Instrução Normativa ConTIC-IN-01/2017, de 21 de setembro de 2017

Dispõe sobre a instalação e uso de equipamentos de comunicação de dados sem fio.

O Conselho de Tecnologia de Informação e Comunicação (ConTIC), no uso das atribuições conferidas pela Resolução GR Nº 021/2006 de 23/03/06, com base em proposta aprovada na 117ª Reunião Ordinária do ConTIC de 21/09/2017 e considerando a necessidade de:

1. Estabelecer e manter redes sem fio que sejam seguras e funcionais;
2. Assegurar uma alocação razoável e viável das faixas de frequência, a integridade dos componentes da rede, a distribuição da capacidade de tráfego e a instalação correta de equipamentos de transmissão;
3. Estabelecer medidas contra interferências em outras redes da Universidade;
4. Definir medidas de segurança que protejam os recursos de tecnologia da informação da Universidade contra acessos não autorizados;
5. Garantir a segurança dos dados que trafegam nas redes da Universidade;
6. Atender a determinação da Lei brasileira nº 12.965, de 23 de abril de 2014 que estabelece princípios, direitos e deveres para uso da internet no Brasil resolve:

Artigo 1º- As redes de dados sem fio nos campi da Unicamp são caracterizadas como:

1. Rede sem fio institucional - é a rede sem fio com administração e/ou autenticação centralizadas e que tem como objetivo oferecer acesso à rede da Universidade e à Internet.
2. Rede sem fio da Unidade/Órgão – é a rede sem fio com administração e autenticação localizadas na Unidade/Órgão em que está instalada e que tem como objetivo oferecer acesso aos serviços de rede disponíveis na Unidade/Órgão estendendo e complementando sua rede cabeada.
3. Rede sem fio temporária – é a rede sem fio criada por um período de tempo curto e previamente definido e que tem como objetivo oferecer navegação na Internet para usuários participantes em eventos realizados na Universidade.
4. Rede sem fio de permissionários – é a rede sem fio com administração e autenticação feitas pelo permissionário de serviços da Unicamp (bancos, cantinas, etc.) e que tem como objetivo oferecer acesso à rede de dados do permissionário e/ou à Internet por meio de conexão própria do permissionário a um provedor de serviços de Internet.

Artigo 2º- A implantação de redes de dados sem fio na instituição considera os seguintes conceitos:

1. AP (Access Point) – equipamento que possibilita a interconexão de clientes de uma rede sem fio com uma rede cabeada por meio de ondas de rádio.
2. Cliente – equipamento da rede sem fio que é operada pelo usuário final; é qualquer dispositivo com interface de rádio apropriada para viabilizar a comunicação com um AP.
3. IEEE 802.11 – conjunto de padrões de comunicação sem fio, também conhecidos como padrões Wi-Fi, voltados para comunicações de média distância (dezenas de metros) entre um cliente e um AP ou entre clientes.
4. Bluetooth – tecnologia definida pelo padrão IEEE 802.15.1 voltada para comunicações de curta distância (alguns metros) entre um equipamento principal(computador, telefone celular, etc.) e seus periféricos (teclado, fones, telefones, etc.).
5. ISM – bandas de rádio não licenciadas e reservadas para uso industrial, científico e médico (Industrial, Scientific and Medical radio bands).

6. Dispositivos de IoT (Internet of Things) - no contexto da IoT (ou Internet das Coisas), são dispositivos conectados à rede, que podem ser, por exemplo, câmeras de CFTV, sensores de energia, impressoras, monitores cardíacos, ou qualquer outro dispositivo que utilize a conectividade para realizar suas funções e/ou trafegar dados.
7. Redes sem fio – redes de comunicação de dados que fazem uso de ondas de rádio para estabelecer os enlaces de comunicação entre os componentes.
8. Wi-Fi – termo utilizado para descrever redes locais sem fio baseadas nos padrões IEEE 802.11.

Artigo 3º – Cabe à Unidade/Órgão controlar a utilização de sinais de RF das transmissões de dados sem fio em bandas não licenciadas (faixas ISM de 2.4 GHz e 5 GHz), de forma a garantir que as diversas redes sem fio possam operar em sua região geográfica sem interferências entre si e sem interferências provenientes de outros dispositivos que utilizem a mesma banda.

§ 1º – Um equipamento que venha a emitir ondas de rádio em nível que provoque interrupções, interferências ou sobrecarga em outros serviços ou sistemas da Universidade, deve permanecer desligado até que se consiga eliminar as causas da interferência.

§ 2º – Em caso de interferência entre redes sem fio, deve ser estabelecida a prioridade de uso e o desligamento ou remanejamento de um dos dispositivos.

§ 3º – Os custos associados à eliminação de interferências causadas por equipamentos que se enquadrem nos parágrafos anteriores ficam a cargo da Unidade/Órgão responsável pela rede ou pelo dispositivo que causa as interferências.

Artigo 4º – As redes sem fio devem implantar mecanismos de acesso (login) autenticados e arquivos de logs que registrem todas as autenticações permitindo a rastreabilidade do usuário de forma única e inequívoca.

§ 1º – Os registros de conexão devem ser mantidos sob sigilo, em ambiente controlado e de segurança, pelo prazo de, no mínimo, 1 (um) ano.

Artigo 5º – Usuários sem vínculo formal direto ou indireto com a Universidade podem utilizar uma rede sem fio atendendo um dos seguintes requisitos: utilizando autenticação por conta do usuário em redes sociais previamente autorizadas pela Unicamp ou por credencial temporária criada sob a responsabilidade de um docente ou funcionário.

§ 1º – As redes sociais autorizadas pela Unicamp serão definidas por instrução normativa pelo ConTIC.

§ 2º – A rede sem fio deve garantir, no mínimo, acesso através dos protocolos:

Serviço	**Protocolos**
Web	HTTP, HTTPS
E-mail seguro	IMAPS, POP3S, SMTPS, SMTP-TLS
VPN	OpenVPN, IPSec VPN, L2TP, PPTP, IPsec NAT-T, Cisco IPSec VPN
Mensagem instantânea	Skype, Gtalk, WhatsApp

§ 3º – Os demais protocolos poderão ser permitidos a critério do responsável pela rede sem fio.

§ 4º – A rede deve ter mecanismo de restrição de banda compatível com a disponibilidade de saída.

Artigo 6º – Para dispositivos de IoT (Internet of Things), onde não se aplica a autenticação por conta de usuário, será permitida a autenticação por chave compartilhada e as seguintes recomendações devem ser seguidas:

§ 1º – Adotar medidas de segurança visando impedir acessos indevidos e possíveis problemas para a rede da Universidade:

1. ser criterioso na escolha do fornecedor do dispositivo:

   • verificar políticas de atualização de *firmware*;

   • verificar o histórico de tratamento de vulnerabilidades;

   • verificar se é possível desabilitar serviços desnecessários e trocar senhas;

   • realizar testes antes de efetuar a compra.

2. planejar a implementação:

   - implementar mecanismos de gerência remota;
   - implementar mecanismos de atualização remota;
   - realizar testes em ambientes controlados;
   - isolar os dispositivos da sua rede local utilizando uma rede de gerência;
   - implementar mecanismos de auditorias que permitam rastreabilidade e registros de logs que devem ser mantidos sob sigilo, em ambiente controlado e de segurança, pelo prazo de, no mínimo, 1 (um) ano.

3. manter os dispositivos atualizados.

Artigo 7º – A instalação de uma rede sem fio temporária (para eventos, congressos, etc.) que necessite utilizar a infraestrutura da rede sem fio na Unicamp deve ser solicitada ao responsável da unidade/órgão para a tomada de providências necessárias, respeitando o tempo mínimo definido pela administração local.

Artigo 8º – Os usuários de redes sem fio estão sujeitos a todas as normas constantes na Resolução GR-052/2012 e outras que venham complementá-la ou substituí-la.

Artigo 9º – Os casos omissos serão avaliados pela CTIC e, caso necessário, levados ao ConTIC.

Artigo 10º – Esta Instrução Normativa entra em vigor nesta data revogando-se disposições em contrário.

Prof. Dr. Sandro Rigo

Presidente do Conselho de Tecnologia de Informação e Comunicação

ConTIC / UNICAMP