T.I.			


- Qualquer utilização não autorizada ou tentativa de utilização não autorizada de credenciais e senhas de acesso a ativos/serviços de informação ou recursos computacionais será tratada como um incidente de segurança da informação, cabendo uma análise da infração pelo CSI e aplicação das sanções e punições previstas na Política Geral de Segurança da Informação (*documento SED-POL-TI-002*), conforme a gravidade da violação.

4.2 Senha de acesso

As senhas associadas às contas de acesso a ativos/serviços de informação ou recursos computacionais da UNIMED PINDAMONHANGABA são de **uso pessoal e intransferível**, sendo dever do usuário zelar por sua guarda e sigilo;

A UNIMED PINDAMONHANGABA adota os seguintes padrões para geração de senhas de acesso a seus ativos/serviços de informação ou recursos computacionais:

- A equipe de tecnologia da informação será responsável por fornecer senhas de acesso inicial ao usuário, que deve proceder com a troca imediata da mesma;
- As senhas possuem validade de 90 (noventa) dias. Passado este prazo, os sistemas solicitarão automaticamente a troca da senha;
- As senhas associadas a contas com privilégio não-administrativo serão compostas usando uma quantidade mínima de 8 (oito) dígitos, combinando letras maiúsculas e minúsculas, números e caracteres especiais;
- As senhas associadas a contas que possuem privilégio administrativo serão compostas usando uma quantidade mínima de 15 (quinze) dígitos, combinando letras maiúsculas e minúsculas, números e caracteres especiais;
- Após 5 (cinco) tentativas de acesso com senhas inválidas, a conta do usuário será bloqueada, assim permanecendo assim por, no mínimo, 30 (trinta) minutos;

DS


DS
EMS

DS
EAD

DS
EB


DS
PL

DS
JDDSG

DS
JRPM

DS
AMFLF

DS
MUSM

	Procedimento Sistêmico	Referência nº: SED-PS-TI-007	
		Estabelecido em: 26/10/2022 Válido até: 26/10/2024	
		Página 5 de 9	
Atividade: Gestão de Identidade e controle de acesso Responsável: Coordenador de T.I.		Classificação: Interno	I

- Os sistemas de informação manterão um histórico das últimas 3 (três) senhas utilizadas, não permitindo sua reutilização;
- Quando efetuada uma troca da senha, o usuário não pode realizar nova alteração dentro de um prazo mínimo de 7 (sete) dias. Caso seja necessário realizar alteração dentro deste período, o usuário deverá solicitar o apoio da equipe de tecnologia da informação.


Quando criando uma nova senha, usuários devem estar atentos as seguintes recomendações:

- Não utilizar nenhuma parte de sua credencial na composição da senha;
- Não utilizar qualquer um de seus nomes, sobrenomes, nomes de familiares, colegas de trabalho ou informação a seu respeito de fácil obtenção como, por exemplo, placa do carro, data de aniversário, ou endereço;
- Não utilizar repetição ou sequência de caracteres, números ou letras;
- Qualquer parte ou variação do nome UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO;
- Qualquer variação dos itens descritos acima como duplicação ou escrita invertida.

4.3 Autorização de acesso (privilégios de acesso)

A autorização e o nível permitido de acesso ativos/serviços de informação da UNIMED PINDAMONHANGABA é feita com base em perfis que definem o nível de privilégio dos usuários.

O acesso à ativos/serviços de informação é fornecido a critério da UNIMED PINDAMONHANGABA, que define permissões baseadas nas necessidades laborais dos usuários definidas pela coordenação do setor.

DS


DS
EMS

DS
EAD

DS
EB


DS
PL

DS
JDDSG

DS
JRPM

DS
AMFLF

DS
MUSM

	Procedimento Sistemico	Referência nº: SED-PS-TI-007	
		Estabelecido em: 26/10/2022 Válido até: 26/10/2024	
		Página 6 de 9	
		Atividade: Gestão de Identidade e controle de acesso Responsável: Coordenador de T.I.	Classificação: Interno

Autorizações de acesso a perfis são fornecidas e/ou revogadas com base na solicitação dos coordenadores de cada colaborador. As solicitações devem ser encaminhadas a equipe de tecnologia da informação via chamado (GLPI). *Para abertura do chamado seguir o processo estabelecido no documento **SED-PS-TI-001 Aberturas de chamados no GLPI**.*

Os usuários devem ainda observar as seguintes diretrizes:

A seu critério exclusivo, a UNIMED PINDAMONHANGABA pode ativar uma cota para armazenamento de arquivos em sua infraestrutura computacional local ou serviços de armazenamento remoto (nuvem). Caso o usuário necessite de mais espaço, deve realizar uma solicitação ao departamento de Tecnologia da Informação *através do GLPI*;

É expressamente proibido o armazenamento de informações de caráter pessoal, que infrinjam direitos autorais ou que não sejam de interesse da UNIMED PINDAMONHANGABA tanto na infraestrutura computacional local ou serviços de armazenamento remoto (nuvem);

Usuários não devem ter expectativa de privacidade quanto aos arquivos armazenados na infraestrutura computacional local ou serviços de armazenamento remoto (nuvem) da UNIMED PINDAMONHANGABA.


4.4 Acesso Físico

As regras e determinações para o acesso físico às dependências da UNIMED PINDAMONHANGABA seguem o procedimento sistêmico **SED-PS-AUT-006 Acesso físico a Operadora**.

Existem câmeras de monitoramento em corredores de acesso e na Sala dos Servidores auxiliando o controle de acesso. (**SED-PS-TI-009 Monitoramento** - Item 4.2).

4.5 Papéis e Responsabilidades

4.5.1 Departamento Pessoal


DS


DS


DS



DS



DS


DS


DS


DS


DS


	Procedimento Sistêmico	Referência nº: SED-PS-TI-007	
		Estabelecido em: 26/10/2022 Válido até: 26/10/2024	
		Página 7 de 9	
		Atividade: Gestão de Identidade e controle de acesso Responsável: Coordenador de T.I.	Classificação: Interno

É responsabilidade do departamento pessoal (Recursos Humanos):

- Reportar em tempo hábil o desligamento de empregados da UNIMED PINDAMONHANGABA a equipe de tecnologia da informação para que contas de acesso possam ser revogadas;
- Apoiar a gestão de identidades enviando relatórios periódicos sobre colaboradores desligados ou que mudaram de posição na UNIMED PINDAMONHANGABA;
- Apoiar a revisão periódica da validade de credenciais de acesso a ativos/sistemas de informação fornecendo informações sobre os empregados.

4.5.2 Gestores e Coordenadores


É responsabilidade dos gestores e coordenadores:

- Solicitar a equipe de tecnologia da informação a concessão de acesso novos empregados ou empregados que necessitem de novos acessos conforme mudanças em suas atividades laborais;
- Solicitar a equipe de tecnologia da informação concessão de acesso a terceiros/prestadores de serviços contratados justificando a necessidade de acesso a ativos/sistemas de informação;
- Informar a equipe de tecnologia da informação quando ao encerramento do contrato com terceiros/prestadores de serviços contratados que tenham a ativos/sistemas de informação.

4.5.3 Setor de Tecnologia da Informação

É responsabilidade do setor de Tecnologia da Informação:

- Receber e analisar solicitações para criação de contas de acesso ou fornecimento de privilégios para usuários de empregados, terceiros/prestadores de serviços;

	Procedimento Sistemico	Referência nº: SED-PS-TI-007	
		Estabelecido em: 26/10/2022 Válido até: 26/10/2024	
		Página 8 de 9	
		Classificação: Interno	I
Atividade: Gestão de Identidade e controle de acesso Responsável: Coordenador de T.I.			

- Conceder, quando autorizado, o acesso aos usuários de empregados, terceiros/prestadores de serviço, conforme indicado pelos gestores da informação;
- Revogar, quando solicitado, o acesso dos usuários de empregados, terceiros/prestadores de serviço, conforme indicado pelos gestores da informação;
- Apoiar a revisão periódica da validade de credenciais de acesso a ativos/sistemas de informação dos usuários de empregados, terceiros/prestadores de serviço fornecendo informações sobre os privilégios atualmente efetivados em ativos/sistemas de informação.

5. Sanções e Punições

Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação (documento SED-POL-TI-002).

Registros


Não se aplica.

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)

DS


DS


DS



DS



DS


DS


DS


DS


DS


	Procedimento Sistêmico	Referência nº: SED-PS-TI-007	
		Estabelecido em: 26/10/2022 Válido até: 26/10/2024	
		Página 9 de 9	
		Atividade: Gestão de Identidade e controle de acesso Responsável: Coordenador de T.I.	Classificação: Interno

SED-POL-TI-002 Política Geral da Segurança da Informação. Disponível para consulta no sistema de gestão da qualidade da Operadora e do Hospital 10 de Julho.

Controle de Alterações

Revisão 0 – Inicial.
Revisão 1 – Alteração no cabeçalho (classificação do documento), Siglas e Definições, Abrangência, Diretrizes – item 1, 3, 4.1, 4.3 e 5, Registros e Referências. Inclusão do item 4.4. Excluído o item 6.

DS
ED

Comitê de Segurança da Informação:

DS
AMFLF

Ana Maria Farias Leal Freire

DS
JDDSG

João Diego dos Santos Guimarães

DS
EB

Edmilson Braz Filho

DS
P

Drª Maura Aparecida da Silva

DS
EMS

Dr. Eduardo Mayer Schmidt

DS
NMSM

Nathallia Matta S. Moreira

DS
JRPm

Jacqueline Romão Prado Morais

DS
PC

Pablo da Silva Camargo