I. Título

A. Nome: Instrução Normativa CITIC 003/2020

B. Assunto: Dispõe sobre a obrigatoriedade de se manter o mapeamento físico e lógico das redes de dados

C. Número: IN-CITIC-003/2020

D. Autores: Comitê de Segurança da Informação

E. Status: [] proposta [ ] em revisão [X] aprovada [ ] rejeitada [ ] obsoleta

F. Quando foi proposta: 29/10/2020

G. Quando foi revisada: não se aplica

H. Quando foi aprovada: 03/11/2020

I. Quando entrou em vigor: 19/11/2020

II. Definições

- **CSIRT Unicamp:** do inglês, Computer Security Incident Response Team. É a Equipe de Resposta e Tratamento de Incidentes de Segurança da Informação, responsável por receber, analisar, processar e responder os incidentes de segurança em computadores envolvendo a rede da Unicamp.
- **UniNet**: é a rede de comunicação de dados da Unicamp, composta por sua rede principal e pelas demais redes a ela conectadas, responsável por toda a troca de tráfego de dados entre as Unidades/Órgãos e com a Internet;
- **IP Address Management (IPAM):** é uma metodologia implementada em tecnologia da informação para planejar e gerenciar o uso dos endereços IP e suas relações com os recursos de tecnologia da informação.

III. Autoridade e Responsabilidade

Os responsáveis pela infraestrutura computacional têm a responsabilidade e autoridade de manter os mapeamentos físico e lógico da rede.

IV. Resumo

Esta política define as diretrizes para gestão de redes computacionais, objetivando documentação e mapeamento físico e lógico.

V. Propósito

O propósito desta política é criar base para gestão da segurança da informação identificando, mapeando e controlando as redes computacionais.

VI. Riscos do não cumprimento

Quando não há a identificação, mapeamento e o controle da rede computacional e ocorre um incidente de segurança da informação, não há meios para auditoria; o tempo de resposta do incidente também é prejudicado, assim como o tempo para solucionar o problema, causando prejuízos financeiros maiores que os esperados.

VII. Escopo

- Mapeamento lógico de rede (IPAM):
  - Hosts (físicos e virtuais),
  - Gateways,
  - Switches,
  - Routers,
  - Subredes,
  - Redes privadas,
  - VPCs e Túneis com outras unidades/instituições/provedores,
  - Fluxos de conexões.

- Mapeamento físico de rede:
  - Portas utilizadas,
  - Interligação dos dispositivos.

- Controles:
  - Bloqueio de dispositivos não autorizados,
  - Atualização do inventário

VIII. Declaração da Política

1. É necessário que se mantenha o mapeamento lógico da rede atualizado, observando a necessidade de inclusão de todos os ativos. Também faz-se necessária a documentação do escopo das sub-redes e redes privadas presentes.
2. É necessário que se mantenha o mapeamento físico da rede em *software* específico ou diagrama de rede atualizado.
3. É necessário manter meios de controle para executar bloqueios de dispositivos não autorizados à rede UniNet.
4. É necessário manter rotinas para garantir que o inventário dos ativos de rede que fazem parte do escopo desta política se mantenha atualizado.

   Os casos omissos serão levados para deliberação do Comitê de Segurança da Informação da Unicamp.

IX. Conformidade

A. **Verificação:** o Comitê de Segurança da Informação não tem planos de monitorar ativamente a não conformidade desta política; no entanto, irá deliberar em casos de eventos relevantes e incidentes.

B. **Notificação:** não se aplica a esta política.

C. **Remediação:** em caso de não conformidade, que se proceda ao bloqueio do dispositivo até que se averigue a necessidade de conexão do mesmo à UniNet.

X. Referências

1. Penn University Office of Information Security disponível em: https://www.isc.upenn.edu/security/overview.
2. CIS Center for Internet Security disponível em: https://www.cisecurity.org/

Documento assinado eletronicamente por **PAULO LICIO DE GEUS**, **DIRETOR GERAL DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO**, em 19/11/2020, às 14:40 horas, conforme Art. 10 § 2º da MP 2.200/2001 e Art. 1º da Resolução GR 54/2017.

A autenticidade do documento pode ser conferida no site: sigad.unicamp.br/verifica, informando o código verificador: **ED689CED B96644E6 84BC136B 6244F87A**

UNICAMP
SIGAD