I. Título

A. Nome: Instrução Normativa CITIC 005/2020

B. Assunto: Dispõe sobre a gestão de vulnerabilidades

C. Número: IN-CITIC-005/2020

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

- **Ativo de Informação** – é o patrimônio composto por todos os dados e informações gerados e manipulados durante a execução dos sistemas e processos da Unicamp;
- **Ativo de Processamento** – é o patrimônio composto por todos os elementos de *hardware* e *software* necessários para a execução dos sistemas e processos da Unicamp, tanto os produzidos internamente quanto os adquiridos;
- **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 aos incidentes de segurança em computadores envolvendo a rede da Unicamp.

III. Autoridade e Responsabilidade

Os responsáveis por ativos de informação e de processamento têm a responsabilidade e autoridade de gerir as vulnerabilidades existentes no ambiente computacional sob sua responsabilidade.

O CSIRT UNICAMP tem a responsabilidade de auxiliar no processo de gestão de vulnerabilidades dos ativos de informação e de processamento.

IV. Resumo

Este documento define as diretrizes que devem ser cumpridas para assegurar a devida conformidade da Gestão de Vulnerabilidades relativas à Segurança da Informação no âmbito da UNICAMP.

V. Propósito

Estabelecer a política para gestão de vulnerabilidades no que tange a segurança da informação no âmbito da UNICAMP.

VI. Riscos do não cumprimento

Caso não sejam tratadas as vulnerabilidades expostas a tempo, os atacantes as utilizarão para tomar controle, interromper o serviço, alterar/roubar informações sigilosas, dentre outras possibilidades, podendo causar prejuízos financeiros ou à imagem da instituição.

O não cumprimento desta política pode expor os serviços e permitir o acesso indevido à rede e às informações da Universidade, podendo causar prejuízos financeiros ou à imagem da Instituição.

VII. Escopo

Aplicável ao CSIRT UNICAMP e a todos os responsáveis por ativos de informação ou de processamento.

VIII. Declaração da Política

1. É necessário que se mantenham atualizados sistemas, serviços e equipamentos computacionais, no que tange as vulnerabilidades, limitado ao escopo definido.
2. O CSIRT UNICAMP deverá notificar antecipadamente os responsáveis pelos ativos de informação ou de processamento sobre testes de vulnerabilidade, que serão aplicados no ambiente computacional do Órgão.
3. O CSIRT UNICAMP é responsável por manter registro do processo de tratamento e notificar as equipes de TI dos Órgãos sobre vulnerabilidades identificadas durante testes ou notificadas por terceiros.
4. O CSIRT UNICAMP deverá dar suporte às equipes de TI dos Órgãos na gestão de vulnerabilidades de segurança da informação.

IX. Conformidade

A. Verificação: o CSIRT UNICAMP e os responsáveis pelos sistemas de informação, serviços de informação e equipamentos computacionais devem monitorar a não conformidade a esta política.
B. Notificação:
    a. Em caso de identificação de vulnerabilidades pelo CSIRT UNICAMP, o mesmo deverá notificar os responsáveis pelos ativos de informação ou de processamento.
    b. Em caso de ausência na gestão das vulnerabilidades notificadas pelo CSIRT UNICAMP, a CITIC deverá ser informada;
    c. Em caso de identificação de vulnerabilidades, o CSIRT UNICAMP deverá ser notificado;
    d. Em casos omissos, a CITIC deverá ser informada;

C. Remediação: Em caso de não conformidade, os responsáveis pelos ativos de informação ou de processamento deverão mitigar as vulnerabilidades existentes, reportando ao CSIRT UNICAMP as decisões e ações realizadas.

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:
60D90A64 EAF3469E BF351EE5 884F3537

UNICAMP
SIGAD