I. Título

A. Nome: Instrução Normativa CITIC 006/2020

B. Assunto: Dispõe sobre a gestão de registros (*logs*)

C. Número: IN-CITIC-006/2020

D. Autores: Comitê de Segurança da Informação

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

F. Quando foi proposta: 2019-04-25

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 geradas e manipuladas durante a execução dos sistemas.
- **Ativo de Processamento:** é o patrimônio composto por todos os elementos de *hardware* e *software* necessários para a execução dos sistemas, 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.
- **Registros (*logs*):** Registros de eventos que ocorrem nos sistemas de informação, serviços de informação e equipamentos computacionais.
- **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.
- **UNICAMP:** Universidade Estadual de Campinas.

III. Autoridade e Responsabilidade

Os responsáveis pelos ativos de informação e de processamento têm a responsabilidade e autoridade para configurar e manter os registros (*logs*) para auditoria.
Em se tratando de infraestrutura ou serviço centralizado, o gestor deste serviço tem a responsabilidade de configurar e manter os registros (*logs*) para auditoria.

IV. Resumo

Este documento define as diretrizes que devem ser cumpridas para assegurar a devida conformidade da gestão de registros (*logs*) para auditoria relativas à Segurança da Informação no âmbito da UNICAMP.

V. Propósito

Manter uma base confiável e consolidada de informações para tratamento de incidentes de segurança da informação e auditorias.

VI. Riscos do não cumprimento

Caso haja um acesso indevido e não exista nenhum tipo de registro de auditoria para coletar evidências do incidente, haverá dificuldade na detecção e comprovação do ataque. Também será comprometida a compreensão e recuperação do que foi afetado.

A ausência de registros confiáveis de auditoria pode inviabilizar ações jurídicas para remediação de prejuízos financeiros ou da imagem da instituição.

VII. Escopo

Aplicável a todos os responsáveis por ativos da informação e de processamento da UNICAMP.

VIII. Declaração da Política

1. É necessário que se mantenha registros dos acessos aos ativos de informação e de processamento, conforme regulamenta os artigos 5º, 13º e 15º do Marco Civil da Internet (Lei federal nº 12.965/2014) .
2. É necessário que se mantenha registros de erros aos sistemas de informação, sistemas operacionais e serviços de informação.
3. É necessário que se mantenha os registros dos dispositivos de rede.
4. É orientado que se busque, sempre que possível, que se mantenha os registros da conexão do usuário a rede, desde que possibilite identificar usuário de forma inequívoca, armazenando o nome de usuário (*login*), horário de início da conexão e de desconexão.
5. É necessário que os registros sejam mantidos pelo prazo mínimo de 12 meses, conforme regulamenta o Marco Civil da Internet (Lei federal nº 12.965/2014).
6. É necessário manter o horário dos equipamentos, serviços e sistemas sincronizado com os servidores de sincronismo disponibilizados pela universidade.
7. É necessário manter os registros dos serviços e servidores em pelo menos um servidor remoto, armazenando de forma segura e com controle de acesso.

IX. Conformidade

A. Verificação: a UNICAMP não atua ativamente na verificação de não conformidade na gestão de registro (*logs*) de auditoria, mas atuará nos casos descobertos de não conformidade durante as atividades normais de resolução de problemas ou incidentes.
B. Notificação:
    a. Em caso de ausência da gestão de logs, o responsável deverá ser notificado para ativar os registros imediatamente;
    b. Em casos omissos, a CITIC deverá ser notificada.

C. Remediação: em caso de não conformidade o responsável deverá ativar os registros imediatamente.

XI. 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:
3AB7F5F8 E28546B5 A9183DC7 4B0608EB

UNICAMP
SIGAD