

Instrução Normativa ConTIC-IN-02/2017, de 26 de outubro de 2017

Dispõe sobre a obrigatoriedade do uso de protocolo de canal seguro com certificação, por exemplo SSL, no tráfego de dados institucionais

O Conselho de Tecnologia de Informação e Comunicação (ConTIC), no uso das atribuições conferidas pela Resolução GR Nº 021/2006 de 23/03/2006, com base em proposta aprovada na 117ª Reunião Ordinária do ConTIC de 26/10/2017 e considerando a necessidade de:

1. Identificar corretamente que uma página web pertence à Universidade;
2. Garantir a segurança dos dados sigilosos que trafegam na rede da Universidade;
3. Prover subsídios para cumprir o que está determinado na Resolução GR 52/2012;
4. Garantir a compatibilidade das páginas web da Universidade em navegadores, aparelhos celulares e dispositivos móveis em geral.

Resolve:

Artigo 1º - Para fins desta Instrução Normativa consideram-se os seguintes conceitos:

1. SSL: sigla em inglês para *Secure Sockets Layers*. É um protocolo que provê a privacidade e a integridade de dados entre duas aplicações que se comunicam pela internet. É utilizado em serviços como email (SMTP), navegação por páginas (HTTP) e outros tipos de transferência de dados.
2. HTTPS: sigla em inglês para *Hyper Text Transfer Protocol Secure*. Define um protocolo de comunicação utilizado na internet que protege a integridade e a confidencialidade dos dados entre o computador do usuário e o site que ele deseja acessar.
3. Criptografia: é um conjunto de técnicas matemáticas que permite embaralhar uma mensagem e, assim, impedir que ela seja interpretada por outra pessoa que não o destinatário.
4. Certificado Digital: é um arquivo eletrônico que funciona como se fosse uma assinatura digital, com validade jurídica, e que garante proteção às transações eletrônicas e outros serviços via internet.
5. Autoridade Certificadora (AC): é uma entidade, pública ou privada, responsável por emitir, distribuir, renovar, revogar e/ou gerenciar certificados digitais.
6. Certificado Corporativo: serviço oferecido pela Rede Nacional de Pesquisa (RNP) para a Unicamp, dentro do projeto de Infraestrutura de Chaves Públicas para Ensino e Pesquisa (ICPEdu), onde é permitido às instituições clientes da RNP emitirem gratuitamente certificados digitais qualificados pela GlobalSign.

Artigo 2º - É obrigatória a implantação e uso de um protocolo de canal seguro com certificação, por exemplo SSL, sempre que houver o tráfego de dados institucionais através da rede da Universidade.

§ 1º - A implantação de um protocolo de canal seguro com certificação, por exemplo SSL,

deve ser feito através do uso de certificado digital assinado por Autoridade Certificadora reconhecida pelos principais navegadores web, clientes de e-mail, dispositivos móveis e demais aplicações cliente.

§ 2º - Páginas web da Universidade, que contenham formulários que solicitem dados pessoais dos usuários devem utilizar um protocolo de canal seguro de certificação, por exemplo HTTPS, com certificado digital assinado por Autoridade Certificadora reconhecida pelos principais navegadores web.

§ 3º. Visando garantir o uso racional dos recursos da Universidade, os certificados digitais devem, sempre que possível, serem emitidos através do serviço de Certificado Corporativo oferecido pela RNP, sendo o Centro de Computação (CCUEC) o responsável pela gestão do mesmo.

Artigo 3º - A solicitação de emissão, alteração, renovação ou revogação; instalação e manutenção dos certificados digitais é de responsabilidade do solicitante.

§ 1º. Os certificados digitais assinados pela Autoridade Certificadora GlobalSign na parceria com a RNP no projeto ICPEdu, destinam-se ao serviços computacionais institucionais da Unicamp.

§ 2º. Somente podem solicitar emissão, alteração, renovação ou revogação de certificado digital os colaboradores indicados pelos Órgãos da Unicamp junto ao CCUEC.

§ 3º. O CCUEC é o responsável por estabelecer os requisitos técnicos e operacionais, compatíveis com as especificações definidas pela Autoridade Certificadora GlobalSign, para a emissão, alteração, renovação ou revogação do certificado digital.

Artigo 4º - Os Órgãos da Universidade terão o prazo de 90 (noventa) dias, a contar da data de publicação desta Instrução Normativa, para realizar as mudanças necessárias para adequação dos ambientes computacionais.

Artigo 5º - Os casos omissos serão avaliados pela CTIC e, caso necessário, levados ao ConTIC.

Artigo 6º - Esta Instrução Normativa entra em vigor nesta data.

Prof. Dr. Sandro Rigo
Presidente do Conselho de Tecnologia de Informação e Comunicação
ConTIC / UNICAMP