Histórico de Versões e Alterações				
Versão	Data	Responsável	Tipo de Alteração	Revisor/Aprovador
1	17/11/2025	Larissa	Criação da Política	Ageu

Sumário

1. Objetivo

O objetivo deste procedimento é estabelecer um processo técnico e operacional padrão para garantir o inventário, a instalação segura, a atualização (patching) e o descomissionamento de todos os dispositivos médicos conectados (IoMT) à rede do Hospital LISA.

Este processo visa proteger a segurança do paciente, a confidencialidade, integridade e disponibilidade dos dados, especialmente Dados Pessoais Sensíveis de saúde e a estabilidade da rede.

2. Escopo

Este procedimento se aplica a todos os dispositivos médicos que possuem capacidade de conexão de rede (com ou sem fio) e que interagem com pacientes ou Dados Pessoais Sensíveis de pacientes.

a. **Inclui:** Bombas de infusão, monitores de sinais vitais, ventiladores, máquinas de Raio-X digital, Tomografia, Ressonância Magnética e carrinhos de telemedicina.
b. **Exclui:** Estações de trabalho padrão ou dispositivos pessoais e ativos que não se conectam à rede.

3. Responsabilidades

A segurança do IoMT requer uma estrutura de responsabilidade compartilhada:

Área	Atribuição no Ciclo de Vida do IoMT
Engenharia Clínica	Proprietária do dispositivo (hardware). Lidera a aquisição, manutenção, calibração, contato com o fornecedor e o processo de descomissionamento.
Equipe de TI	Custodiante da Informação. Gerencia a configuração

(Infraestrutura)	da rede (VLAN, Wi-Fi, firewall) e o gerenciamento técnico do inventário (CMDB).
Equipe de Segurança da Informação (SI)	Define os requisitos de segurança, realiza a análise de risco, audita a configuração e lidera o monitoramento e a resposta a incidentes de segurança.
Equipe Clínica/Assistencial	Usuário Final. Responsável pelo uso correto do equipamento e por reportar imediatamente qualquer anomalia ou mau funcionamento à SI e à Engenharia Clínica.

4. Fases do Procedimento

4.1. Fase 1: Aquisição e Avaliação de Risco

Esta fase é crucial, pois define o risco que o hospital aceita gerenciar.

a. A Engenharia Clínica deve envolver a Equipe de SI no planejamento de qualquer nova aquisição de equipamento conectado.

b. A Equipe de SI deve solicitar e analisar um Questionário de Segurança do Fabricante. Este documento é usado para avaliar a capacidade do dispositivo de cumprir os requisitos de segurança do hospital.

c. A SI deve usar este questionário para verificar:

i. Se o dispositivo armazena Dados Pessoais Sensíveis, o que aumenta a criticidade da Fase 4 (Sanitização).

ii. A disponibilidade e o processo de atualizações de segurança (patches).

iii. O Sistema Operacional utilizado (para identificar o risco de se tornar legado ou sem suporte do fabricante).

d. É vedada a aquisição de dispositivos cuja senha de administrador ou serviço de fábrica não possa ser alterada.

e. Além do previamente citado, passam a ser requisitos mínimos no contrato de compra:

i. Garantia de suporte contínuo e atualizações de segurança durante todo o ciclo de vida útil do equipamento

ii. Definição de Acordo de Nível de Serviço (SLA) com prazos máximos para a disponibilização de correções (*patches*) após a identificação de uma vulnerabilidade;

iii. Obrigação de divulgação responsável e notificação proativa ao Hospital LISA sobre quaisquer vulnerabilidades identificadas no produto;

iv. Obrigatoriedade de fornecimento do questionário de segurança do fabricante devidamente preenchido antes da aquisição;

v. Existência de um plano formal de *recall* para recolhimento ou substituição do equipamento em casos de falhas críticas de segurança que não possam ser mitigadas remotamente;

vi. Garantia de que o dispositivo opera corretamente em conformidade com os controles de segurança da rede hospitalar (segmentação de VLANs, firewall, etc.).

vii. Exigência de apresentação de documentos técnicos que comprovem a segurança do produto, incluindo relatórios de testes de intrusão (*Pentest*), lista de componentes de software (*SBOM*) e política de ciclo de vida (*Lifecycle Policy*).

4.2. Fase 2: Instalação e Onboarding

a. **Inventário e Registro:** Nenhum dispositivo pode ser conectado à rede sem antes ser cadastrado no CMDB (inventário central) pela TI, conforme exigido pela PGA.
b. **Troca de Credenciais:** No momento da instalação, o técnico (Engenharia Clínica ou TI) deve alterar todas as senhas padrão de fábrica para credenciais complexas, conforme os Requisitos Mínimos de Força (mínimo de 12 caracteres, alfanuméricos e especiais) da PUA e PGA. As senhas devem ser gerenciadas em um cofre de senhas do hospital.
c. **Segmentação de Rede:** Esta é a ação mais importante para proteger os ativos.
    i. **VLAN Específica:** O dispositivo deve ser colocado em uma Rede Virtual (VLAN) específica: "VLAN_IOMT".
    ii. **Regras de Firewall Estritas:** O firewall deve impor as seguintes restrições, garantindo o Princípio do Menor Privilégio:
        - Proibido acesso direto de saída à Internet.
        - Proibido acesso à rede administrativa (RH, Financeiro) e à rede de visitantes (Wi-Fi de Pacientes).
        - Permitido acesso apenas aos servidores e portas específicos que o dispositivo precisa para operar.
d. **Desativação de Serviços:** O técnico de TI deve desabilitar quaisquer serviços de gerenciamento inseguros (ex: Telnet, FTP, SMBv1) no dispositivo.

4.3. Fase 3: Operação e Manutenção

a. **Monitoramento Ativo (Detecção):** A Equipe de SI deve monitorar o tráfego da "VLAN_IOMT" em busca de comportamento anômalo.
b. **Gerenciamento de *Patches* (Resposta):**
    i. **Monitoramento:** A Engenharia Clínica é responsável por monitorar os boletins de segurança dos fornecedores.
    ii. **Homologação:** Nenhum *patch* pode ser aplicado diretamente em produção. Ele deve ser testado em um dispositivo de

homologação (reserva) para garantir que a atualização não afete a funcionalidade clínica.

iii. **Janela de Manutenção:** A atualização de dispositivos em uso (Prioridade 0 e 1, conforme o PCNDRP) só pode ocorrer em janelas de manutenção programadas e aprovadas pela chefia do setor, garantindo a disponibilidade de um dispositivo de backup.

iv. **SLA de Correção:** A aplicação de patches deve respeitar a criticidade da vulnerabilidade, contada a partir da disponibilização pelo fabricante:

- **Crítica/Urgente** (Exploit público/Risco iminente): Aplicar em até 7 dias.
- **Alta:** Aplicar em até 30 dias.
- **Média/Baixa:** Aplicar em até 90 dias ou na próxima manutenção preventiva.

v. **Gestão de Exceção:** Caso não seja possível aplicar o patch no prazo (ex: risco operacional alto ou incompatibilidade), deve-se abrir um processo formal de Aceite de Risco, documentando os controles compensatórios adotados.

c. **Controle Compensatório para Legados:** Para dispositivos "incorrigíveis" (que rodam em SOs obsoletos ou sem *patch*), a SI deve implementar:

i. **Isolamento de Rede:** Garantir que o dispositivo permaneça na VLAN_IOMT com o mínimo de acesso possível.

ii. ***Virtual Patching*** **(Patch Virtual):** Aplicar políticas de segurança (regras/assinaturas) em um Sistema de Prevenção de Intrusão (IPS) ou Firewall. O IPS/Firewall intercepta o tráfego malicioso *antes* que ele chegue ao dispositivo vulnerável, mitigando o risco sem necessidade de aplicar o *patch* no dispositivo.

4.4. Fase 4: Descomissionamento

a. **Sanitização de Dados:** O dispositivo não pode sair do controle do hospital (para lixo, revenda ou devolução) antes que a TI realize a sanitização de todos os dados de paciente armazenados nele, conforme a LGPD.
b. **Padrão de Descarte:** A TI deve seguir métodos padronizados para garantir a eliminação dos dados, variando conforme o destino do ativo:
    i. **Reutilização Interna:** Método *Clear* (ex: redefinição de fábrica) é aceitável.
    ii. **Revenda ou Devolução:** Método *Purge* (ex: formatação de baixo nível ou *ATA Secure Erase*) é o mínimo obrigatório para garantir que a recuperação dos dados seja inviável.
    iii. **Descarte (Lixo):** Método *Destroy* (ex: trituração física ou incineração da mídia de armazenamento) é obrigatório.
c. **Registro:** Deve haver um registro (log) e cadeia de custódia do processo de sanitização e descarte para fins de auditoria.
d. **Remoção de Acesso:** A TI deve remover o dispositivo do inventário (CMDB), desativar sua porta de rede e revogar suas credenciais de acesso imediatamente.

5. Auditoria e Monitoramento

A Equipe de Segurança da Informação (SI) deve monitorar ativamente o cumprimento deste procedimento, focando especificamente nos riscos únicos dos dispositivos médicos conectados. As auditorias devem incluir:

a. **Auditoria de Rede (Trimestral):** Varreduras ativas da rede para confirmar que todos os dispositivos IoMT identificados estão corretamente isolados na "VLAN_IOMT" e procurar por dispositivos não catalogados conectados indevidamente.
b. **Auditoria de Credenciais (Contínua):** Monitoramento para identificar dispositivos IoMT que ainda utilizam senhas de fábrica ou serviços inseguros (ex: Telnet).

c. **Auditoria de Inventário (Semestral):** Cruzamento do inventário da Engenharia Clínica com o CMDB da TI para validar o status do ciclo de vida (em operação, em manutenção, descomissionado) de todos os ativos IoMT.
d. **Auditoria de Descarte (Por Demanda):** Verificação dos registros de sanitização sempre que um dispositivo médico for descomissionado, garantindo que nenhum dado de paciente saia do hospital.

6. Revisão e Manutenção

Este procedimento deve ser revisado anualmente ou sempre que:

a. Uma nova categoria de dispositivo médico (ex: novas bombas de infusão inteligentes, scanners portáteis) for adquirida pelo hospital.
b. Um incidente de segurança global relevante para IoMT (ex: uma nova vulnerabilidade em um sistema operacional embarcado) for divulgado.
c. Ocorrer uma mudança significativa na arquitetura da rede hospitalar.