3.2 Norma de Atualização de Sistemas

1. Objetivo

Estabelecer diretrizes para varredura, avaliação e aplicação de patches e atualizações de segurança em sistemas operacionais, aplicações e infraestrutura, atendendo ao CIS Controls v8 IG1 (C7) e reduzindo riscos de vulnerabilidades exploráveis.

2. Escopo

Esta norma se aplica a todos os ativos de informação definidos no inventário:

- Servidores físicos e virtuais
- Sistemas operacionais (Windows, Linux, etc.)
- Aplicações corporativas e de terceiros
- Dispositivos de rede (firewalls, switches, roteadores)
- Serviços em nuvem gerenciados pela empresa

3. Responsabilidades

- **Equipe de TI / Administradores**: Conduzir varreduras de vulnerabilidades, aplicar patches e registrar evidências.
- **Gestor de Segurança da Informação**: Aprovar calendário de atualizações, revisar relatórios de conformidade e indicar planos de ação.
- **Fornecedores de Software**: Fornecer patches e suporte técnico dentro dos prazos acordados.
- **Gestores de Área**: Autorizar janelas de manutenção e validar impactos no negócio.

4. Definições

- **Patch**: Atualização para corrigir vulnerabilidades ou bugs críticos.
- **Vulnerabilidade**: Fraqueza em um sistema que pode ser explorada.
- **Varredura de Vulnerabilidades**: Processo automatizado de identificação de falhas.

5. Pré-requisitos

- Inventário atualizado de ativos e versões de software.
- Ferramenta automatizada de gerenciamento e distribuição de patches.
- Acesso administrativo aos ambientes alvo.

6. Procedimento e Diretrizes

- **Varredura de vulnerabilidades em ativos críticos** (CIS C7)
- **Calendário de aplicação de patches (semanal/mensal) e verificação de sucesso** (CIS C7)

1. **Planejamento**: Definir escopo da varredura e agendar frequência (semanal para ativos críticos).
2. **Execução da Varredura**: Utilizar ferramenta X para rodar scan completo e gerar relatório.
3. **Classificação de Resultados**: Avaliar severity (CVSS) e priorizar correções.
4. **Aplicação de Patches**:
    - Correções de alta e média severidade: aplicar em até 7 dias.
    - Correções de baixa severidade: aplicar na janela mensal ou trimestral.
5. **Verificação de Sucesso**: Reexecutar scan nos sistemas após patch e validar a ausência da vulnerabilidade.
6. **Gerenciamento de Exceções**: Documentar justificativa para atrasos e definir controles compensatórios.

7. Verificação e Auditoria

- **Relatórios Semanais**: Indicadores de ativos com patches pendentes e aplicados.
- **Auditoria Mensal**: Revisar registros de patch e identificar não conformidades.
- **Teste em Homologação**: Validar patches críticos em ambiente de teste antes de produção.

8. Registros e Relatórios

- Armazenar relatórios de varredura e logs de aplicação em repositório centralizado.
- Gerar relatório trimestral de conformidade para a Alta Direção, incluindo métricas de tempo de correção.

9. Revisão da Norma

Revisar anualmente ou sempre que houver mudanças relevantes em ativos, ferramentas ou requisitos regulatórios.