


| | | | |
|---|------------------------|---|---|
|  | Procedimento Sistêmico | Referência nº: SED-PS-TI-010 | |
| | | Estabelecido em: 26/10/2022 Válido até: 26/10/2024 | |
| | | Página 1 de 10 | |
| Atividade: Resposta a incidentes 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 Couppê Schmidt e Edemilson Antonio Donola |
| 1 | 26/10/2022 | Edmilson Braz Filho e Pablo da Silva Camargo | Comitê de Segurança da Informação | Dra. Maura Aparecida da Silva e Edemilson Antonio Donola |

Siglas e Definições

ANPD – *Autoridade Nacional de Proteção de Dados*

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.


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

D.P.O. – *Encarregado de proteção de dados.*

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.

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

DS


DS
EMS

DS
EB


DS
PC

DS
JDDSG

DS
JRPM

DS
AMFLF

DS
MUSM

| | | | |
|---|------------------------|---|---|
|  | Procedimento Sistêmico | Referência nº: SED-PS-TI-010 | |
| | | Estabelecido em: 26/10/2022 Válido até: 26/10/2024 | |
| | | Página 2 de 10 | |
| | | Classificação: Interno | I |
| Atividade: Resposta a incidentes Responsável: Coordenador de T.I. | | | |

Materiais

Computador com acesso à rede.

Abrangência

Aplica-se a *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-010 complementa a Política de Segurança da Informação (*documento SED-POL-TI-002*), definindo as diretrizes para responder eventos ou incidentes de segurança estejam impactando ou possam vir a impactar ativos/serviços de informação ou recursos computacionais da UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO.


2. Propósito

Estabelecer diretrizes para garantir a resposta e tratamento adequados a incidentes de segurança da informação que possam impactar ativos/serviços de informação ou recursos computacionais da UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO.

3. Escopo

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

4. Diretrizes

DS


DS
EMS

DS
EB


DS
PL

DS
JDDSG

DS
JRPM

DS
AMFLF

DS
MUSM

| | | | |
|---|------------------------|---|---|
|  | Procedimento Sistêmico | Referência nº: SED-PS-TI-010 | |
| | | Estabelecido em: 26/10/2022 Válido até: 26/10/2024 | |
| | | Página 3 de 10 | |
| | | Classificação: Interno | I |
| Atividade: Resposta a incidentes Responsável: Coordenador de T.I. | | | |


4.1 Incidentes de segurança da informação

Todas as ocorrências que possam vir a ter impacto negativo sobre a confidencialidade, integridade ou disponibilidade dos ativos/serviços de informação ou recursos computacionais da UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO são caracterizadas como um incidente de segurança da informação, devendo as referidas ocorrências serem tratadas de maneira a minimizar qualquer tipo de impacto e recuperar as características de segurança da informação dos itens afetados.

Incidentes de segurança devem ser priorizados com base na criticidade dos ativos/serviços de informação ou recursos computacionais afetados, combinada com a estimativa de impacto prevista.

Os Incidentes podem ser de vários tipos, como por exemplo:

- A. Vazamento de Dados Pessoais.** É o Incidente no qual Dados Pessoais ou corporativos são indevidamente expostos e disponibilizados, por meios físicos ou digitais, para um número indeterminado de pessoas, no Brasil ou em qualquer país;
- B. Negação de Serviço.** É o Incidente no qual o acesso (lógico ou físico) a um sistema que armazene Dados Pessoais ou corporativos é prejudicado ou impossibilitado, de forma que a integridade dos Dados Pessoais ou do negócio (existência e/ou veracidade) pode ser comprometida permanentemente, dada a indisponibilidade do acesso;
- C. Acesso Não Autorizado.** É o Incidente no qual o acesso (lógico ou físico) a um sistema que possua Dados Pessoais ou corporativos é tentado ou obtido, sem que se tenha a devida autorização para tal acesso. Considera-se acesso não autorizado qualquer acesso cuja permissão para conexão, leitura, gravação, autenticação, modificação, eliminação ou criação não tenha sido concedida; e
- D. Uso Inapropriado.** É o Incidente no qual há a violação das políticas de uso de dados, informações e sistemas da Empresa, incluindo a Política de Segurança da Informação.

DS


DS
EMS

DS
EB


DS
PL

DS
JDDSG

DS
JRPm

DS
AMFLF

DS
MUSM

| | | | |
|---|------------------------|---|---|
|  | Procedimento Sistêmico | Referência nº: SED-PS-TI-010 | |
| | | Estabelecido em: 26/10/2022 Válido até: 26/10/2024 | |
| | | Página 4 de 10 | |
| Atividade: Resposta a incidentes Responsável: Coordenador de T.I. | | Classificação: Interno | I |

Todos os incidentes de segurança da informação ou suspeitas de incidentes de segurança da informação **devem ser imediatamente comunicados à área de Tecnologia da Informação, presencialmente, por e-mail ou telefone, e o comunicante deve registrar a ocorrência no GLPI, com as seguintes descrições:**

| |
|---|
| <p><i>Tipo: Incidente</i></p> <p><i>Categoria: Incidente de segurança</i></p> |
|---|

*Para registrar essas ocorrências consultar o processo estabelecido no documento **SED-PS-TI-001** **Abertura de chamados no GLPI.***


A área de Tecnologia da Informação deve determinar a criticidade do incidente e, quando pertinente, comunicar o *Comitê de Segurança da Informação* e o Time de resposta a incidentes de segurança da informação (conforme item 4.2).

Na ocorrência de um incidente de segurança da informação, ativos/serviços de informação ou recursos computacionais com suspeita de ter sua segurança comprometida, devem ser isolados do ambiente corporativo, de forma a garantir a contenção do incidente.

A extensão dos danos do incidente de segurança deve ser avaliada para, em seguida, ser identificado o melhor curso de ação para erradicação completa do incidente e restauração dos ativos de informação afetados.

Após a erradicação completa do incidente, deve ser realizada uma revisão completa da ocorrência, identificando o nível real de impacto, vulnerabilidades exploradas, a efetividade do tratamento aplicado e a necessidade de maiores ações para evitar a recorrência do incidente.

As respectivas avaliações e tratamentos ficarão disponíveis, evidenciadas e arquivadas no chamado via GLPI na aba acompanhamento e serão rastreados via indicadores, conforme classificação da categoria: incidente de segurança.

DS


DS
EMS

DS
EB


DS
PL

DS
JDDSG

DS
JRPM

DS
AMFLF

DS
MUSM

| | | | |
|---|------------------------|---|---|
|  | Procedimento Sistêmico | Referência nº: SED-PS-TI-010 | |
| | | Estabelecido em: 26/10/2022 Válido até: 26/10/2024 | |
| | | Página 5 de 10 | |
| Atividade: Resposta a incidentes Responsável: Coordenador de T.I. | | Classificação: Interno | I |

4.2 Priorização do Incidente e Procedimentos para Resposta

Uma vez que o Incidente seja identificado e classificado, é necessário priorizá-lo conforme o nível de risco oferecido à Unimed Pindamonhangaba Cooperativa de Trabalho Médico e aos titulares dos Dados Pessoais ou corporativos eventualmente afetados e a gravidade da ocorrência. O impacto do Incidente deve ser aferido da seguinte forma:

Sensibilidade:


| | | | | |
|---|-------|-----------------|-----------------|-----------------|
| volume de Dados Pessoais ou corporativos expostos | Alto | Alta Gravidade | Alta Gravidade | Alta Gravidade |
| | Médio | Média Gravidade | Alta Gravidade | Alta Gravidade |
| | Baixo | Baixa Gravidade | Média Gravidade | Média Gravidade |
| | | Baixa | Média | Alta |
| sensibilidade dos dados pessoais ou corporativos afetados | | | | |

Legenda: Volume Baixo (2%), Médio (>2 e <10), Alto (10 ou +)

De acordo com a matriz acima definida, a Equipe de Resposta a Incidentes deve tomar as seguintes ações, simultaneamente ou, quando não for possível, em rápida sucessão:

Baixa Gravidade

- 1. tão logo tenha ciência, trabalhar prioritariamente na resolução do Incidente;
- 2. tomar as medidas adequadas para minimizar os efeitos causados pelo Incidente e para promover sua rápida correção;
- 3. comunicar o Time de resposta a incidentes de segurança da informação presencialmente, por e-mail ou telefone e registrar ocorrência no GLPI (Sistema de Chamados - SED-PS-TI-001);
- 4. comunicar as Áreas Envolvidas, que devem estar à disposição da Equipe de Resposta;
- 5. uma vez que as medidas de resolução sejam tomadas, documentar o Incidente; e

DS


DS
EMS

DS
EB


DS
PL

DS
JDDSG

DS
JRPm

DS
AMFLF

DS
MUSM

| | | | |
|---|------------------------|---|---|
|  | Procedimento Sistêmico | Referência nº: SED-PS-TI-010 | |
| | | Estabelecido em: 26/10/2022 Válido até: 26/10/2024 | |
| | | Página 6 de 10 | |
| Atividade: Resposta a incidentes Responsável: Coordenador de T.I. | | Classificação: Interno | I |


6. reunir-se para analisar o Incidente e antecipar, prevenir e melhor identificar Incidentes semelhantes no futuro, devendo esta reunião ser transcrita em ata, que deve ser apresentada ao Comitê de Segurança da Informação.

Média Gravidade

- 1. tão logo tenha ciência, trabalhar de forma exclusiva na resolução do Incidente;
- 2. tomar as medidas imediatas para minimizar os efeitos causados pelo Incidente e para promover sua rápida correção e, se a correção não for possível de forma imediata, deve adotar as medidas temporárias para minimização de riscos;
- 3. comunicar o Time de resposta a incidentes de segurança da informação presencialmente, por e-mail ou telefone e registrar ocorrência no GLPI (Sistema de Chamados - SED-PS-TI-001);
- 4. comunicar as Áreas Envolvidas, que devem estar à disposição para atender, com prioridade, a Equipe de Resposta;
- 5. uma vez que as medidas de resolução sejam tomadas, documentar o Incidente, o mais breve possível;
- 6. reunir-se o mais breve possível para analisar o Incidente e antecipar, prevenir e melhor identificar Incidentes semelhantes no futuro, devendo esta reunião ser transcrita em ata documentada, que deve ser apresentada ao Comitê de Segurança da Informação; e
- 7. realizar, imediatamente, treinamento interno com as áreas afetadas para conscientizar os seus Colaboradores sobre o Incidente e medidas preventivas.

Alta Gravidade

- 1. tão logo tenha ciência, trabalhar de forma exclusiva na resolução do Incidente;
- 2. imediatamente comunicar os gestores responsáveis pelas Áreas Envolvidas, os quais, em conjunto com outra pessoa de cada uma das respectivas Áreas Envolvidas, devem atuar de forma exclusiva no suporte à Equipe de Resposta e preferencialmente no mesmo local em que a Equipe de Resposta esteja trabalhando; Registrar ocorrência no GLPI (Sistema de Chamados - SED-PS-TI-001);
- 3. uma vez que as medidas de resolução sejam tomadas, documentar o Incidente, imediatamente;

DS


DS
EMS

DS
EB


DS
PL

DS
JDDSG

DS
JRPM

DS
AMFLF

DS
MUSM

| | | | |
|---|------------------------|---|---|
|  | Procedimento Sistêmico | Referência nº: SED-PS-TI-010 | |
| | | Estabelecido em: 26/10/2022 Válido até: 26/10/2024 | |
| | | Página 7 de 10 | |
| Atividade: Resposta a incidentes Responsável: Coordenador de T.I. | | Classificação: Interno | I |

- 4. reunir-se, imediatamente, para avaliar o Incidente e antecipar, prevenir e melhor identificar Incidentes semelhantes no futuro, devendo esta reunião ser transcrita em ata, que deve ser apresentada ao Comitê de Segurança da Informação;
- 5. realizar, imediatamente, treinamento interno com todos os Colaboradores da Empresa para conscientizar sobre o Incidente e medidas preventivas; e
- 6. comunicar, imediatamente, os Colaboradores internos sobre medidas preventivas.

4.3 Time de resposta a incidentes de Segurança da Informação

O time de resposta a incidentes de segurança da informação da UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO deve ser composto por, no mínimo, representantes das seguintes áreas:

- D.P.O. (Data Protection Officer);
- Coordenação de Tecnologia da Informação;
- Coordenação de Recursos Humanos;
- Coordenação Jurídica.


Conforme a natureza do incidente, colaboradores de qualquer setor da UNIMED PINDAMONHANGABA podem ser convocados a participar do time de resposta a incidentes de segurança da informação.

4.4 Disseminação de informação sobre incidentes de Segurança da Informação

Nenhum tipo de informação sobre incidentes e ocorrências de segurança da informação pode ser divulgado para entidades ou pessoas externas a UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO sem aprovação expressa e formal da diretoria.

5 Papéis e Responsabilidades

5.1 Setor de Tecnologia da Informação

| | | | |
|---|------------------------|---|---|
|  | Procedimento Sistêmico | Referência nº: SED-PS-TI-010 | |
| | | Estabelecido em: 26/10/2022 Válido até: 26/10/2024 | |
| | | Página 8 de 10 | |
| | | Classificação: Interno | I |
| Atividade: Resposta a incidentes Responsável: Coordenador de T.I. | | | |

É responsabilidade do SETOR DE TECNOLOGIA DA INFORMAÇÃO:

- Comunicar prontamente o Time de resposta a incidentes de segurança da informação da UNIMED PINDAMONHANGABA sobre eventos e incidentes de segurança.

5.2 Time de resposta a incidentes de Segurança da Informação

É responsabilidade do TIME DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO:

- Apoiar a equipe de tecnologia da informação no tratamento de ocorrências e incidentes de segurança da informação, fornecendo orientação e direcionamento estratégico dentro da área de especialidade de cada um dos participantes do time de resposta a incidentes de segurança da informação;
- Aconselhar a diretoria da UNIMED PINDAMONHANGABA COOPERATIVA DE TRABALHO MÉDICO sobre quais informações de eventos e incidentes de segurança da informação podem ser divulgadas para públicos internos e externos e comunicados à ANPD.


5.3 Gerência Administrativa/Financeira

É responsabilidade da GERÊNCIA ADMINISTRATIVA/FINANCEIRA:

Aprovar qualquer tipo de comunicação ou disseminação total ou parcial de informações sobre ocorrências e incidentes de segurança da informação para qualquer parte ou público.

6. Sanções e Punições

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

DS


DS
EMS

DS
EB


DS
PL

DS
JDDSG

DS
JRPM

DS
AMFLF

DS
MUSM

| | | | |
|---|------------------------|---|---|
|  | Procedimento Sistêmico | Referência nº: SED-PS-TI-010 | |
| | | Estabelecido em: 26/10/2022 Válido até: 26/10/2024 | |
| | | Página 9 de 10 | |
| Atividade: Resposta a incidentes Responsável: Coordenador de T.I. | | Classificação: Interno | I |

Registros

Notificações de incidentes de segurança da informação registradas no GLPI.
Atas de reunião do Comitê de Segurança da Informação.

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_alter%C3%A7%C3%A3o.pdf)
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” – Emissão Inicial.
Revisão “1” – Alteração no cabeçalho (classificação do documento), Siglas e Definições, Abrangência, Diretrizes – item 1, 3, 4.1, 4.2, 4.3, 5.2 e 6, Registros e Referências. Exclusão do item 7.

DS


DS
EMS

DS
EB


DS
PL

DS
JDDSG

DS
JRPm

DS
AMFLF

DS
MUSM

| | | | |
|---|------------------------|--|---------------------------|
|  | Procedimento Sistêmico | Referência nº: SED-PS-TI-010 | |
| | | Estabelecido em: 26/10/2022 Válido até: 26/10/2024 | |
| | | Página 10 de 10 | |
| | | Atividade: Resposta a incidentes Responsável: Coordenador de T.I. | Classificação: Interno |

Comitê de Segurança da Informação:

^{DS}
AMFLF

Ana Maria Farias Leal Freire

^{DS}
EB

Edmilson Braz Filho

^{DS}
EMS


Dr. Eduardo Mayer Schmidt

^{DS}
JRPM

Jacqueline Romão Prado Moraes

^{DS}
JDDSG

João Diego dos Santos Guimarães

^{DS}


Drª Maura Aparecida da Silva

^{DS}
NMSM

Nathallia Matta S. Moreira

^{DS}
PC

Pablo da Silva Camargo