Deliberação CONSU-A-031/2020, de 04/08/2020

Reitor: Marcelo Knobel
Secretária Geral: Ângela de Noronha Bignami

Aprova a Política de Segurança da Informação da Universidade Estadual de Campinas – Unicamp.

O Reitor da Universidade Estadual de Campinas, na qualidade de Presidente do Conselho Universitário, tendo em vista o decidido na 167ª Sessão Ordinária de 04.08.20, baixa a seguinte Deliberação:

Artigo 1º – Fica aprovada a "Política de Segurança da Informação da Universidade Estadual de Campinas – Unicamp", que integra esta Deliberação como Anexo I e que contém princípios e diretrizes gerais aplicáveis à segurança das informações custodiadas ou de propriedade da Universidade.

Artigo 2º – As atribuições e responsabilidades pela execução da Política de Segurança da Informação da Unicamp serão confiadas ao Comitê de Segurança da Informação – CSI, que responderá à Coordenadoria Integrada de Tecnologia da Informação e Comunicação – CITIC e será designado por Resolução do Gabinete do Reitor.

Artigo 3º – Esta Deliberação entra em vigor na data de sua publicação, revogadas as disposições em contrário. (Proc. nº 01-P-10342/2020)

ANEXO I

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA UNIVERSIDADE ESTADUAL DE CAMPINAS

Coordenadoria de Tecnologia da Informação e Comunicação - CITIC
Comitê de Segurança da Informação - CSI

Referências legais e normativas:

ABNT ISO GUIA 73:2009 – Gestão de riscos – Vocabulário – Definições de termos genéricos relativos à gestão de riscos.
ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação - Requisitos.
ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação.
Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014) - Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
Instrução Normativa ConTIC IN-01/2019 - Dispõe sobre as normas e procedimentos para o uso dos Recursos de Tecnologia da Informação e Comunicação na Unicamp.

Campo de Aplicação:
Este documento se aplica no âmbito da Universidade Estadual de Campinas - Unicamp.

1. Objetivo
Estabelecer direcionamentos e valores para a gestão da segurança da informação no âmbito da Universidade Estadual de Campinas.

2. Descrição e Escopo
Este documento contém princípios e diretrizes aplicáveis à segurança das informações custodiadas ou de propriedade da Universidade Estadual de Campinas, estabelecendo direcionamentos e valores para a gestão da segurança da informação.

3. Público-alvo
Este documento se destina a toda a comunidade acadêmica: docentes ativos e inativos (docentes, funcionários, pesquisadores), alunos, ex-alunos, estagiários, patrulheiros, prestadores de serviço, visitantes e usuários externos que façam uso de algum sistema de informação da Unicamp, sendo de responsabilidade de cada um o seu cumprimento.

4. Conceitos e 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, recebidos por doação ou incorporados.

CITIC - Coordenadoria Integrada de Tecnologia da Informação e Comunicação, instituída pela Resolução GR-009/2020 .

CONSU - Conselho Universitário

5. Princípios
A Política de Segurança da Informação da Unicamp está fundamentada na preservação das informações necessárias às atividades da Instituição e nos seguintes princípios:

- **Autenticidade**: garante a veracidade da autoria da informação.
- **Confidencialidade**: somente pessoas devidamente autorizadas devem ter acesso à informação.
- **Integridade**: somente alterações, supressões e adições autorizadas devem ser realizadas nas informações.
- **Disponibilidade**: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado.
- **Legalidade**: o uso da informação deve estar de acordo com as leis, regulamentos, licenças e contratos em vigência.

6. Valores e Diretrizes

Segurança Focada na Instituição
Garantir a segurança da informação tanto aos sistemas no ambiente de computação quanto aos meios convencionais de processamento, comunicação e armazenamento em papel.

Informação é patrimônio
Considerar que toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela Unicamp é patrimônio da instituição e deve ser protegida quanto aos aspectos de confidencialidade, autenticidade, integridade e disponibilidade.

Proteção compatível com os riscos
Dimensionar e aplicar os investimentos necessários em medidas de segurança, segundo o valor do ativo que está sendo protegido e de acordo com a identificação de riscos de potenciais prejuízos ao negócio, à atividade fim e aos objetivos institucionais.

Tratamento conforme a classificação
Todas as informações devem ser adequadamente armazenadas e protegidas quanto ao uso e acesso, conforme definido em sua classificação de segurança.

Responsabilização baseada na credencial
Responsabilizar, com base no uso da credencial, que se caracteriza por ser pessoal e intransferível, qualificando aquele que se encontra formalmente associado a ela como responsável por todas as atividades desenvolvidas em seu uso.

Utilização restrita às atividades
Administrar o acesso e o uso da informação e dos ativos de informação de acordo com as atribuições necessárias para o cumprimento das atividades institucionais. Qualquer outra forma de uso necessitará de prévia autorização.

Utilização orientada à segurança
Permitir somente o uso de ativos de informação ou ativos de processamento autorizados pelos gestores, sempre se atentando que estes estejam identificados, protegidos, inventariados e de acordo com a legislação vigente.

Autorização definida pelos gestores
Definir e cancelar acessos aos recursos e aos locais restritos com base na solicitação dos gestores de cada órgão, que também são responsáveis pelos ativos disponibilizados para uso.

Segregação de funções
Segregar a administração e execução de funções ou áreas de responsabilidade críticas para o negócio, evitando o controle de um processo na sua totalidade, visando à redução do risco de mau uso acidental ou deliberado.

Educação e Capacitação
Promover continuamente ações educativas e de capacitação sobre segurança da informação ao público-alvo para

que realizem suas atividades na instituição de forma segura, utilizando procedimentos que minimizem os riscos e que possibilitem o uso correto dos ativos e ferramentas de informação.

Auditoria
Monitorar e auditar, pela área competente da Universidade, a implementação e o cumprimento da Política de Segurança da Informação. Consultorias externas especializadas poderão ser utilizadas para avaliação da Política de Segurança da Informação e de seu cumprimento, bem como para validar protocolos e procedimentos especiais, quando necessário.

Continuidade aplicada aos serviços
Planejar e definir estratégias para reduzir, a um nível aceitável, a possibilidade de interrupção causada por desastres ou falhas nos recursos que suportam os processos de trabalho. O resultado desse planejamento deve ser documentado, testado e revisado conforme a necessidade, assegurados os recursos necessários à sua implementação.

Notificação imediata de incidentes de segurança
Notificar todos os incidentes de segurança à Equipe de Tratamento e Resposta a Incidentes de Segurança da Unicamp (CSIRT Unicamp) para apuração e gestão do incidente. O gestor de cada órgão deve ser envolvido para encaminhamento dos processos necessários à apuração de responsabilidades.

7. Penalidades
O público-alvo desta política está sujeito às regras da mesma, devendo observar integralmente suas disposições. A inobservância dessas regras acarretará apuração de responsabilidades, na forma da legislação em vigor, podendo haver responsabilização penal, civil e/ou administrativa.

8. Competências e Responsabilidades
Ao público-alvo não é dado o direito de desconhecimento desta política, devendo o mesmo seguir rigorosamente o estabelecido nas normas de segurança.

9. Disposições Gerais
Qualquer tipo de dúvida sobre a Política de Segurança da Informação da Unicamp e seus documentos deve ser imediatamente esclarecida junto ao Comitê de Segurança da Informação.

Casos omissos, os quais não estão cobertos por esta política, deverão ser submetidos ao Comitê de Segurança da Informação em exercício, para que haja apreciação e deliberação, definindo assim se o objeto será incluído ou resultará na alteração de algum ponto da política em vigência.

10. Vigência e atualização

Vigência:
Este documento entra em vigor a partir da data de sua publicação e deve ser revisto em caso de ocorrência de alguma das condições obrigatórias de atualização do documento.

Atualização:
Essas diretrizes foram atualizadas em 28/04/2020.

Condições obrigatórias para atualização do documento:
- Surgimento ou alteração de leis e/ou regulamentações vigentes;
- Mudança estratégica da instituição;
- Mudança nas tecnologias utilizadas na Unicamp.

11. Atribuições e Responsabilidades

Responsável pela atualização desta política:
Comitê de Segurança da Informação – CSI

Responsável pela aprovação desta política e de atualizações propostas pelo CSI:
Conselho Universitário – Consu

Responsável pela aprovação das Instruções Normativas de segurança da informação:
Coordenadoria Integrada de Tecnologia da Informação e Comunicação – CITIC

12. Atribuições e Responsabilidades
O Comitê de Segurança da Informação responde à CITIC e será designado pelo Reitor por Resolução.

Publicada no D.O.E. em 08/08/2020.