## I. Título

**A. Nome: Instrução Normativa CITIC 002/2020**

**B. Assunto: Dispõe sobre o desenvolvimento seguro de sistemas de informação**

**C. Número: IN-CITIC-002/2020**

**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 geradas e manipuladas 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;
- **Captcha**: teste de desafio cognitivo completamente automatizado para diferenciação entre computadores e humanos;
- **CCUEC**: Centro de Computação;
- **LGPD:** Lei Geral de Proteção dos Dados;
- **NTP**: do inglês, Network Time Protocol;
- **OWASP**: do inglês, Open Web Application Security Project;
- **SSL**: do inglês, Secure Sockets Layer;
- **UNICAMP**: Universidade Estadual de Campinas.

## III. Autoridade e Responsabilidade

Gestores responsáveis pelo desenvolvimento de *software* dentro da Universidade, bem como todo profissional envolvido na especificação, desenvolvimento, implantação, correção e melhoria dos *software* mantidos pela Unicamp.

### a) Autoridade Máxima da Aplicação ou Integração de Software

Para cada aplicação ou solução de *software* desenvolvida ou hospedada nas estruturas da Unicamp, ou de cunho externo, mas que utilize de informações produzidas pela comunidade desta Universidade, é necessária a intitulação de um gestor ou grupo responsável que possa responder quaisquer questionamentos que venham a surgir sobre a aplicação.

**b) Responsabilidade Co-participativa**

Todos os membros participantes do desenvolvimento e manutenção da solução de *software*, com ou sem vínculo com a Unicamp, seja este em qualquer perspectiva, mas que colabore para manter tal solução disponível para a comunidade, tem como responsabilidade a segurança e preservação dos dados.

## IV. Resumo

Esta seção compreende um conjunto de medidas e procedimentos no âmbito de desenvolvimento de *software* a ser observado por toda a comunidade universitária, além de prestadores de serviço, na preservação e integração dos ativos de informação ou de processamento existentes e a serem criados.

## V. Propósito

O propósito desta política é criar base para o desenvolvimento de *software* seguro dentro da Universidade, visando preservar a disponibilidade, integridade, confiabilidade e autenticidade dos dados, informações e conhecimentos que compõem os ativos de informação ou de processamento da UNICAMP.

## VI. Riscos do não cumprimento

O não cumprimento desta política poderá gerar prejuízos para a UNICAMP em suas várias áreas de negócio, tais como o prejuízo financeiro decorrente do vazamento de informações pessoais, estratégicas e intelectuais de pesquisa e inovação e prejuízos à sua imagem institucional.

## VII. Escopo

Qualquer pessoa envolvida nas etapas do desenvolvimento, implantação, customização e manutenção de software (construídos internamente, adquiridos ou obtidos de comunidades de código livre) para a UNICAMP ou que utilizem informações e conhecimentos gerados por esta, com ou sem vínculo à mesma.

## VIII. Declaração da Política

1. **Arquitetura de *software* com foco em segurança da informação:** tanto a concepção da arquitetura do software, aplicação, ou aplicativo móvel, quanto a codificação devem seguir boas práticas de segurança da informação, para não ser suscetível às principais estratégias de ataques, conforme definido pela OWASP (*webapp* Top 10 *risks* e *mobile* Top 10 *risks*). Vide tópico Referências deste documento.

2. **Ambientes:** servidores WEB (por exemplo *proxy* ou servidores de aplicação) que hospedam soluções de *software*, no desenvolvimento, homologação e produção, devem utilizar canal

seguro de comunicação (por exemplo TLS/SSL) compatível com a tecnologia atual e protegido de vulnerabilidades identificadas.

3. **Autenticação:** todos os sistemas corporativos de informação desenvolvidos para uso na Unicamp devem autenticar seus usuários via sistema de Autenticação Centralizada/Senha Única da Unicamp, conforme Deliberação CAD-A-005/2017 de 06/06/2017. Os sistemas que apresentarem alguma dificuldade técnica não contornável para usar esta autenticação, com ciência do CCUEC, devem utilizar o LDAP corporativo mantido por este órgão.

4. **Gestão do código fonte:** as equipes deverão realizar o versionamento do código fonte das aplicações desenvolvidas. O acesso à ferramenta deverá ser via canal seguro de comunicação (por exemplo TLS/SSL) compatível com a tecnologia atual e protegido de vulnerabilidades identificadas.

5. **Testes e validação:** os sistemas deverão passar por testes antes da sua implantação. O plano de testes deve contemplar aspectos de segurança da informação. A validação final é de responsabilidade da área de negócio solicitante do sistema.

6. **Trilha de Auditoria:**
    a. Todas as soluções de *software* da Universidade devem ter registro de acesso (*logs*), que deverão estar sincronizados com o servidor de horário (NTP) da Unicamp. No caso de hospedagem externa, o sincronismo deve ter como referência o serviço NTP do NIC.br. Os *logs* devem ser analisados para identificar eventos anormais, por exemplo acessos indevidos. Não se deve armazenar informações sensíveis no *log*, por exemplo senhas). Os logs deverão ser copiados e mantidos também em servidor separado a fim de manter o histórico e evitar exclusão de rastros por um possível invasor.
    b. Guardar informações para auditoria de concessão e retirada (manual ou automática) de acessos, permissões especiais, permanência de membros em comissões e demais casos aplicáveis.
    c. Seguir Instrução Normativa CITIC IN-006/2020 - Gestão Operacional - Gestão de registros (logs) de auditoria.

7. **Controle de Acesso:** todos os sistemas devem restringir o acesso conforme o público alvo a que se destinam — discente, servidor e público externo. Devem ser estabelecidos papéis (perfis), para liberar o acesso a cada funcionalidade. Para funcionalidades públicas deve-se avaliar os dados exibidos (conforme classificação de sigilo e LGPD), bem como se o acesso às informações requer validação de captcha, para minimizar processamento de requisições advindas de robôs.

## IX. Conformidade

A. **Verificação:** os responsáveis pelos Ativos de Processamento 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 da UNICAMP, a CITIC deverá ser informada.
c. Em caso de identificação de vulnerabilidades, o CSIRT deverá ser notificado imediatamente.
d. Em casos omissos, a CITIC deverá ser informada.

C. **Remediação:** Em caso de não conformidade, deve-se:
a. Tornar os Ativos de Processamento vulneráveis inacessíveis a todos os usuários;
b. Medir a extensão dos Ativos de Informação e Processamento afetados, e implementar ações que reduzam o potencial de disseminação do incidente por outros sistemas e redes.
c. Realizar as correções necessárias, visando o retorno à normalidade.
d. Reportar ao CSIRT da UNICAMP as decisões e ações realizadas.

## X. Referências

1. CIS Controls version 7.1 disponível em https://www.cisecurity.org/
2. OWASP webapp Top 10 risks disponível em https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet
3. OWASP mobile Top 10 risks disponível em: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Risks https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide#tab=Main
4. NTP Unicamp disponível em https://www.ccuec.unicamp.br/ccuec/servicos/sincronismo-de-horario-ntp

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:
**C294A82C 78C84C85 B1311DE6 5B092129**

UNICAMP
SIGAD