I. Título

A. Nome: Instrução Normativa CITIC 004/2020

B. Assunto: Dispõe sobre a gestão de incidentes de segurança da informação

C. Número: IN-CITIC-004/2020

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;
- **CITIC**: Coordenadoria Integrada de Tecnologia da Informação e Comunicação;
- **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.
- **TI**: Tecnologia da Informação.
- **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 a Internet.
- **Unicamp**: Universidade Estadual de Campinas.

III. Autoridade e Responsabilidade

Os responsáveis por ativos de informação ou de processamento têm a responsabilidade e autoridade para gerir a ocorrência dos incidentes de segurança da informação sob sua responsabilidade.

O CSIRT UNICAMP tem a responsabilidade de coordenar o processo de gestão de incidentes de segurança da informação na rede Unicamp.

IV. Resumo

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

V. Propósito

Minimizar os impactos relacionados aos incidentes em tempo hábil.

VI. Riscos do não cumprimento

Caso não haja uma gestão de incidentes, pode-se prejudicar a imagem da UNICAMP, assim como ter seus serviços indisponíveis e/ou causar prejuízos financeiros.

VII. Escopo

Aplicável a todos os responsáveis por ativos de informação ou de processamento.

VIII. Declaração da Política

O CSIRT da Unicamp é responsável por:

- Coordenar o tratamento de incidentes de segurança na rede UniNet;
- Notificar os administradores de TI dos Órgãos sobre incidentes de segurança sob sua responsabilidade;
- Documentar e manter um sistema de controle de incidentes de segurança;
- Prestar suporte aos administradores de TI dos Órgãos quando da ocorrência de comprometimento de algum ativo de informação ou de processamento.
- Notificar outras equipes de segurança quando identificado um ataque direcionado;
- Realizar monitoramento da segurança de rede através da análise do cabeçalho do pacote de rede, de sistemas de detecção de intrusão e/ou através da correlação de logs e eventos para identificar possíveis problemas de segurança.

Os responsáveis pelos ativos de informação ou de processamento devem atuar na identificação dos incidentes de segurança, assim como informar o CSIRT UNICAMP sobre quaisquer incidentes de segurança. Cabe à equipe de TI dos Órgãos atuar na resolução dos incidentes de segurança sob sua responsabilidade, em conjunto com a equipe do CSIRT UNICAMP.

Nos casos onde sejam necessários, o CSIRT UNICAMP poderá solicitar o bloqueio do ativo de informação ou de processamento.

VIII. Conformidade

A. **Verificação:** os responsáveis pelos ativos de informação ou de processamento atuam ativamente na identificação dos incidentes de segurança. É realizado pelo CSIRT UNICAMP o monitoramento da rede através da análise do cabeçalho dos pacotes de dados trafegados pela UniNet, de sistemas de detecção de intrusão e/ou através da correlação de logs e eventos para identificar possíveis problemas de segurança.

B. **Notificação:**
   a. Em caso de identificação de incidentes pelo CSIRT UNICAMP, o mesmo deverá notificar os responsáveis pelos ativos de informação ou de processamento;
   b. Em caso de identificação de incidentes envolvendo entidades externas, o CSIRT UNICAMP deverá notificar outras equipes de segurança;
   c. Em caso de ausência na gestão de incidentes notificados pelo CSIRT UNICAMP, a CITIC deverá ser informada;
   d. Em caso de identificação de incidentes na rede interna do Órgão, o CSIRT Unicamp deverá ser informado;
   e. 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 gerir os incidentes existentes, reportando ao CSIRT UNICAMP as decisões e ações realizadas.

IX. Referências

1. Equipe de Resposta e Tratamento de Incidentes de Segurança da Informação(Computer Security Incident Response Team – CSIRT Unicamp) disponível em https://www.security.unicamp.br/
2. Penn University Office of Information Security disponível em https://www.isc.upenn.edu/security/overview
3. 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:
07872432 C1AD4D7C 9965036D 9C108F4F

UNICAMP
SIGAD