RESUMO DAS REVISÕES		
Edição	**Data**	**Alteração**
01	05/05/2025	Emissão inicial
02	15/05/2026	Não houve alterações

1. Objetivo

O objetivo desta política é garantir que os ativos de informação sejam identificados adequadamente e que os controles de proteção recomendados para estes ativos de informação estejam em vigor.

Para manter a segurança e continuidade do negócio da Unimed de Tupã em sua missão é fundamental mapear e monitorar os ativos tecnológicos, para maior controle da organização, auxiliando na aplicação de atualizações, implementação de controles de segurança e gestão de risco da organização. Auxiliando também na recuperação de incidentes.

Os ativos de informação da Unimed de Tupã devem ser classificados a fim de permitir a definição de níveis de segurança para eles. Cada ativo de informação deverá ter um "dono", no qual realizará a classificação do ativo de informação e deverá ser registrado em uma base de dados gerenciada de forma centralizada.

2. Aplicação

Esta política se aplica a todos os Diretores, Gestores, Colaboradores e demais partes interessadas que se relacionem com a Unimed de Tupã em todas suas áreas de atendimento.

3. Definições

ATIVOS DE INFORMAÇÃO - meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

INCIDENTE - interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido,

ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

4. Responsabilidades

Alta Direção: Aprovar e revisar esta política, garantir recursos para sua implementação e cumprimento.

Equipe de TI: Implementar e manter as soluções corporativas de comunicação, garantir a segurança e privacidade das informações, monitorar o uso das ferramentas e realizar auditorias.

Colaboradores: Utilizar as soluções corporativas de comunicação de forma responsável, seguindo as diretrizes estabelecidas nesta política e reportando qualquer incidente de segurança.

5. Descrição

PRINCÍPIOS GERAIS

- ✓ A Política de Gestão de Ativos de informação deve estar alinhada com à Política de Segurança da Informação da Unimed de Tupã.
- ✓ A Política de Gestão de Ativos de informação deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.
- ✓ O processo de mapeamento de ativos de informação deve estruturar e manter um registro de ativos de informação, destinados a subsidiar os processos de gestão de risco, de gestão de continuidade e de gestão de mudanças nos aspectos relativos à segurança da informação.
- ✓ As rotinas de inventário e mapeamento de ativos de informação devem ser orientadas para a identificação dos ativos de informação da organização, a fim de manter o escopo da organização mapeado e documentado.
- ✓ O processo de mapeamento de ativos de informação deve considerar, preliminarmente, os objetivos estratégicos da organização, seus processos internos, os requisitos legais e sua estrutura organizacional.
- ✓ O registro de ativos de informação resultante do processo de mapeamento de ativos de informação deverá conter: os responsáveis (proprietários e custodiantes) de cada ativo de informação; as informações básicas sobre

os requisitos de segurança da informação de cada ativo de informação; os contêineres de cada ativo de informação; as interfaces de cada ativo de informação e as interdependências entre eles.

- ✓ Os seguintes ativos de informação devem ser considerados no processo de mapeamento de ativos de informação:
  a) Ativos físicos;
  b) Bancos de dados;
  c) Dispositivos móveis;
  d) Hardwares;
  e) Mídias removíveis;
  f) Níveis de permissões;
  g) Serviços;
  h) Softwares.

DIRETRIZES

- ✓ Informações ou ativos de informação de instalações de processamento de informações devem ser inventariados e documentados e esse registro deve ser mantido atualizado.
- ✓ A categorização do inventário deve ser aprovada pelas partes apropriadas ou autoridade de autorização
- ✓ A organização empregará o uso de mecanismos automatizados para identificar sistemas autorizados e não autorizados, incluindo hardware ou software.
- ✓ A organização deve assegurar que os ativos de informação inventariados possuam contrato de suporte em vigor.
- ✓ A organização empregará o uso de ferramentas de descoberta ativa e/ou passiva para identificar dispositivos conectados à rede da instituição e automaticamente atualizar o inventário de ativos.
- ✓ A organização utilizará ferramentas de inventário de software, quando possível, em toda a organização para automatizar a descoberta e documentação do software instalado.
- ✓ A organização assegurará que exista um processo semanal para lidar com ativos não autorizados.
- ✓ A organização utilizará controles técnicos em todos os ativos para garantir que apenas software autorizado seja executado, sendo estes reavaliados semestralmente ou com mais frequência.
- ✓ A organização utilizará controles técnicos para garantir que apenas bibliotecas e scripts autorizados, e assinados digitalmente tenham permissão para serem executados.
- ✓ A organização utilizará ferramenta de gerenciamento de endereços IP - ex.: Dynamic Host Configuration Protocol (DHCP) - para atualizar o inventário

de ativos da instituição.

- ✓ O inventário também deverá incluir atualizações ou remoções dos softwares, bem como dos sistemas de informação.
- ✓ As atualizações e novas versões de softwares devem ser avaliadas e aprovadas antes da instalação.
- ✓ Cada ativo de informação (por exemplo, desktops, laptops, servidores, tablets), quando aplicável, deve ter uma etiqueta afixada ao dispositivo com esse identificador.

Registre o identificador de ativos da informação juntamente com outras informações relevantes no inventário de TI. Isso inclui:

a) Identificador de ativos
b) Data da compra
c) Preço de compra
d) Descrição do item
e) Fabricante
f) Número do modelo
g) Número de série
h) Nome do proprietário do ativo corporativo (por exemplo, administrador, usuário), função ou unidade de negócios, quando aplicável.
i) Localização física do ativo da empresa, quando aplicável
j) Endereço físico (controle de acesso à mídia (MAC))
k) Endereço de Protocolo de Internet (IP)
l) Data de validade da garantia/vida útil
m) Qualquer informação de licenciamento relevante

No caso de softwares instalados na organização deve ser registrado no inventário informações como:

a) Título do software;
b) Desenvolvedor ou editor de software;
c) Data de aquisição;
d) Data de instalação;
e) Duração do uso;
f) Finalidade comercial;
g) Lojas de aplicativos;
h) Versões;
i) Mecanismo de implantação;
j) Data de fim do suporte, se conhecida;
k) Qualquer informação de licenciamento relevante;
l) Data de descomissionamento.

22. Das responsabilidades do proprietário do processo:
    a) Identificar potenciais ameaças aos ativos de informação;
    b) Identificar vulnerabilidades dos ativos de informação;
    c) Consolidar informações resultantes da análise do nível de segurança da informação de cada ativo de informação ou de grupos de ativos de informação em um relatório;
    d) Avaliar os riscos dos ativos de informação ou do grupo de ativos de informação.
    e) Indivíduos que requerem acesso aos sistemas de informação devem seguir o procedimento adequado para receber tal acesso, como descritos na política de controle de acesso e catalogadas no sistema de gestão de ativos.
    f) Os processos em torno do gerenciamento de mudança e de configuração também serão estabelecidos e monitorados.
    g) Todos os ativos de informação devem ser devolvidos após a rescisão do contrato de trabalho ou contrato.

23. A criticidade dos ativos de informação críticos da organização é determinada pelo:

a) Requisitos legais;
b) Pelo valor financeiro;
c) Pelo seu potencial de agregar valor ao negócio;
d) Por sua vida útil;

24. Classificação de Nível de Acesso das Informações:
    a) Todos os ativos de informação devem ser classificados de acordo com seu nível de acesso, a fim de assegurar o direito fundamental de acesso à informação, bem como dispor sobre a devida restrição de acesso sobre informações sigilosas, conforme previsto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI) e demais normas aplicáveis.
    b) As informações armazenadas, transmitidas, processadas ou que se encontram sob a guarda dos ativos de da Unimed de Tupã
    c) Independentemente de seu formato e suporte, devem ser classificadas segundo seu nível de acesso, de acordo com a legislação pertinente, sobretudo com as disposições da LAI, do Decreto nº 7.724, de 16 de maio de 2012, e orientações ou normas complementares editadas por órgãos competentes.
    d) A classificação de nível de acesso das informações deve observar as diretrizes constantes na LAI, Decreto nº 7.724, de 16 de maio de 2012 e outros normativos complementares que abordam o assunto.

As informações devem ser classificadas conforme os seguintes níveis de acesso:

a) Pública, com acesso irrestrito e visível a todos os usuários, inclusive pelo público externo;
b) Restrita, quando se tratar de informação sigilosa não classificada em grau de sigilo, protegidas por demais hipóteses legais de restrição de acesso; e
c) Sigilosa classificada em grau de sigilo, nos termos do art. 23 da Lei nº 12.527/2011, subdividida nos graus ultrassecreto, secreto ou reservado.
d) Os ativos de informação serão rotulados e manuseados com base nos procedimentos apropriados de classificação de nível de acesso de informações usados pela organização.

25. Manipulação de mídia:
a) A mídia removível também deve ser gerenciada pelo mesmo procedimento de classificação de ativos de informação usado pela organização.
b) A mídia removível deve ser protegida contra acesso não autorizado e uso indevido durante o uso e em trânsito, e deve ser descartada com segurança, usando os procedimentos apropriados.
c) A mídia contendo informações confidenciais e internas do [Órgão ou entidade] devem ser protegidas contra acesso não autorizado, uso indevido, corrupção durante o transporte e, preferencialmente, com o uso de criptografia.

26. Uso aceitável:
a) Padrões ou diretrizes para o uso aceitável de ativos devem ser documentados para indicar o que os usuários dos ativos de informação podem ou não fazer.
b) Os seguintes itens devem ser cobertos nas diretrizes de uso aceitáveis:
c) Uso do computador e dos sistemas de informação;
d) Uso de softwares e dados;
e) Uso da Internet e e-mail;
f) Uso do telefone;
g) Uso de equipamentos e materiais de escritório.
h) Como requisito de acesso ao ativo de informação e como componente do treinamento de conscientização de segurança, todos os usuários dos ativos de informação, sejam funcionários ou terceiros, serão obrigados a fornecer aceitação assinada das diretrizes de uso aceitáveis

6. Monitoramento

7. Distribuição de Cópias

Política disponível no Quallix

8. Registros

Política disponível no Quallix

9. Anexos

Não há

10. Referências

Aprovação

ANTONIO CARLOS ANDRADE:00190337885

Assinado de forma digital por ANTONIO CARLOS ANDRADE:00190337885
Dados: 2026.05.14 08:59:22 -03'00'

Presidente