



PARECER PG 1404/2012

DESPACHO PG 6897/2012

INTERESSADO: Procuradoria Geral - PG

ASSUNTO: Alterações Resolução GR 05/2005

### **DECISÃO ConTIC D-18/2012**

O Conselho de Tecnologia de Informação e Comunicação, em sua 68ª Reunião Ordinária realizada em 06.12.2012, aprovou por unanimidade as alterações sugeridas pela Procuradoria Geral e membros dos Fóruns Técnicos Consultivos de reformulação da Resolução GR 05/2005 conforme documento no anexo.

Cidade Universitária “Zeferino Vaz”

06 de dezembro de 2012

**MARCO AURÉLIO AMARAL HENRIQUES**

Presidente

## **Proposta de atualização da Resolução GR-05/2005**

Em 2011 o Reitor designou, por meio da Portaria GR 106/2011, um Grupo de Trabalho para revisar e propor atualizações das regras sobre contas de correio eletrônico institucional. Fazem parte deste GT o Chefe de Gabinete Adjunto e Membro do ConTIC, Prof. Ricardo Anido, a Procuradora de Universidade Assessora, Dra. Veridiana Ribeiro Porto, e o Coordenador Geral de TIC, Prof. Marco Aurélio A. Henriques. Após algumas reuniões para discutir o assunto, a Dra. Veridiana encaminhou uma proposta de alteração da GR-05/2005 que contempla os objetivos do GT, bem como sugere que algumas das Recomendações ConTIC em avaliação na PG sejam incorporadas ao novo texto.

Aproveitando o ensejo, a CTIC fez uma revisão de toda a GR-05 e propôs uma atualização da mesma de maneira a torná-la não só compatível com a estrutura de gestão de TIC atualmente em vigor, mas também com algumas das práticas, tecnologias e serviços em uso atualmente.

A proposta de texto foi apresentada ao ConTIC em sua reunião ordinária de novembro e em seguida encaminhada para todos os membros dos Fóruns Técnicos Consultivos, com o objetivo de coletar o maior número possível de sugestões de melhorias para o novo texto.

Além disso, foi realizada uma reunião extraordinária do ConTIC no dia 29/11/2012, com o objetivo de adiantar as discussões sobre o texto e permitir que o mesmo chegasse mais amadurecido na reunião ordinária do ConTIC de dezembro. Desta reunião participaram membros do ConTIC e dos FTCs.

O texto final aprovado por unanimidade pelo ConTIC em sua reunião ordinária de dezembro/2012 é agora enviado para análise jurídica pela PG e posteriormente para o Gabinete do Reitor a fim de ser publicado como uma nova Resolução GR.

Cidade Universitária Zeferino Vaz

06 de dezembro de 2012

Marco Aurélio Amaral Henriques  
Coordenador Geral da CTIC

## Proposta de atualização da Resolução GR-05/2005

### Texto atual

RESOLUÇÃO GR Nº 5, de 17-01-2005

Publicada no DOE de 25/01/2005

Reitor: CARLOS HENRIQUE DE BRITO CRUZ

Estabelece as Normas e Procedimentos para o Uso dos Recursos de Tecnologia da Informação e Comunicação na Universidade Estadual de Campinas

O Reitor da Universidade Estadual de Campinas baixa a seguinte resolução:

Artigo 1º – Esta resolução estabelece as Normas e Procedimentos para o Uso dos Recursos de Tecnologia da Informação e Comunicação na Universidade Estadual de Campinas – Unicamp.

Artigo 2º – Para fins desta resolução, considera-se:

I – A Coordenadoria Geral de Informática – CGI, nos termos da Resolução GR-51/2002 como órgão executivo da Reitoria que traça as políticas e programas da Unicamp na área de informática e, uma vez aprovados pela CDI -Comissão Diretora de Informática, coordena a sua execução pelos órgãos executivos.

II – A Comissão Diretora de Informática – CDI, nos termos da Resolução GR-51/2002, como órgão deliberativo da Reitoria que estabelece políticas e programas na área de informática de acordo com propostas encaminhadas pela CGI.

III – Recursos de Tecnologia da Informação e Comunicação – TIC, são os equipamentos, instalações e recursos de informação direta ou indiretamente administrados, mantidos ou operados pelos Órgãos da

### Texto proposto

Resolução GR nº XXX

Publicada no DOE de xx/xx/201x

Reitor: Fernando Ferreira Costa

Estabelece as Normas e Procedimentos para o Uso dos Recursos de Tecnologia da Informação e Comunicação na Universidade Estadual de Campinas

O Reitor da Universidade Estadual de Campinas baixa a seguinte resolução:

Artigo 1º – Esta resolução estabelece as Normas e Procedimentos para o Uso dos Recursos de Tecnologia da Informação e Comunicação na Universidade Estadual de Campinas – Unicamp.

Artigo 2º – Para fins desta resolução, considera-se que:

I – um Órgão da Unicamp é qualquer unidade universitária formalmente constituída como Unidade de Ensino e Pesquisa, Centro, Núcleo ou Órgão Administrativo;

II – a Coordenadoria de Tecnologia de Informação e Comunicação – CTIC, nos termos da Resolução GR-021/2006, de 23/03/2006, é o Órgão executivo da Reitoria que traça as políticas e programas da Unicamp nas áreas de tecnologia da informação e comunicação e que, uma vez aprovados pelo ConTIC – Conselho de Tecnologia da Informação e Comunicação, coordena a sua execução com o apoio do Centro de Computação da Universidade Estadual de Campinas – CCUEC;

III – o Conselho de Tecnologia da Informação e Comunicação – ConTIC, nos termos da Resolução GR-021/2006, é o órgão deliberativo da Reitoria que estabelece políticas e programas nas áreas de tecnologia da informação e comunicação;

IV – os recursos de Tecnologia da Informação e Comunicação – TIC, são os equipamentos, instalações e recursos de informação direta ou indiretamente administrados, mantidos ou operados pelos Órgãos da

Unicamp – Unidades de Ensino e Pesquisa, Centros, Núcleos e Órgãos Administrativos, tais como:

- a) equipamentos de informática de qualquer espécie;
- b) impressoras;
- c) equipamentos de redes e de telecomunicações de qualquer espécie;
- d) laboratórios de informática de qualquer espécie;
- e) recursos de informação que incluem todas as informações eletrônicas, serviço de correio eletrônico, mensagens eletrônicas, dados corporativos, documentos, programas ou software, arquivos de configuração que são armazenados, executados ou transmitidos através da infra-estrutura computacional da Unicamp, redes ou outros sistemas de informação.

IV – Todos os equipamentos conectados à rede Unicamp estão sujeitos às mesmas políticas, diretrizes e regulamentações.

V – Usuário é qualquer pessoa, física ou jurídica, com vínculo oficial com a Unicamp ou em condição autorizada que utiliza, de qualquer forma, algum recurso de TIC da Unicamp.

VI – O Administrador de Sistemas e Rede de um Órgão da Unicamp é pessoa designada formalmente pelo Diretor deste Órgão e tem como atribuição principal o gerenciamento da rede local, bem como dos recursos de TIC do Órgão, a ela conectados, direta ou indiretamente.

VII – A Equipe de Segurança de Recursos Computacionais – CSRC, estabelecida através da Portaria GR-66/97 é responsável pela segurança preventiva, atendimento a emergências de segurança e assessoria à CGI.

VIII – O Representante de Usuários de um Órgão da Unicamp é pessoa designada formalmente pelo Diretor do Órgão, com a atribuição de representar seus usuários, nos assuntos relacionados com a utilização dos serviços oferecidos pelo Centro de

Unicamp, tais como:

- a) equipamentos de informática de qualquer espécie e seus componentes periféricos;
- b) impressoras;
- b) equipamentos de redes e de telecomunicações de qualquer espécie;
- c) laboratórios de informática de qualquer espécie, incluindo, mas não limitados a, salas multimídia e de vídeoconferência;
- d) recursos de informação que incluem todas as informações eletrônicas, serviço de correio eletrônico e outras formas de comunicação eletrônica, dados corporativos, documentos, páginas Web, programas ou software, arquivos de configuração que são armazenados, executados ou transmitidos através da infra-estrutura computacional da Unicamp, redes ou outros sistemas de informação.

V – todos os equipamentos conectados à rede Unicamp estão sujeitos às mesmas políticas, diretrizes e regulamentações;

VI – Usuário é qualquer pessoa, física ou jurídica, com vínculo formal direto ou indireto com a Unicamp, ou em condição autorizada, que utiliza, de qualquer forma, algum recurso de TIC da Unicamp;

VII – vínculo formal indireto é aquele caracterizado pela participação da Unicamp em redes federadas que permitem que usuários formais de outras instituições façam uso de recursos de TIC da Unicamp e vice-versa;

VIII – os Administradores de Sistemas e de Redes de um Órgão da Unicamp são as pessoas designadas formalmente pelo Diretor deste Órgão com a atribuição principal de gerenciar a rede local, bem como os recursos de TIC do Órgão a ela conectados, direta ou indiretamente;

~~VII – A Equipe de Segurança de Recursos Computacionais – CSRC, estabelecida através da Portaria GR-66/97 é responsável pela segurança preventiva, atendimento a emergências de segurança e assessoria à CGI;~~

IX – o Representante de Usuários de um Órgão da Unicamp é a pessoa designada formalmente pelo Diretor do Órgão, com a atribuição de representar seus usuários, nos assuntos relacionados com a utilização dos serviços oferecidos pelo Centro de

Computação da Unicamp – CCUEC.

IX – Uninet – rede corporativa da Unicamp (backbone)

Artigo 3º – Fica aprovado para vigorar a partir de 1º-1-2005, as normas e procedimentos para o uso de recursos de tecnologia da informação e comunicação na Unicamp que com esta baixa.

Parágrafo único – As alterações necessárias nas normas e procedimentos para o uso dos recursos de TIC na Unicamp devem ser analisadas pela CGI e aprovadas pela CDI.

Artigo 4º – Com esta resolução a Unicamp não renuncia a nenhuma pendência que possa ter quanto à propriedade ou controle de quaisquer software e hardware e dos dados criados ou armazenados em seus sistemas ou transmitidos através de sua rede.

Artigo 5º – Violações desta Resolução estarão sujeitas a ações disciplinares da Unicamp específicas e podem resultar em ações disciplinares previstas nos estatutos da Unicamp, e às penas previstas em lei.

§ 1º – A Unicamp adotará ações em consonância com as suas regulamentações, as leis federais, estaduais, municipais e às normas para uso da Internet recomendadas pelo Comitê Gestor da Internet Brasil, para identificar e estabelecer mecanismos técnicos e procedimentos que garantam a funcionalidade, segurança e robustez do ambiente dos recursos de TIC.

§ 2º – A Unicamp reconhece que toda a sua comunidade está sujeita a leis locais, estaduais e federais relacionadas a direitos autorais, privacidade, segurança e outros estatutos relacionados à mídia eletrônica.

Artigo 6º – Esta resolução entrará em vigor na data de sua publicação, revogadas as disposições em contrário, de modo especial a Portaria GR-065/97, Portaria GR-71/97, Portaria GR-17/98 e Resolução GR-170/99.

Normas e Procedimentos de Uso dos Recursos de Tecnologia da Informação e Comunicação – TIC – na

Computação da Unicamp – CCUEC;

X – UniNet é a rede de comunicação de dados da Unicamp, composta por seu *backbone* e pelas demais redes da Unicamp a ele conectadas, responsável por toda a troca de tráfego entre os órgãos e com a Internet.

~~Artigo 3º – Fica aprovado para vigorar a partir de 1º-1-2005, as normas e procedimentos para o uso de recursos de tecnologia da informação e comunicação na Unicamp que com esta baixa.~~

Artigo 3º – As alterações necessárias nas normas e procedimentos para o uso dos recursos de TIC na Unicamp devem ser analisadas pela **CTIC** e aprovadas pelo **ConTIC**.

Artigo 4º – Com esta Resolução a Unicamp não renuncia a nenhuma pendência que possa ter quanto à propriedade ou controle de quaisquer software e hardware e dos dados criados ou armazenados em seus sistemas ou transmitidos através de sua rede.

Artigo 5º – Violações desta Resolução estarão sujeitas a ações disciplinares da Unicamp específicas e podem resultar em ações disciplinares previstas nos estatutos da Unicamp, e às penas previstas em lei.

§ 1º – A Unicamp adotará ações em consonância com as suas regulamentações, as leis federais, estaduais, municipais e às normas para uso da Internet recomendadas pelo Comitê Gestor da Internet Brasil, para identificar e estabelecer mecanismos técnicos e procedimentos que garantam a funcionalidade, segurança e robustez do ambiente dos recursos de TIC.

§ 2º – A Unicamp reconhece que toda a sua comunidade está sujeita a leis locais, estaduais e federais relacionadas a direitos autorais, privacidade, segurança e outros estatutos relacionados à mídia eletrônica.

~~Artigo 6º – Esta resolução entrará em vigor na data de sua publicação, revogadas as disposições em contrário, de modo especial a Portaria GR-065/97, Portaria GR-71/97, Portaria GR-17/98 e Resolução GR-170/99.~~

~~Normas e Procedimentos de Uso dos Recursos de Tecnologia da Informação e Comunicação – TIC – na~~

## CAPÍTULO I

### Das Normas de Uso e Segurança dos Recursos Computacionais

Artigo 1º – É política da Unicamp prover para a sua comunidade o acesso a fontes de informação locais, nacionais e internacionais, promovendo um ambiente de produção, uso e compartilhamento do conhecimento e de comprometimento com a liberdade acadêmica.

§ 1º – As fontes de informações devem ser utilizadas pelos membros da comunidade dentro do respeito e da ética de acordo com as regulamentações estabelecidas pela Unicamp.

§ 2º – Os Recursos Computacionais ou Recursos de TIC, como definidos na Resolução GR Nº. 05/2005, devem ser utilizados de maneira responsável, consistente com objetivos educacionais, de pesquisa e administrativos da UNICAMP.

§ 3º – O uso deve estar de acordo com os objetivos específicos do projeto ou tarefa para a qual o uso foi autorizado.

§ 4º – Todas as utilizações que não estiverem de acordo com estes objetivos são consideradas inapropriadas e podem colocar em risco os demais acessos a serviços.

§ 5º – Os Recursos Computacionais da Unicamp não podem ser utilizados para constranger, assediar, ameaçar ou perseguir qualquer pessoa.

§ 3º (do Art. 60) – Material obtido de forma fraudulenta, racista, profana, obscena, intimidadora, difamatória, ilegal, ofensiva, abusiva ou inapropriada não pode ser enviado via correio eletrônico ou através de qualquer outra forma de comunicação eletrônica.

§ 6º – Os Recursos Computacionais da Unicamp não podem ser usados para invadir, alterar ou destruir recursos computacionais de outras instituições.

§ 7º – Se a partir de uma conta, um Usuário estiver, de qualquer maneira, interferindo no trabalho de um outro usuário, este deve comunicar o fato ao responsável pelo equipamento onde está a conta, o

## CAPÍTULO I

### Das Normas de Uso e Segurança dos Recursos Computacionais

Artigo 6º – É política da Unicamp prover para a sua comunidade o acesso a fontes de informação locais, nacionais e internacionais, promovendo um ambiente de produção, uso e compartilhamento do conhecimento e de comprometimento com a liberdade acadêmica.

**Parágrafo Único** – As fontes de informações devem ser utilizadas pelos membros da comunidade dentro do respeito e da ética de acordo com as regulamentações estabelecidas pela Unicamp.

Artigo 7º – Os Recursos Computacionais ou Recursos de TIC, como definidos **nesta Resolução**, devem ser utilizados de maneira responsável, consistente com objetivos educacionais, de pesquisa e administrativos da UNICAMP.

§ 1º – O uso **dos recursos** deve estar de acordo com os objetivos específicos do projeto ou tarefa para a **qual foi** autorizado.

§ 2º – Todas as utilizações que não estiverem de acordo com estes objetivos são consideradas inapropriadas e podem colocar em risco os demais acessos a serviços.

§ 3º – Os Recursos Computacionais da Unicamp não podem ser utilizados para constranger, assediar, ameaçar ou perseguir qualquer pessoa.

§ 4º – É vedado o envio, por meio de qualquer forma de comunicação eletrônica, de material racista, profano, obsceno, intimidador, difamatório, ilegal, ofensivo, abusivo, inapropriado ou obtido de forma fraudulenta.

§ 5º – Os Recursos Computacionais da Unicamp não podem ser usados para invadir, alterar ou destruir recursos computacionais de outras instituições.

Artigo 8º – Se a partir de uma conta **qualquer**, um Usuário **interferir** no trabalho de um outro usuário, este **último** deverá comunicar o fato ao responsável pelo equipamento **onde a conta está sendo utilizada**, o

qual, a seu critério, e sem prejuízo de outras sanções, poderá determinar a imediata suspensão temporária da conta de onde parte a interferência, comunicando o caso a Equipe de Segurança de Recursos Computacionais.

Artigo 2º – Constituem responsabilidades do Usuário relativamente ao uso dos Recursos Computacionais da Unicamp:

I. Respeitar todas as políticas e procedimentos da Unicamp incluindo, mas não limitado, às normas e procedimentos de uso dos recursos de TIC.

II. Respeitar os direitos de outros usuários, incluindo os direitos garantidos em outras políticas da Unicamp para alunos, docentes e funcionários.

III. Utilizar qualquer Recurso Computacional da Unicamp somente após obter uma autorização por escrito e assinar o Termo de Responsabilidade, no qual declara conhecer as políticas e normas em vigor e se compromete a cumpri-las.

IV. Exibir a comprovação de vínculo com a Unicamp ou autorização especial ao pessoal responsável, sempre que solicitado durante a utilização dos recursos, sob pena de imediata suspensão da conexão, sem prejuízo das disposições legais pertinentes.

V. Respeitar a integridade e limites de sua autorização de acesso ou conta.

VI. Qualquer atividade desenvolvida com o auxílio dos recursos computacionais da Unicamp e pelos eventuais prejuízos dela decorrentes, em qualquer nível.

VII. A segurança de suas contas e de suas senhas – a conta e a respectiva senha são atribuídas a um único usuário e não devem ser compartilhadas com mais pessoas sem a autorização expressa e por escrito da CGI.

VIII. Informar imediatamente a Equipe de Segurança de Recursos Computacionais qualquer suspeita de tentativa de violação de segurança, em qualquer nível.

qual, mediante justificativa devidamente fundamentada por escrito, poderá determinar a imediata suspensão temporária da conta de onde parte a interferência.

Parágrafo Único – Estão excluídas do escopo deste Artigo as atividades de administração do sistema, preventivas ou corretivas, que venham a interferir direta ou indiretamente nas atividades dos usuários.

Artigo 9º – Constituem responsabilidades do Usuário relativamente ao uso dos Recursos Computacionais da Unicamp:

I – respeitar todas as políticas e procedimentos da Unicamp incluindo, mas não limitado a, normas e procedimentos de uso dos recursos de TIC;

II – respeitar os direitos de outros usuários, incluindo os direitos garantidos em outras políticas da Unicamp;

III – utilizar qualquer Recurso Computacional da Unicamp somente após obter autorização e aderir a um Termo de Responsabilidade, no qual declara conhecer as políticas e normas em vigor e se compromete a cumpri-las;

IV – exibir a comprovação de vínculo com a Unicamp ou autorização especial ao pessoal responsável, sempre que solicitado durante a utilização dos recursos, sob pena de imediata suspensão do acesso a recursos TIC, sem prejuízo das disposições legais pertinentes;

V – respeitar a integridade e limites de sua autorização de acesso ou conta;

VI – responder pelos eventuais prejuízos decorrentes de qualquer atividade desenvolvida com o auxílio dos recursos computacionais da Unicamp;

VII – a segurança de suas contas e de suas senhas – a conta e a respectiva senha são atribuídas a um único usuário e não devem ser compartilhadas com mais pessoas sem a autorização expressa e por escrito do responsável pelo sistema de contas utilizado;

VIII – informar imediatamente aos Administradores de Sistemas e de Redes locais ou ao SAU (Serviço de Apoio ao Usuário) do CCUEC qualquer suspeita de



IX. Não permitir ou colaborar com o acesso aos Recursos Computacionais da Unicamp por parte de pessoas não autorizadas, sob pena de ser responsabilizado pelos eventuais problemas que esses acessos vierem a causar.

X. Usar o computador, sistema ou a rede de forma a não interferir ou interromper a operação normal do computador, sistema ou rede.

XI. Respeitar a integridade dos recursos computacionais da Unicamp. Os usuários, a menos que tenham uma autorização específica para esse fim, não podem tentar, permitir ou causar qualquer alteração ou destruição de ambientes operacionais, dados ou equipamentos de processamento ou comunicações instalados na Universidade, de sua propriedade ou de qualquer outra pessoa ou instituição.

XII. Não ligar ou desligar fisicamente ou eletricamente a um recurso computacional da Unicamp, nenhum componente externo, como cabos, impressoras, discos ou sistemas de vídeo, sem uma autorização específica.

XIII. Respeitar os direitos de propriedade intelectual, de acordo com a regulamentação pertinente, em particular a lei de direitos autorais de software.

XIV. Utilizar apenas produtos de software com as licenças de uso válidas.

XV. Respeitar todas as obrigações contratuais da Unicamp, inclusive com as limitações definidas nos contratos de software e outras licenças no uso dos Recursos Computacionais.

XVI. Comunicar ao Administrador de Sistemas e Rede local ou a Equipe de Segurança de Recursos Computacionais qualquer evidência de violação das normas em vigor, não podendo acobertar, esconder ou ajudar a esconder violações de terceiros, de qualquer natureza.

tentativa de violação de segurança, em qualquer nível;

IX – não permitir ou colaborar com o acesso aos Recursos Computacionais da Unicamp por parte de pessoas não autorizadas, sob pena de ser responsabilizado pelos eventuais problemas que esses acessos vierem a causar;

X – usar o computador, sistema ou a rede de forma a não interferir ou interromper a operação normal do computador, sistema ou rede;

XI – respeitar a integridade dos recursos computacionais da Unicamp;

XII – não conectar, física ou logicamente, a um recurso computacional da Unicamp componentes estranhos à sua configuração atual, sem que haja uma autorização genérica ou específica fornecida pelos Administradores de Sistemas e de Redes;

XIII – respeitar os direitos de propriedade intelectual, de acordo com a regulamentação pertinente, em particular a lei de direitos autorais de software;

XIV – utilizar apenas produtos de software com as licenças de uso válidas;

XV – respeitar todas as obrigações contratuais da Unicamp, inclusive com as limitações definidas nos contratos de software e outras licenças no uso dos Recursos Computacionais;

XVI – comunicar aos Administradores de Sistemas e de Redes locais ou ao CCUEC qualquer evidência de violação das normas em vigor, não podendo acobertar, esconder ou ajudar a esconder violações de terceiros, de qualquer natureza.

Parágrafo Único – A menos que tenham uma autorização específica para esse fim, é vedado aos usuários permitir ou causar qualquer alteração ou destruição de ambientes operacionais, dados ou equipamentos de processamento ou comunicações instalados na Universidade, de sua propriedade ou de



Artigo 3º – Constituem responsabilidades do Administrador de Sistemas e Rede:

I. Proteger os direitos dos usuários, fixar políticas consistentes com estes direitos e levar ao conhecimento dos usuários estas políticas.

II. Controlar e, se for o caso, vetar o acesso a qualquer um que violar estas políticas ou ameaçar os direitos de outros usuários.

III. Decidir sobre procedimentos locais referentes a:

- a) Armazenamento das mensagens recebidas
- b) Armazenamento das mensagens em pastas pessoais
- c) Mensagens não lidas na caixa de entrada
- d) Acúmulo de mensagens em contas
- e) Retenção de cópia de segurança
- f) Retenção de mensagens enviadas e mensagens descartadas

IV. Notificar os usuários afetados pelas decisões tomadas quanto à matéria prevista no inciso anterior.

Artigo 4º – A Unicamp caracteriza como não ético e inaceitável e considera como motivo de ação disciplinar prevista em seus estatutos qualquer atividade através da qual um indivíduo:

I. Viole questões tais como direitos autorais ou proteção de patentes e autorizações da Unicamp ou de terceiros, como também licenças de uso e outros contratos.

II. Interfira no uso correto dos recursos de informação.

III. Tente conseguir ou consiga acesso não autorizado a recursos de informação.

IV. Sem autorização, destrói, altera, desmonta, desconfigura, impede o acesso de direito ou interfere

qualquer outra pessoa ou instituição.

Artigo 10 – Constituem responsabilidades dos Administradores de Sistemas e de Redes de cada Órgão:

I – proteger os direitos dos usuários, fixar políticas consistentes com estes direitos e levar ao conhecimento dos usuários estas políticas;

II – controlar e, se for o caso, vetar o acesso a qualquer um que violar estas políticas ou ameaçar os direitos de outros usuários;

III – propor, obter aprovação da direção do Órgão e implantar políticas locais de TIC em consonância com estas normas e demais regulamentações publicadas pela CTIC;

- ~~a) armazenamento das mensagens recebidas;~~
- ~~b) armazenamento das mensagens em pastas pessoais;~~
- ~~c) mensagens não lidas na caixa de entrada;~~
- ~~d) acúmulo de mensagens em contas;~~
- ~~e) retenção de cópia de segurança;~~
- ~~f) retenção de mensagens enviadas e mensagens descartadas.~~

IV – notificar os usuários afetados pelas decisões tomadas quanto à matéria prevista no Inciso anterior;

V – promover a segurança preventiva e realizar o tratamento de incidentes de segurança na UniNET em colaboração com o CCUEC.

Artigo 11 – A Unicamp caracteriza como não ético e inaceitável e considera como motivo de ação disciplinar prevista em seus estatutos qualquer atividade através da qual um indivíduo:

I – viole questões tais como direitos autorais ou proteção de patentes e autorizações da Unicamp ou de terceiros, como também licenças de uso e outros contratos;

II – interfira no uso correto dos recursos de informação;

III – tente conseguir ou consiga acesso não autorizado a recursos de informação;

IV – sem autorização, destrua, altere, desmonte, desconfigure, impeça o acesso de direito ou interfira

na integridade dos recursos computacionais.

V. Sem autorização, invade a privacidade de indivíduos ou entidades que são autores, criadores, usuários ou responsáveis pelos recursos computacionais.

VI. Remova dos recursos computacionais da Unicamp algum documento de propriedade da Unicamp ou por ela administrado, sem uma autorização específica.

VII. Se faça passar por outra pessoa ou esconda sua identidade na utilização dos Recursos Computacionais da Unicamp com exceção dos casos em que o acesso anônimo é explicitamente permitido.

VIII. Viole ou tente violar os sistemas de segurança dos recursos computacionais da Unicamp, como quebrar ou tentar adivinhar identificação ou senhas de terceiros, interferir em fechaduras automáticas ou sistemas de alarme.

IX. Intercepte ou tente interceptar transmissão de dados não destinados ao seu próprio acesso.

X. Tente interferir ou interfira em serviços de outros usuários ou o seu bloqueio, provocando, por exemplo, congestionamento da rede, inserindo vírus ou tentando a apropriação dos Recursos Computacionais da Unicamp.

XI. Consiga benefícios financeiros ou de outra espécie diretos, para si ou para terceiros fora da Universidade através da utilização dos recursos computacionais da Unicamp exceto quando autorizado explicitamente pelo Diretor do Órgão para os recursos locais ou pelo Coordenador Geral de Informática no caso dos recursos computacionais corporativos.

Artigo 5º – As penalidades a serem aplicadas às condutas elencadas no artigo anterior, sem prejuízo de outras penas previstas em lei ou em normas da Universidade, são: redução ou eliminação, temporárias ou permanentes, de privilégios de acesso, tanto aos Recursos Computacionais, quanto às redes, salas de computadores da Unicamp e outros serviços ou facilidades.

Artigo 6º – Qualquer violação ou suspeita de violação dessas normas deve ser comunicada imediatamente ao

na integridade dos recursos computacionais;

V – sem autorização, **invada** a privacidade de indivíduos ou entidades que são autores, criadores, usuários ou responsáveis pelos recursos computacionais;

VI – **remova** dos recursos computacionais da Unicamp algum documento de propriedade da Unicamp ou por ela administrado, sem uma autorização específica;

VII – **faça-se** passar por outra pessoa ou esconda sua identidade na utilização dos Recursos Computacionais da Unicamp com exceção dos casos em que o acesso anônimo é explicitamente permitido;

VIII – **viole** ou tente violar os sistemas de segurança dos recursos computacionais da Unicamp, como quebrar ou tentar adivinhar identificação ou senhas de terceiros, interferir em fechaduras automáticas ou sistemas de alarme;

IX – **intercepte** ou tente interceptar transmissão de dados não destinados ao seu próprio acesso;

X – **tente** interferir ou interfira em serviços de outros usuários ou **cause** seu bloqueio, provocando, por exemplo, congestionamento da rede, inserindo vírus ou tentando **se apropriar, ainda que temporariamente**, dos Recursos Computacionais da Unicamp;

XI – **consiga** benefícios financeiros ou de outra espécie diretos, para si ou para terceiros fora da Universidade através da utilização dos recursos computacionais da Unicamp, exceto quando autorizado explicitamente pelo Diretor do Órgão para os recursos locais ou pela **CTIC** no caso dos recursos computacionais corporativos.

Artigo 12 – As penalidades a serem aplicadas às condutas elencadas no **Artigo 11**, sem prejuízo de outras penas previstas em lei ou em normas da Universidade, são: redução ou eliminação, temporária ou permanente, **de privilégios de acesso aos Recursos Computacionais, tais como redes, salas de computadores e outros serviços ou facilidades da Unicamp.**

Artigo 13 – Qualquer violação ou suspeita de violação dessas normas deve ser comunicada

responsável direto pelo recurso computacional no local onde o fato tenha ocorrido.

Artigo 7º – A infração ou tentativa de infração às regras constantes desta norma ou às regras previstas em lei serão apuradas por meio de sindicância administrativa, processo administrativo disciplinar ou processo sumário, nos termos do Regimento Geral e Estatuto dos Servidores da Unicamp.

Artigo 8º – Sempre que julgar necessário para a preservação da integridade dos Recursos Computacionais da Unicamp, dos serviços aos usuários ou dos dados, o Administrador de Sistemas e Rede poderá suspender temporariamente qualquer conta, seja o responsável pela conta suspeito de alguma violação, ou não.

Artigo 9º – Esta Norma se aplica a qualquer membro da comunidade universitária, quer ele esteja dentro da Unicamp ou fora, e se refere a todos os recursos computacionais, controlados individualmente ou compartilhados, isolados ou em rede.

Artigo 10 – Os Órgãos da Unicamp podem definir condições de uso específicas para os recursos sob seu controle, consistentes com a política geral, mas com detalhes, diretrizes e/ou restrições adicionais.

Artigo 11 – Cabe ao Órgão tratar das violações de restrições adicionais de acordo com as normas internas vigentes e onde não houver estes mecanismos específicos, o exposto nesta Norma deve prevalecer.

Artigo 12 – No caso do uso de redes externas, as políticas envolvendo este tipo de uso também são aplicáveis e precisam ser adotadas.

## CAPÍTULO II

Das Normas da Uninet – Rede Corporativa da Unicamp

Artigo 13 – São requisitos mínimos a serem satisfeitos pelas redes locais das Unidades de Ensino e Pesquisa, Órgãos e Unidades Administrativas para se ligarem a UniNet os seguintes:

I. Todo Órgão da Unicamp que queira se ligar a UniNet deve possuir um Administrador de Sistemas e

imediatamente ao responsável direto pelo recurso computacional no local onde o fato tenha ocorrido.

Artigo 14 – A infração ou tentativa de infração às regras constantes desta norma ou às regras previstas em lei serão apuradas por meio de sindicância administrativa, processo administrativo disciplinar ou processo sumário, nos termos do Regimento Geral e do Estatuto dos Servidores da Unicamp.

Artigo 15 – Sempre que julgar necessário para a preservação da integridade dos Recursos Computacionais da Unicamp, dos serviços aos usuários ou dos dados, **os Administradores de Sistemas e de Redes poderão, mediante justificativa devidamente fundamentada,** suspender temporariamente qualquer conta, seja o responsável pela conta suspeito de alguma violação, ou não.

Artigo 16 – Esta Resolução aplica-se a qualquer membro da comunidade universitária, quer ele esteja dentro da Unicamp ou fora, e refere-se a todos os recursos computacionais, controlados individualmente, **compartilhados,** isolados ou em rede.

Artigo 17 – Os Órgãos da Unicamp podem definir condições de uso específicas para os recursos sob seu controle, consistentes com a política geral, mas com detalhes, diretrizes e/ou restrições adicionais.

Artigo 18 – Cabe ao Órgão tratar das violações de restrições adicionais de acordo com as normas internas vigentes e onde não houver estes mecanismos específicos, o exposto nesta Norma deve prevalecer.

Artigo 19 – **A presente norma é aplicável e deve ser adotada também quando houver uso de redes externas a partir de uma das redes da Unicamp.**

## CAPÍTULO II

**Das Normas da UniNet**

Artigo 20 – **Os requisitos mínimos a serem satisfeitos pelas redes locais dos Órgãos da Unicamp para se ligarem a UniNet são:**

I – **todo** Órgão da Unicamp que queira se ligar à UniNet deve possuir **pelo menos** um **Administrador**

Rede que será responsável pela administração e manutenção da rede interna do Órgão, devendo possuir o perfil para o exercício da função e se comprometer a seguir as recomendações descritas no Guia do Administrador de Redes da Unicamp;

II. Cada Órgão conectado a UniNet deve permitir a conexão de um novo Órgão através de um ponto na sua rede local quando não houver viabilidade técnica para atendê-la;

III. Cada Órgão tem o direito de se conectar a rede da Unicamp através de um único ponto.

A conexão pode ser feita diretamente ao backbone ou através de um ponto à rede de outra Unidade geograficamente mais próxima;

IV. A definição do ponto de conexão (backbone ou rede de uma Unidade) será feita pelo Centro de Computação da Unicamp – CCUEC;

V. A conexão única da Unidade a UniNet deve ser efetuada através de um gateway/router. Qualquer outro tipo de equipamento que possa substituir o gateway/router somente poderá ser instalado com a autorização do CCUEC;

VI. Para uma nova Unidade se conectar a rede da Unicamp, ela deve apresentar uma proposta ou projeto que especifique a necessidade de conexão à rede; a proposta deve ser preliminarmente submetida ao CCUEC para avaliação e parecer;

VII. É de responsabilidade da Unidade proteger seus equipamentos, a fim de evitar conexões e alterações físicas à sua rede local. Para tanto deve manter repetidores, switches, hubs, e outros equipamentos, em locais de acesso restrito.

## SEÇÃO I

Da distribuição de blocos de endereços IP alocados à Unicamp pelo órgão competente da Internet-BR

Artigo 14 – Compete ao CCUEC cuidar do controle dos blocos de endereços IP alocados à Unicamp e de sua distribuição às Unidades, com base em justificativas técnicas das suas necessidades.

de Sistemas e de Redes, que será responsável pela administração e manutenção da rede interna do Órgão, devendo possuir o perfil para o exercício da função e comprometer-se a seguir as normas descritas nesta resolução;

II – cada Órgão conectado a UniNet deve permitir a conexão de um outro Órgão através de um ponto na sua rede local quando não houver viabilidade técnica ou econômica para atender este segundo Órgão diretamente;

III – cada Órgão tem o direito de se conectar direta ou indiretamente ao *backbone* da UniNet através de pelo menos um ponto de conexão;

IV – a conexão pode ser feita diretamente ao backbone ou através de um ponto da rede de outro Órgão;

V – a definição do ponto de conexão (*backbone* ou rede de um Órgão) será feita pelo Centro de Computação da Unicamp – CCUEC;

VI – a conexão do Órgão à UniNet deve ser efetuada através de um roteador ou de outro tipo de equipamento que tenha sido previamente autorizado pelo CCUEC;

VII – a conexão de um novo Órgão à UniNet só poderá ser feita mediante avaliação e autorização do CCUEC com base em uma proposta ou projeto que especifique as características da conexão e justifique sua necessidade.

Parágrafo Único – É responsabilidade do Órgão proteger seus equipamentos em locais de acesso restrito, a fim de evitar conexões e alterações físicas não autorizadas em sua rede local.

## SEÇÃO I

Da distribuição de blocos de endereços IP alocados à Unicamp pelo órgão competente da Internet-BR

Artigo 21 – Compete ao CCUEC cuidar do controle dos blocos de endereços IP alocados à Unicamp e de sua distribuição aos Órgãos, conforme Instrução Normativa específica para este fim.

§ 1º – Os endereços IP serão distribuídos em blocos de 254 endereços.

§ 2º – Excepcionalmente poderá haver Unidades recebendo 128 ou até 64 endereços.

Artigo 15 – Compete às Unidades alterar ou não a máscara de suas sub-redes, assumindo para si a responsabilidade de tratar o roteamento de forma eficiente.

## SEÇÃO II

Da distribuição dos blocos de endereços IP especialmente reservados (RFC 1918) para a construção de Intranets

Artigo 16 – Compete ao CCUEC cuidar da distribuição dos blocos de endereços especialmente reservados para a construção de Intranets nas Unidades da Unicamp.

Artigo 17 – A distribuição deve ser normatizada de forma a garantir unicidade de blocos de endereço por Unidade.

Artigo 18 – Compete à Unidade cuidar da configuração de seus roteadores, firewalls, gateway e outros equipamentos, de modo a evitar que os endereços especialmente reservados sejam visíveis no backbone da Unicamp.

Artigo 19 – Para sub-redes da Unicamp onde não há acesso à Internet ou tal acesso é bastante restrito, devem ser especialmente utilizados blocos de endereços reservados, adquiridos junto ao CCUEC, obedecendo ao disposto no artigo anterior.

Artigo 20 – Para cada Unidade serão distribuídos blocos de até 254 endereços IP reservados.

## SEÇÃO III

Da atribuição de Nameservers da Unicamp

~~§ 1º – Os endereços IPv4 serão distribuídos em blocos de até 254 endereços, com base em justificativas técnicas sobre as necessidades do Órgão.~~

~~§ 2º – Excepcionalmente poderá haver Unidades recebendo 128 ou até 64 endereços.~~

Artigo 22 – Compete aos Órgãos alterar ou não a máscara de suas sub-redes, assumindo a responsabilidade de tratar o roteamento de forma eficiente.

## SEÇÃO II

Da distribuição dos blocos de endereços IPv4 especialmente reservados (RFC 1918) para a construção de Intranets

Artigo 23 – Os blocos de endereços especialmente reservados para a construção de intranets (RFC 1918) nos Órgãos da Unicamp podem ser utilizados livremente pelos Administradores de Sistemas e de Redes.

Artigo 24 – Os blocos de endereços especialmente reservados não podem ser roteados no *backbone* da UniNet.

Parágrafo Único – Caso exista a necessidade do roteamento citado no *caput*, deverá ser utilizado um bloco de endereço reservado especialmente definido para esta finalidade, o qual será designado pelo CCUEC.

~~Artigo 25 – Compete ao Órgão cuidar da configuração de seus roteadores, firewalls, gateways e outros equipamentos, de modo a evitar que os endereços especialmente reservados sejam visíveis no *backbone* da Unicamp.~~

~~Artigo 26 – Para sub-redes da Unicamp onde não há acesso à Internet ou tal acesso é bastante restrito, devem ser especialmente utilizados blocos de endereços reservados, obtidos junto ao CCUEC, obedecendo ao disposto no Artigo 25.~~

~~Artigo 27 – Para cada Órgão serão distribuídos blocos de até 254 endereços IPv4 reservados.~~

## SEÇÃO III

Da atribuição de servidores de nomes – DNS

Artigo 21 – Compete à Unidade que possui servidor próprio de DNS a atualização permanente de seus dados.

Artigo 22 – A Unidade deverá informar ao CCUEC qualquer alteração de configuração que afete o servidor de DNS primário da Unicamp.

Parágrafo único – Os servidores de DNS da Unicamp devem ser mantidos com versões de software atualizadas, para se evitar problemas de contaminação por "vírus" e/ou falhas de segurança gerados por outros servidores na Internet.

Artigo 23 – A Unidade que desejar ter DNS próprio deverá contatar o CCUEC para viabilizar tal processo e atualizar o servidor primário de DNS da Unicamp.

Artigo 24 – Os servidores de DNS da Unicamp não devem permitir a transferência de seus mapas (zone files) por outros servidores que não sejam seus servidores secundários.

§ 1º – O servidor de DNS primário da Unicamp somente delegará autoridade para o domínio de uma Unidade e não a determinados departamentos da mesma.

§ 2º – A Unidade deve administrar os mapas de seu domínio, incluindo todas as sub-redes que atende seus laboratórios e departamentos.

Artigo 25 – Os servidores de DNS secundários das Unidades devem ser definidos dentro do próprio domínio ".Unicamp.br", não se permitindo que isto ocorra fora dele.

#### SEÇÃO IV

Da gateways/roteadores da UniNet

Artigo 26- Os gateways/roteadores da UniNet devem atender as seguintes características:

- I. Suportar roteamento dinâmico e multiprotocolar;
- II. Realizar roteamento através de software e protocolos definidos pelo CCUEC;
- III. Realizar roteamento multicast, quando necessário,

Artigo 25 – Compete ao Órgão que possui servidor DNS próprio garantir a atualização permanente de seus dados.

Artigo 26 – O Órgão deverá informar ao CCUEC qualquer alteração de configuração que afete o servidor DNS primário da Unicamp.

Parágrafo Único – Os servidores DNS da Unicamp devem ser mantidos com versões de software atualizadas, para se evitar problemas de contaminação por "vírus" e/ou falhas de segurança gerados por outros servidores na Internet.

Artigo 27 – O Órgão que desejar ter DNS próprio deverá contatar o CCUEC para viabilizar tal processo e atualizar o servidor primário de DNS da Unicamp.

Artigo 28 – Os servidores DNS da Unicamp não devem permitir a transferência de seus mapas (zone files) por outros servidores que não sejam seus servidores secundários.

§ 1º – O servidor DNS primário da Unicamp somente delegará autoridade para o domínio de um Órgão e não para determinados departamentos do mesmo.

§ 2º – O Órgão deve administrar os mapas de seu domínio, incluindo todas as sub-redes que atendem seus laboratórios e departamentos.

Artigo 29 – Os servidores DNS secundários dos Órgãos só podem ser definidos dentro do domínio ".unicamp.br".

#### SEÇÃO IV

Dos roteadores conectados ao backbone da UniNet

Artigo 30 – Os roteadores conectados ao backbone da UniNet devem atender as seguintes normas:

- I – suportar roteamento dinâmico e multiprotocolar;
- II – realizar roteamento através de equipamentos, protocolos e configurações definidas por meio de Instrução Normativa ConTIC;
- ~~III – realizar roteamento multicast, quando~~



através de software e protocolos de roteamento definidos pelo CCUEC;

IV. Não fazer roteamento de redes reservadas definidas pela RFC 1918, fazendo apenas anúncio das rotas da UniNet para suas redes internas;

V. Não divulgar rota padrão para os demais gateways/roteadores da UniNet, sendo este um papel unicamente de responsabilidade do gateway/roteador entre a rede UniNet e a rede ANSP;

VI. Ser dedicado unicamente ao serviço de roteamento e filtragem de pacotes e não possuir serviços destinados a usuários, tais como: correio eletrônico, www, pop, imap, listas de discussão, print server, ftp, entre outros;

VII. Não possuir contas destinadas a usuários, devendo conter apenas contas para os Administradores de Redes da Unidade e para Administradores da UniNet quando necessário;

VIII. Permitir o acesso remoto apenas aos hosts definidos como seguros pelo Administrador da UniNet e da Unidade; este acesso somente será permitido através de software com criptografia, definido pelo CCUEC;

IX. Implementar o filtro de pacotes de acordo com as diretrizes da Coordenadoria Geral de Informática – CGI e CCUEC, levando em conta as políticas de rede adotadas pela Unidade;

X. Utilizar os sistemas operacionais conforme orientação do CCUEC;

XI. Manter atualizadas (as mais recentes) as versões de software e sistema operacional, com todas as correções dos problemas já conhecidos, inclusive os de segurança;

XII. Localizar-se fisicamente num ambiente cujo acesso seja permitido exclusivamente aos Administradores de Rede da Unidade.

~~necessário, através de software e protocolos de roteamento definidos pelo CCUEC;~~

III – não fazer roteamento de redes reservadas definidas pela RFC 1918, **exceto com autorização do CCUEC**, fazendo apenas **anúncio** das rotas da UniNet para suas redes internas;

IV – quando conectado diretamente ao *backbone* da UniNet, não divulgar rota padrão para os demais roteadores conectados ao *backbone*, sendo este um papel unicamente de responsabilidade dos roteadores definidos pelo CCUEC;

~~V – ser dedicado unicamente ao serviço de roteamento e filtragem de pacotes e não possuir serviços destinados a usuários, tais como: correio eletrônico, www, pop, imap, listas de discussão, print server, ftp, entre outros;~~

~~VI – não possuir contas destinadas a usuários, mas apenas contas para os Administradores de Redes do Órgão e para Administradores da UniNet, quando necessário;~~

~~VII – permitir o acesso remoto apenas aos computadores definidos como seguros pelo Administrador de Sistemas e de Redes do Órgão, sendo este acesso feito apenas por meio de software que utilize recursos de criptografia forte (128 bits pelo menos) e que proteja todos os dados trafegados, incluindo aqueles necessários para autenticação do usuário;~~

V – implementar o filtro de pacotes de acordo com as diretrizes da **CTIC e do CCUEC**, levando em conta as políticas de rede **adotadas pelo Órgão**;

VI – utilizar os sistemas operacionais conforme orientação do CCUEC;

VII – manter **atualizadas as versões** de software e de sistema operacional, com **a aplicação** de todas as correções dos problemas já **conhecidos**;

VIII – localizar-se fisicamente num ambiente cujo acesso seja permitido exclusivamente aos Administradores **de Sistemas e de Redes do Órgão e a pessoas por eles autorizadas ou acompanhadas.**



## SEÇÃO V

### Do roteamento na UniNet

Artigo 27 – São deveres da:

§ 1º – Não anunciar rotas para as redes reservadas definidas pela RFC 1918;

§ 2º – Não anunciar rota padrão na UniNet, com exceção do gateway/roteador que interconecta a rede UniNet à rede ANSP;

§ 3º – Anunciar na UniNet somente rotas para as redes internas da Unidade, previamente alocadas à Unidade;

Artigo 28 – O roteamento multicast deve ser realizado de forma a não existir túneis na UniNet.

Artigo 29 – O Roteamento para teste em IPv6 deve ser encapsulado via IPv4, até que normas de implantação, adequação e utilização sejam normatizadas pela CGI.

## SEÇÃO VI

### Do filtro de pacotes

Artigo 30 – Os Filtros que podem ser aplicados no roteador/gateway de conexão da UniNet à rede ANSP são os seguintes:

- a) Filtro de pacotes objetivando que os recursos computacionais das Unidades não sejam utilizados como base de ataque por hackers/crackers;
- b) Filtro de pacotes de aplicações que estejam prejudicando o tráfego da UniNet, ou colocando em risco a segurança das redes da Unicamp;
- c) Filtro de pacotes saindo para a rede ANSP utilizando "proxy transparente" para melhor aproveitamento da banda utilizada.

Artigo 31 – Os Filtros que devem ser aplicados nos roteadores/gateways de conexão da Unidade a UniNet os seguintes:

- a) Filtro de pacotes entrando na Unidade, cujo

## SEÇÃO V

### Do roteamento na UniNet

~~Artigo 27 – São deveres da:~~

~~§ 1º – Não anunciar rotas para as redes reservadas definidas pela RFC 1918;~~

~~§ 2º – Não anunciar rota padrão na UniNet, com exceção do gateway/roteador que interconecta a rede UniNet à rede ANSP;~~

~~§ 3º – Anunciar na UniNet somente rotas para as redes internas da Unidade, previamente alocadas à Unidade;~~

~~Artigo 28 – O roteamento multicast deve ser realizado de forma a não existir túneis na UniNet.~~

~~Artigo 29 – O Roteamento para teste em IPv6 deve ser encapsulado via IPv4, até que normas de implantação, adequação e utilização sejam normatizadas pela CGI.~~

## SEÇÃO V

### Do filtro de pacotes

Artigo 31 – Os filtros que podem ser aplicados nos roteadores responsáveis pela conexão da UniNet a outros sistemas autônomos são os seguintes:

- I – filtro de pacotes objetivando que os recursos computacionais dos Órgãos não sejam utilizados como base de ataque por invasores;
- II – filtro de pacotes para aplicações que estejam prejudicando o tráfego da UniNet, ou colocando em risco a segurança das redes da Unicamp;
- III – filtro de pacotes saindo para outros sistemas autônomos permitindo a utilização da técnica de "proxy transparente" para melhor aproveitamento da banda disponível.

Artigo 32 – Os Filtros que devem ser aplicados nos roteadores/gateways de conexão do Órgão à UniNet são os seguintes:

- I – filtro de pacotes entrando no Órgão, cujo endereço

endereço de origem pertence às redes atribuídas à própria Unidade;

b) Filtro de pacotes entrando na Unidade, cujo endereço destino não pertence às redes atribuídas à Unidade;

c) Filtro de pacotes entrando na Unidade, cujo endereço de destino não são tornados públicos, ou que não se deseja acesso externo;

d) Bloqueio de todas as redes reservadas (RFC 1918);

e) Bloqueio de serviços que podem causar rompimento de segurança (deny of service) em alguma das máquinas internas à Unidade;

f) Filtro de pacotes saindo na Unidade, cujo endereço de origem não pertence às redes atribuídas à própria Unidade;

g) Filtro de qualquer tráfego que a Unidade julgue que não deva sair da rede interna;

h) Filtro de pacotes conforme orientação da CGI ou CCUEC.

## SEÇÃO VII

### Do tráfego na UniNet

Artigo 32 – A banda consumida por determinadas aplicações específicas fica sujeita à limitação, sendo de responsabilidade do Administrador de Rede da Unidade definir juntamente com o CCUEC o percentual de uso da banda total;

Artigo 33 – Será permitida uma única conexão entre um servidor externo e a UniNet quando da necessidade de alimentação de uma base de dados aqui existente, evitando-se assim duplicidade de acesso e minimizando tráfego externo e interno.

Parágrafo único – Caso necessário o servidor interno propagará dos dados para outros servidores internos da Unicamp.

Artigo 34 – Os usuários não podem:

I. Adicionar nenhum equipamento na rede da Unidade sem prévio conhecimento e autorização do

de origem pertence às redes atribuídas ao próprio Órgão;

II – filtro de pacotes entrando no Órgão, cujo endereço destino não pertence às redes atribuídas ;

III – filtro de pacotes entrando no Órgão, cujo endereço de destino não são tornados públicos, ou que não se deseja acesso externo;

IV – bloqueio de todas as redes reservadas (RFC 1918);

V – bloqueio de conexões que possam causar ataques de segurança (como denial of service, por exemplo) em alguma das máquinas internas ao Órgão;

VI – filtro de pacotes saindo do Órgão, cujo endereço de origem não pertence às redes atribuídas ao próprio Órgão;

VII – filtro de qualquer tráfego que o Órgão julgue que não deva sair da rede interna;

VIII – filtro de pacotes conforme orientação da CTIC ou do CCUEC.

## SEÇÃO VI

### Do tráfego na UniNet

Artigo 33 – A banda consumida por aplicações específicas fica sujeita à limitação, sendo de responsabilidade dos Administradores de Sistemas e de Redes do Órgão definir juntamente com o CCUEC o percentual de uso da banda total disponível.

~~Artigo 40 – Será permitida uma única conexão entre um servidor externo e a UniNet quando da necessidade de alimentação de uma base de dados aqui existente, evitando-se assim duplicidade de acesso e minimizando tráfego externo e interno.~~

~~Parágrafo único. Caso necessário o servidor interno propagará dos dados para outros servidores internos da Unicamp.~~

Artigo 34 – É vedado:

I – adicionar qualquer equipamento na rede do Órgão sem autorização prévia, específica ou genérica, dada

Administrador de Rede da Unidade;

II. Adicionar nenhum equipamento de rede a UniNet sem prévio conhecimento e autorização do CCUEC.

Parágrafo único. Os equipamentos referenciados são: Hub, repetidor, switch, roteador, microcomputador, estação de trabalho, modem, placas, impressoras, entre outros.

## SEÇÃO VIII

Do acesso externo aos recursos computacionais da Unicamp por docentes, pesquisadores, alunos, funcionários e usuários

Artigo 35 – As Unidades poderão oferecer o serviço de linhas discadas residenciais para os seus usuários.

Artigo 36 – Para que esse serviço não coloque em risco as redes de outras Unidades e a da própria UniNet, a Unidade deverá atender aos seguintes requisitos:

I. Encaminhar um pedido juntamente com a justificativa à CGI;

II. Possuir um Administrador de Redes e um representante de usuários oficializados perante o CCUEC;

III. Usar servidor de comunicação seguro, com firmware atualizado, com logs que possibilitem o rastreamento e a identificação, garantindo um serviço de autenticação eficiente e seguro;

IV. Responsabilizar-se totalmente pela segurança deste serviço e adotar os critérios recomendados no parecer emitido pelo CCUEC;

V. Utilizar apenas uma máquina para receber todas as chamadas delinhas discadas. Esta máquina não deve conter contas de usuários, mas sim uma base de dados contendo o cadastro dos usuários que tem permissão de acesso ao serviço de linhas discadas. Todas as atividades dos usuários devem ficar registradas em arquivos de log;

VI. Não utilizar esse serviço para prover conexões a empresas conveniadas ou a pessoas físicas estranhas ao quadro funcional da Unicamp;

pelos seus Administradores de Sistemas e de Redes;

II – adicionar **qualquer** equipamento de rede **ao backbone** da UniNet sem prévio conhecimento e autorização do CCUEC;

~~Parágrafo único. Os equipamentos referenciados são: Hub, repetidor, switch, roteador, microcomputador, estação de trabalho, modem, placas, impressoras, entre outros.~~

## ~~SEÇÃO VIII~~

~~Do acesso externo aos recursos computacionais da Unicamp por docentes, pesquisadores, alunos, funcionários e usuários~~

~~Artigo 35 – As Unidades poderão oferecer o serviço de linhas discadas residenciais para os seus usuários.~~

~~Artigo 36 – Para que esse serviço não coloque em risco as redes de outras Unidades e a da própria UniNet, a Unidade deverá atender aos seguintes requisitos:~~

~~I. Encaminhar um pedido juntamente com a justificativa à CGI;~~

~~II. Possuir um Administrador de Redes e um representante de usuários oficializados perante o CCUEC;~~

~~III. Usar servidor de comunicação seguro, com firmware atualizado, com logs que possibilitem o rastreamento e a identificação, garantindo um serviço de autenticação eficiente e seguro;~~

~~IV. Responsabilizar-se totalmente pela segurança deste serviço e adotar os critérios recomendados no parecer emitido pelo CCUEC;~~

~~V. Utilizar apenas uma máquina para receber todas as chamadas delinhas discadas. Esta máquina não deve conter contas de usuários, mas sim uma base de dados contendo o cadastro dos usuários que tem permissão de acesso ao serviço de linhas discadas. Todas as atividades dos usuários devem ficar registradas em arquivos de log;~~

~~VI. Não utilizar esse serviço para prover conexões a empresas conveniadas ou a pessoas físicas estranhas ao quadro funcional da Unicamp;~~

VII. Todas as conexões de login remotos nas máquinas da Unidade oriundas da Internet ou de redes externas à Unidade devem ser aceitas por apenas uma única máquina da Unidade, denominada de servidora de login remoto;

VIII. O usuário deve se autenticar no servidor de login remoto para depois se conectar na máquina de seu interesse interna da Unidade;

IX. O servidor de login remoto não deve possuir contas de usuários e sim uma base de dados contendo o cadastro dos usuários que tem permissão de acesso de login (por exemplo, proxy de login remoto).

## SEÇÃO IX

Das conexões externas à rede da Unicamp

Artigo 37 – As Unidades da Unicamp podem expandir suas redes para localidades geograficamente remotas através de LPCD, rádio, fibra ótica, ou qualquer outro meio.

Artigo 38 – Para garantir a segurança das redes locais das outras Unidades e a da própria UniNet, devem ser atendidos os seguintes requisitos:

I. A rede remota não deve possuir conexões com redes de outras instituições;

II. A rede remota não deve possuir conexões com outros backbones, como ANSP ou provedores locais;

III. Os acessos aos recursos computacionais da Unidade, à Internet e a UniNet, somente serão permitidos desde que autorizados e cadastrados pela própria Unidade;

IV. A Unidade deve utilizar um bloco de endereços reservados (RFC 1918) para esta rede remota, sendo previamente atribuído pelo órgão da Unicamp que é responsável pela distribuição destes endereços. Além disto, a Unidade deve utilizar o esquema NAT

~~VII. Todas as conexões de login remotos nas máquinas da Unidade oriundas da Internet ou de redes externas à Unidade devem ser aceitas por apenas uma única máquina da Unidade, denominada de servidora de login remoto;~~

~~VIII. O usuário deve se autenticar no servidor de login remoto para depois se conectar na máquina de seu interesse interna da Unidade;~~

~~IX. O servidor de login remoto não deve possuir contas de usuários e sim uma base de dados contendo o cadastro dos usuários que tem permissão de acesso de login (por exemplo, proxy de login remoto).~~

## SEÇÃO VII

Das conexões externas à rede da Unicamp

Artigo 35 – Não é permitido prover acesso externo aos recursos computacionais da Unicamp via linhas discadas, exceto nos casos explicitamente autorizados e registrados pela CTIC.

Artigo 36 – Os Órgãos da Unicamp podem expandir suas redes para localidades geograficamente remotas através de LPCD (Linha Privada de Comunicação de Dados), rádio, fibra ótica, ou outro meio de conexão dedicada.

Artigo 37 – Para garantir a segurança das redes locais dos outros Órgãos e a da própria UniNet, devem ser atendidos os seguintes requisitos:

I – a rede remota não deve possuir conexões com redes de outras instituições;

II – a rede remota não deve possuir conexões com outros *backbones*, como ANSP ou provedores locais;

III – os acessos aos recursos computacionais do Órgão, à Internet e à UniNet, somente serão permitidos desde que autorizados e cadastrados pelo próprio Órgão;

~~IV. A Unidade deve utilizar um bloco de endereços reservados (RFC 1918) para esta rede remota, sendo previamente atribuído pelo órgão da Unicamp que é responsável pela distribuição destes endereços. Além disto, a Unidade deve utilizar o esquema NAT~~

(Network Address Translate);

V. Ficam sob responsabilidade da Unidade e de seu Administrador de Redes a implementação física e a segurança desta rede remota, bem como os custos para implantação da mesma em conformidade com as portarias e normas vigentes quanto a recursos computacionais e redes.

Artigo 39 – Havendo convênio entre Unidades da Unicamp e Instituições Públicas, somente será permitida a ligação dessa Instituição a um determinado laboratório ou departamento da Unidade através de rede exclusiva para atender o referido convênio.

§ 1º – Não é permitida a ligação da Instituição conveniada com a rede da Unidade, seja por qualquer meio físico;

§ 2º – Em caso de convênio que necessite comunicação via Internet, fica a cargo da Instituição conveniada conseguir a sua conexão na Internet, via provedor de acesso;

§ 3º – A Unicamp não tem a finalidade de prover pontos de acesso a Instituições Públicas junto a Internet, pois não é provedora de backbone.

Artigo 40 – Havendo convênio entre uma Unidade da Unicamp e uma instituição comercial, é responsabilidade desta última conseguir conexão Internet junto a um provedor de acesso, caso haja necessidade;

Parágrafo único – A Unicamp não tem finalidade de prover pontos de acesso Internet a instituições comerciais, pois não é provedora de backbone.

Artigo 41 – As normas e liberação para conexão e acesso a Internet utilizando-se o backbone da ANSP junto ao PoP-Campinas (ponto de presença operacional) é determinado pela Administração da ANSP / FAPESP.

Parágrafo único – Todas as solicitações de conexão e acesso a Internet utilizando-se o backbone da ANSP

~~(Network Address Translate);~~

~~Parágrafo Único – Ficam sob responsabilidade do Órgão e de seus Administradores de Sistemas e de Redes a implementação física e a segurança da rede remota, bem como os custos para implantação da mesma em conformidade com as portarias e normas vigentes quanto a recursos computacionais e redes.~~

~~Artigo 38 – A Unicamp não provê acesso à Internet a instituições públicas ou privadas, salvo em casos excepcionais e de interesse institucional, devidamente avaliados e aprovados pelo ConTIC.~~

Artigo 39 – Havendo convênio entre **um Órgão** da Unicamp e **uma Instituição Pública**, somente será permitida a ligação dessa Instituição a um determinado laboratório ou departamento **do Órgão** através de rede exclusiva para atender o referido convênio.

§ 1º – Não é permitida a ligação da Instituição conveniada com a rede **do Órgão**.

§ 2º – Em caso de convênio que necessite comunicação via Internet, fica a cargo da Instituição conveniada conseguir a sua conexão **à Internet** via **algum** provedor de acesso.

~~§ 3º – A Unicamp não tem a finalidade de prover pontos de acesso a Instituições Públicas junto a Internet, pois não é provedora de backbone.~~

Artigo 40 – Havendo convênio entre **um Órgão** da Unicamp e uma instituição comercial, é responsabilidade desta última conseguir conexão Internet junto a um provedor de acesso, caso haja necessidade.

~~Parágrafo único – A Unicamp não tem finalidade de prover pontos de acesso Internet a instituições comerciais, pois não é provedora de backbone.~~

~~Artigo 41 – As normas e permissão para conexão e acesso à Internet utilizando o backbone da ANSP junto ao PoP-Campinas (ponto de presença operacional) são determinadas pela Coordenadoria da Rede ANSP / FAPESP.~~

~~Parágrafo único. Todas as solicitações de conexão e acesso à Internet utilizando o backbone da ANSP~~

junto ao PoP-Campinas devem ser encaminhadas à ANPS/FAPESP.

Artigo 42 – A Unicamp é uma das Instituições ligadas à rede ANSP e apenas gerencia o PoP-Campinas.

Parágrafo único – Caso uma Instituição conveniada a Unicamp não se enquadre nas normas da rede ANSP, não poderá se conectar a ela e não poderá utilizar a UniNet como meio para atingir a Internet.

## SEÇÃO IX

Da criação e uso e nomes de domínios em "Unicamp.br"

Artigo 43 – Nomes de domínios são formados por um conjunto de caracteres que mapeia um ou mais endereços de rede IP na internet. Estes nomes também são usados para identificar sítios na Web e direcionar endereços de mensagens eletrônicas além de outras aplicações na Internet.

Artigo 44 – A criação de nomes de domínios em "Unicamp.br" será permitida somente nos seguintes casos:

I. para os Órgãos da Unicamp, ou seja, Institutos, Faculdades, Pró-Reitorias, Centros e Núcleos com o seguinte padrão de nomenclatura: www.[nome\_do\_orgao].Unicamp.br.

II. para eventos, convênios, projetos ou serviços institucionais nos quais a administração da Unicamp esteja envolvida diretamente ou que necessitam de visibilidade em função de seus objetivos com a Unicamp a frente do processo, com o seguinte padrão de nomenclatura: www.[nome\_do\_evento].Unicamp.br.

III. nos demais casos onde o evento, convênio, projeto ou serviço seja planejado e executado pelo Órgão, deve ser criado o nome dentro do domínio do próprio Órgão e este nome pode ser estruturado de duas formas: www.[nome\_do\_evento].[nome\_do\_orgao].Unicamp.br ou www.[nome\_do\_orgao].Unicamp.br/[nome\_do\_evento].

~~junto ao PoP-Campinas devem ser encaminhadas à Coordenadoria da Rede ANSP/FAPESP.~~

~~Artigo 42 – A Unicamp é uma das Instituições ligadas à rede ANSP e apenas gerencia o PoP-Campinas.~~

~~Parágrafo único. Caso uma Instituição conveniada a Unicamp não se enquadre nas normas da rede ANSP, não poderá se conectar a ela e não poderá utilizar a UniNet como meio para atingir a Internet.~~

## SEÇÃO VIII

Da criação e uso de nomes subordinados ao domínio "unicamp.br"

Artigo 41 – Nomes de domínios podem ser utilizados para mapear um ou mais endereços de rede IP, identificar domínios, sítios, serviços, além de outras aplicações.

Artigo 42 – A criação de nomes diretamente subordinados ao domínio "unicamp.br" somente será permitida quando o nome desejado:

I – identificar um Instituto, Faculdade, Reitoria, Pró-Reitoria, Centro, Núcleo ou Hospital;

II – identificar um órgão subordinado diretamente ao GR (Gabinete do Reitor), à CGU (Coordenadoria Geral da Universidade) ou à uma Pró-Reitoria;

III – estiver relacionado a um projeto, evento ou convênio, no qual o GR, a CGU ou uma Pró-Reitoria estejam diretamente envolvidos;

IV – estiver relacionado a um serviço de TIC institucional ou à uma rede de uso geral, que não estejam restritos a um único órgão.



Artigo 45 – Para a criação de domínios de mensagens eletrônicas em "Unicamp.br" fica definida a utilização das mesmas regras expostas no item acima, ou seja: usuário@[nome\_do\_evento].Unicamp.br para eventos, convênios, projetos ou serviços institucionais no qual a administração da Unicamp está envolvida diretamente ou usuário@[nome\_do\_evento].[nome\_do\_orgao].Unicamp.br para os demais casos.

Artigo 82 – Quanto à instalação de servidores Web na rede da Unicamp ou utilização de servidores Web da Unicamp para a hospedagem de páginas de entidades não vinculadas a Unicamp, em alguns casos usando domínio específico e não subordinado ao domínio "Unicamp.br, fica estabelecido que:

I. A autorização para hospedagem de sítios de entidades externas na rede da universidade será avaliada pela CDI – Comissão Diretora de Informática com base no seu interesse institucional. O pedido deverá ser encaminhado a CDI pelo diretor da Unidade que estará hospedando a página, acompanhado de justificativa e relevância institucional desta hospedagem para a universidade.

II. Devem acompanhar a solicitação:

§ 1º – No caso de criação de um domínio, sua delegação será feita para o servidor DNS do Órgão, ficando o servidor DNS principal da Unicamp como servidor secundário para o domínio. Caso o órgão não possua um servidor DNS, será utilizado o servidor DNS principal da Unicamp.

§ 2º – Para nomes outorgados anteriormente à entrada em vigor da presente Resolução e que não se enquadram em qualquer dos Incisos deste Artigo é recomendada sua adequação à presente norma.

Artigo 43 – Nomes subordinados ao domínio "unicamp.br" só podem ser hospedados em máquinas da rede da Unicamp.

~~Artigo 45 – Para a criação de domínios de mensagens eletrônicas em "Unicamp.br" fica definida a utilização das mesmas regras expostas no item acima, ou seja: usuário@[nome\_do\_evento].Unicamp.br para eventos, convênios, projetos ou serviços institucionais no qual a administração da Unicamp está envolvida diretamente ou usuário@[nome\_do\_evento].[nome\_do\_orgao].Unicamp.br para os demais casos.~~

## SEÇÃO IX

Da hospedagem de outros domínios na UniNET

Artigo 44 – Quanto à utilização da UniNET para hospedagem de serviços não subordinados ao domínio "unicamp.br", fica estabelecido que:

I – a Unicamp não poderá constar como titular do domínio no órgão oficial de registro;

II – a autorização para a utilização do nome de domínio será avaliada pelo ConTIC com base no seu interesse institucional, mediante pedido do interessado, que deverá ser encaminhado ao ConTIC pelo diretor do órgão responsável pela solicitação e hospedagem do domínio;

III – devem acompanhar a solicitação os seguintes documentos assinados:



a. Declaração explícita de responsabilidade legal com relação ao conteúdo destes sítios, garantindo a total isenção da universidade quanto a ações legais decorrentes desta hospedagem, de seu conteúdo e eventuais infrações à legislação.

b. Declaração de não utilização para uso comercial.

III. A autorização será sempre concedida por prazo determinado, renovável, podendo ser cancelada a qualquer momento, a critério do diretor da Unidade ou da CDI de modo a preservar o interesse institucional da Unidade/Unicamp e adequação às normas vigentes.

IV. Em todos os casos aplicam-se as seguintes condições:

a) A página inicial deve incluir declaração explícita de que seu conteúdo é de responsabilidade da entidade e não representa necessariamente a posição da instituição hospedeira.

b) Computadores pertencentes a essas entidades e que eventualmente venham a ser instalados/utilizados para hospedagem do sítio devem atender a todas as normas estabelecidas pela Unicamp e o seu gerenciamento feito obrigatoriamente pelo Administrador de Sistemas e Rede em que ela estiver instalada.

c) No caso de domínios não subordinados ao domínio "Unicamp.br" a resolução de endereços deve ser feita no DNS primário da Unicamp.

## CAPÍTULO VI

### Do Correio Eletrônico

Artigo 60 – Os serviços de correio eletrônico são oferecidos como um recurso profissional para apoiar alunos, docentes e funcionários no cumprimento de

a) justificava sobre a relevância institucional desta utilização para a universidade;

b) declaração explícita de responsabilidade legal com relação ao conteúdo de sítios vinculados ao nome de domínio em questão;

c) declaração de não utilização para uso comercial.

IV – a autorização está sujeita a análise técnica;

V – a autorização será sempre concedida por prazo determinado, renovável, podendo ser cancelada a qualquer momento, a critério do diretor do Órgão ou do ConTIC, de modo a preservar o interesse institucional do Órgão (ou da Unicamp) e adequação às normas vigentes;

VI – em todos os casos aplicam-se as seguintes condições:

a) os sítios e os serviços sob o domínio em questão devem apresentar de forma clara o responsável pelo seu conteúdo;

~~b) Computadores pertencentes a essas entidades e que eventualmente venham a ser instalados/utilizados para hospedagem do sítio devem atender a todas as normas estabelecidas pela Unicamp e o seu gerenciamento feito obrigatoriamente pelo Administrador de Sistemas e Rede em que ela estiver instalada.~~

b) o servidor DNS principal da Unicamp deverá figurar entre os servidores de nomes com autoridade sobre o domínio, além de manter uma cópia do mapa que contém os nomes do domínio.

VII – no caso de espelhamento (*mirror*) de informações, não se aplica o disposto na alínea "b" do Inciso III, nem o disposto no Inciso VI.

## CAPÍTULO III

### Do Serviço de Comunicação Eletrônica

Artigo 45 – Os serviços de comunicação eletrônica institucional pertencem à Unicamp e são oferecidos como um recurso profissional para apoiar alunos,

seus objetivos nas áreas de educação, pesquisa, comunicação e serviços.

§ 1º – O uso pessoal é permitido e não priorizado, desde que não provoque efeitos negativos para qualquer outro usuário, não viole o sistema de mensagens, não interfira nas suas atividades ou viole qualquer outra lei ou norma vigente na Unicamp.

§ 2º – Cada usuário é responsável por utilizar os serviços de correio eletrônico de maneira profissional, ética e legal.

§ 3º – Material obtido de forma fraudulenta, racista, profana, obscena, intimidadora, difamatória, ilegal, ofensiva, abusiva ou inapropriada não pode ser enviado via correio eletrônico ou através de qualquer outra forma de comunicação eletrônica.

§ 4º – A Unicamp, de forma geral, não pode e não tem por objetivo, ser o árbitro do conteúdo de mensagens eletrônicas e impedir que os usuários recebam mensagens ofensivas, mas os membros da comunidade universitária são encorajados a utilizar o serviço de correio eletrônico de acordo com a mesma ética aplicada a outras formas de comunicação.

§ 5º – Mensagem encadeada, para fins deste Capítulo, é uma mensagem enviada a um certo número de pessoas pedindo para que cada uma delas retransmita para outras pessoas a mesma mensagem com o mesmo pedido.

Artigo 61 – Todos os usuários que possuem uma conta de correio eletrônico nos servidores da Universidade devem possuir um nome padrão no formato "identificação\_do\_usuario@nome\_do\_servidor.Unicamp.br".

Parágrafo único – O nome do servidor pode ser omitido quando se trata do servidor central da Universidade.

Artigo 63 – Os usuários do correio eletrônico não devem:

I. falsificar sua identidade ou o seu nome de usuário ao utilizar o sistema de mensagens ou alterar a linha de origem da mensagem ou qualquer outra indicação da origem da mensagem;

docentes e funcionários no cumprimento de seus objetivos nas áreas de educação, pesquisa, comunicação e serviços.

~~§ 1º – O uso pessoal é permitido e não priorizado, desde que não provoque efeitos negativos para qualquer outro usuário, não viole o sistema de mensagens, não interfira nas suas atividades ou viole qualquer outra lei ou norma vigente na Unicamp.~~

Parágrafo Único – Cada usuário é responsável por utilizar os serviços de **comunicação eletrônica institucional** de maneira profissional, ética e legal.

~~§ 3º – Material obtido de forma fraudulenta, racista, profana, obscena, intimidadora, difamatória, ilegal, ofensiva, abusiva ou inapropriada não pode ser enviado via correio eletrônico ou através de qualquer outra forma de comunicação eletrônica.~~

~~§ 4º – A Unicamp, de forma geral, não pode e não tem por objetivo, ser o árbitro do conteúdo de mensagens eletrônicas e impedir que os usuários recebam mensagens ofensivas, mas os membros da comunidade universitária são encorajados a utilizar o serviço de correio eletrônico de acordo com a mesma ética aplicada a outras formas de comunicação.~~

~~§ 5º – Mensagem encadeada, para fins deste Capítulo, é uma mensagem enviada a um certo número de pessoas pedindo para que cada uma delas retransmita para outras pessoas a mesma mensagem com o mesmo pedido.~~

Artigo 46 – Todas as contas de correio eletrônico nos servidores **de correio eletrônico** da Universidade devem possuir um nome padrão no formato "**identificação@domínio.unicamp.br**".

Parágrafo Único – O **domínio** deve ser definido de acordo com a Seção VIII do Capítulo II e pode ser omitido quando se tratar do servidor **de correio eletrônico** central da Universidade.

~~Artigo 63 – Os usuários do correio eletrônico não devem:~~

~~I. falsificar sua identidade ou o seu nome de usuário ao utilizar o sistema de mensagens ou alterar a linha de origem da mensagem ou qualquer outra indicação da origem da mensagem;~~

II. iniciar ou reenviar mensagens encadeadas;

III. enviar mensagens não solicitadas, ou que não se referem a assuntos universitários, a pessoas com as quais não tenham relacionamentos pessoais.

Artigo 62 – Os usuários de mensagens eletrônicas não devem dar a impressão que estão representando, dando opiniões ou fazendo declarações em nome da Unicamp ou qualquer outro Órgão da Unicamp a menos que autorizado, implícita ou explicitamente.

Parágrafo único – As mensagens eletrônicas devem conter uma declaração explícita, informando que o autor do texto, declaração, ou opinião não está representando a Unicamp, a menos que este dado já esteja claro a partir do contexto.

Artigo 64 – Listas de discussão são criadas sob demanda sem a necessidade de consultar os usuários inseridos nas mesmas.

Parágrafo único – É facultada ao usuário a opção de se descadastrar posteriormente da lista de discussão.

Artigo 65 – Todo servidor deve ter um sistema de anti-vírus que deve ser mantido atualizado pelo administrador do servidor.

Artigo 66 – As mensagens transferidas para arquivos em computadores de uso pessoal ou para sistemas de mensagens, externos a Unicamp, são cobertas por outras políticas e procedimentos.

Artigo 67 – A inconveniência e possível ameaça contida em mensagens indesejáveis, provenientes de fontes comerciais ou não, pode levar o Administrador de Sistemas e Rede a bloquear a recepção de mensagens provenientes de alguns locais da rede.

Parágrafo único – Não é permitido o uso do conteúdo da mensagem ou da sua linha referente ao "assunto" para bloquear ou redirecionar a entrega de qualquer mensagem, exceto no caso de mensagens encadeadas, ameaça de vírus ou outro conteúdo igualmente destrutivo.

Artigo 68 – As mensagens endereçadas para uma conta são entregues numa caixa de correio que podem

~~II. iniciar ou reenviar mensagens encadeadas;~~

~~III. enviar mensagens não solicitadas, ou que não se referem a assuntos universitários, a pessoas com as quais não tenham relacionamentos pessoais.~~

Artigo 47 – Os usuários de **comunicações eletrônicas** não devem dar a impressão que estão representando, dando opiniões ou fazendo declarações em nome da Unicamp ou **de qualquer Órgão** da Unicamp a menos que autorizado, implícita ou explicitamente.

~~Parágrafo único. As mensagens eletrônicas devem conter uma declaração explícita, informando que o autor do texto, declaração, ou opinião não está representando a Unicamp, a menos que este dado já esteja claro a partir do contexto.~~

Artigo 48 – Listas de discussão **podem ser** criadas sob demanda sem a necessidade de consultar os usuários inseridos nas mesmas.

Parágrafo Único – **Deve ser** facultada ao usuário a opção de se descadastrar **a qualquer momento de uma** lista de discussão.

Artigo 49 – **Todo servidor de comunicações eletrônicas** deve usar os mecanismos disponíveis e atualizados anti-vírus, anti-spam e de controle de encaminhamento (relay) de comunicações eletrônicas.

~~Artigo 58 – As mensagens transferidas para arquivos em computadores de uso pessoal ou para sistemas de mensagens, externos a Unicamp, são cobertas por outras políticas e procedimentos.~~

~~Artigo 67 – A inconveniência e possível ameaça contida em mensagens indesejáveis, provenientes de fontes comerciais ou não, pode levar o Administrador de Sistemas e Rede a bloquear a recepção de mensagens provenientes de alguns locais da rede.~~

~~Parágrafo único – Não é permitido o uso do conteúdo da mensagem ou da sua linha referente ao "assunto" para bloquear ou redirecionar a entrega de qualquer mensagem, exceto no caso de mensagens encadeadas, ameaça de vírus ou outro conteúdo igualmente destrutivo.~~

Artigo 50 – As **comunicações eletrônicas** endereçadas para uma conta são entregues **num repositório** que

ser acessadas através de diversos programas sob o controle da senha da conta correspondente.

Artigo 69 – Os serviços de correio eletrônico podem ser utilizados episodicamente para propósitos pessoais desde que, além do que está exposto neste Capítulo, tal uso:

- a) Não interfira direta ou indiretamente nas operações dos recursos computacionais e serviços de correio eletrônico da Unicamp;
- b) Não incorra em gastos adicionais para a Unicamp;
- c) Não interfira nas obrigações internas e externas da Unicamp;
- d) Não interfira na produtividade das atividades funcionais da Unicamp.
- e) Não tenha propósitos comerciais, exceto a serviço autorizado ou institucional.

## CAPÍTULO IX

Do Conteúdo em Mensagens Eletrônicas de Caráter Institucional

pode ser acessado através de diversos programas sob o controle da senha da conta correspondente.

Artigo 51 – Os serviços de **comunicação eletrônica institucional** podem ser utilizados episodicamente para propósitos pessoais, desde que **tal utilização**:

- I – não interfira direta ou indiretamente nas operações dos recursos computacionais e serviços de comunicação eletrônica da Unicamp;**
- II – não incorra em gastos adicionais para a Unicamp;**
- III – não interfira nas obrigações internas e externas da Unicamp;**
- IV – não interfira na produtividade das atividades funcionais da Unicamp.**
- V – não tenha propósitos comerciais, exceto a serviço autorizado ou institucional.**

**Parágrafo Único – Aquele que utilize os serviços de comunicação eletrônica institucional para fins pessoais, deverá fazê-lo ciente da obrigatoriedade de cumprimento das normas da Universidade e da possibilidade de acesso ao conteúdo das comunicações eletrônicas, nos termos do disposto nesta Resolução.**

**Artigo 52 – Após o encerramento de vínculo do usuário, suas contas nos sistemas de comunicação eletrônica devem ser encerradas no prazo máximo de 120 dias, salvo nos casos de servidores aposentados que optem por ingressar em algum programa de atividades junto a Unicamp que mantenha seu vínculo, como os Programas de Professor Colaborador e Pesquisador Colaborador, por exemplo.**

**Parágrafo Único – Em se tratando de conclusão de curso para alunos e aposentadoria para servidores, é permitido o uso de novas contas de comunicação eletrônica com domínio próprio na Unicamp para estes tipos de usuários.**

## CAPÍTULO IV

Do Conteúdo em **Comunicações Eletrônicas** de Caráter Institucional

Artigo 53 – Considerando o bom uso da infra-

Artigo 83 – Considerando o bom uso da infraestrutura computacional da Universidade e a acessibilidade às informações veiculadas em mensagens eletrônicas de caráter institucional, ficam estabelecidas as seguintes normas:

a) O conteúdo principal deve ser veiculado no corpo da mensagem eletrônica e não na forma de um anexo.

b) Em se tratando de um texto mais longo ou outro tipo de conteúdo, como uma planilha eletrônica, este conteúdo pode vir anexado à mensagem eletrônica e necessariamente no formato "Portable Document Format" (PDF), contanto que o corpo da mensagem contenha uma breve descrição de cada anexo.

c) Se um arquivo a ser veiculado for grande, então ele deve ser publicado na Web e o corpo da mensagem deve conter o localizador (URL) de tal arquivo com um breve comentário do assunto tratado.

d) Cabe ao remetente a responsabilidade de escolher a forma de envio que seja a menos onerosa para a infraestrutura computacional da Universidade.

#### CAPÍTULO IV

##### Da Privacidade de Mensagens Eletrônicas e Arquivos de Computador

Artigo 53 – Na Unicamp, mensagens eletrônicas e arquivos de computador são considerados de uso privativo e confidencial na forma permitida em lei.

Artigo 54 – As mensagens eletrônicas ou arquivos de computador somente serão acessados com a permissão do remetente ou destinatário da mensagem ou do dono do arquivo, salvo por ordem judicial.

estrutura computacional da Universidade e a acessibilidade às informações veiculadas em **comunicações eletrônicas** de caráter institucional, ficam estabelecidas as seguintes normas:

**I** – o conteúdo principal deve ser veiculado **preferencialmente** no corpo da **comunicação eletrônica** e não na forma de um anexo;

**II** – em se tratando de um texto mais longo ou outro tipo de conteúdo, como uma planilha eletrônica, **que requeira a anexação de um arquivo à comunicação eletrônica, deverá ser adotado preferencialmente para o arquivo um formato aberto como o PDF (Portable Document Format) ou o ODF (Open Document Format), e o corpo da comunicação deverá conter uma breve descrição de cada anexo;**

**III** – se um arquivo a ser veiculado for grande, então ele deve ser publicado na Web e o corpo da **comunicação eletrônica** deve conter o localizador (URL) de tal arquivo com um breve comentário do assunto tratado;

**IV** – cabe ao remetente a responsabilidade de escolher a forma de envio que seja a menos onerosa para a infra-estrutura computacional da Universidade;

**V** – cabe aos Administradores de Sistemas e de Redes implantar mecanismos de limitação de tamanho máximo de comunicações eletrônicas.

#### CAPÍTULO V

##### Da Privacidade de **Comunicações** Eletrônicas e Arquivos de Computador

Artigo 54 – Na Unicamp, **os conteúdos de todos os tipos de comunicações eletrônicas e de arquivos de computador são considerados privativos e confidenciais.**

Artigo 55 – **Os conteúdos de comunicações eletrônicas ou arquivos de computador somente serão acessados com a permissão do remetente ou destinatário da comunicação ou do dono do arquivo, salvo nos casos em que o acesso for determinado em razão de interesse público, por ordem judicial ou por suspeita da prática de irregularidade, crime ou afronta à ordem pública.**

**§ 1º – O acesso ao conteúdo de comunicações**

§ 1º – Havendo uma investigação feita pela Unicamp, por força de acusações de má conduta de algum usuário, mensagens e arquivos podem ser bloqueados ou copiados pelos Administradores de Sistemas e Rede ou pela Equipe de Segurança de Recursos Computacionais para impedir a destruição ou perda de informações.

§ 2º – Compete a Equipe de Segurança de Recursos Computacionais da Unicamp analisar os conteúdos das cópias de segurança e emitir parecer técnico, caso seja obtida uma autorização legal para tal.

§ 3º – Cabe a Equipe de Segurança de Recursos Computacionais da Unicamp rastrear o trajeto de mensagens eletrônicas consideradas ofensivas ou abusivas pela instituição, a fim de determinar o ponto de origem da qual foi enviada.

eletrônicas e arquivos de computador em razão de interesse público ou por suspeita da prática de irregularidade, crime ou afronta à ordem pública somente poderá ocorrer mediante a justificativa formalizada (por escrito), devidamente fundamentada e submetida à prévia autorização da autoridade máxima da Universidade, que determinará as condições em que o acesso poderá ocorrer.

§ 2º – Entende-se por acesso ao conteúdo o ato de se tomar conhecimento do conteúdo de comunicações eletrônicas (excluídos os cabeçalhos usados para fins de controle de transmissão e recepção) ou arquivos, não sendo portanto consideradas acesso ao conteúdo as atividades administrativas automatizadas de cópia (*backup* e restauração), bem como aquelas de análise automatizada de conteúdo para detecção de conteúdo indesejado como vírus e spam, por exemplo.

Artigo 56 – Nos casos de interesse público ou de suspeita da prática de irregularidade, crime, afronta à ordem pública, mediante justificativa devidamente fundamentada, os Administradores de Sistemas e de Redes e o CCUEC poderão:

I – bloquear ou copiar as comunicações eletrônicas e arquivos, para impedir a destruição ou perda de informações;

~~§ 2º – Compete a Equipe de Segurança de Recursos Computacionais da Unicamp analisar os conteúdos das cópias de segurança e emitir parecer técnico, caso seja obtida uma autorização legal para tal.~~

II – rastrear o trajeto das comunicações eletrônicas, a fim de determinar o ponto de origem das mesmas.

III – bloquear a recepção de comunicações eletrônicas provenientes de alguns locais da rede.

Parágrafo Único – As condutas descritas nos Incisos I a III não implicam na autorização de acesso ao conteúdo das comunicações eletrônicas e arquivos, que somente poderá ocorrer nos termos do Artigo 55 desta Resolução.

~~§ 4º – Os pedidos de rastreamento devem ser~~



§ 4º – Os pedidos de rastreamento devem ser encaminhados à CGI pelo responsável legal do Órgão da Unicamp ao qual se encontra vinculado o destinatário da mensagem ofensiva ou abusiva.

## CAPÍTULO VII

### Da Segurança de Senhas

Artigo 71 – Para fins deste Capítulo considera-se:

I. Administrador de Sistemas e Rede: responsável pela segurança e integridade dos dados e serviços disponíveis no ambiente computacional sob seu controle e responsável por manter o sigilo das senhas de acesso a esse ambiente.

Artigo 70 – O gerenciamento de senhas constitui o mecanismo básico para a autenticação de usuários dos sistemas computacionais da Unicamp.

Parágrafo Único – Senhas são confidenciais, intransferíveis e é responsabilidade do usuário mantê-la como tal, observando mecanismos de segurança e integridade.

Artigo 72 – Novas senhas serão fornecidas e senhas já existentes serão liberadas apenas quando a identidade do requisitante estiver univocamente assegurada.

§ 1º – Senhas são atribuídas a cada indivíduo como um mecanismo para controlar e monitorar seu acesso a sistemas e informações e não devem ser compartilhadas com outras pessoas.

§ 2º – Usuários serão responsabilizados pelas ações de outros se, desrespeitando o item anterior, deliberadamente, compartilharem sua senha e acesso.

§ 3º – Senhas devem ser trocadas periodicamente, num prazo não superior a seis (6) meses.

§ 4º – Senhas devem conter no mínimo cinco caracteres.

§ 5º – Usuários devem trocar suas senhas imediatamente após suspeitarem que foram violadas.

II. Senha temporária: senha gerada inicialmente pelo

~~encaminhados à CGI pelo responsável legal do Órgão da Unicamp ao qual se encontra vinculado o destinatário da mensagem ofensiva ou abusiva.~~

## CAPÍTULO VI

### Do Uso e Gestão de Senhas

~~Artigo 71 – Para fins deste Capítulo considera-se:~~

Artigo 57 – Os Administradores de Sistemas e de Redes são responsáveis pela segurança e integridade dos dados e serviços disponíveis no ambiente computacional sob seu controle e responsáveis por manter o sigilo das senhas de acesso a esse ambiente.

Artigo 58 – O gerenciamento de senhas constitui o mecanismo básico para a autenticação de usuários dos sistemas computacionais da Unicamp, podendo haver a adoção de outros tão ou mais seguros que este.

Artigo 59 – Senhas são confidenciais, intransferíveis e é responsabilidade do usuário mantê-la como tal, observando mecanismos de segurança e integridade.

Artigo 60 – Novas senhas serão fornecidas e senhas já existentes serão liberadas apenas quando a identidade do requisitante estiver assegurada.

§ 1º – Senhas são atribuídas a cada indivíduo como um mecanismo para controlar e monitorar seu acesso a sistemas e informações e não podem ser compartilhadas com outras pessoas.

§ 2º – O usuário será responsabilizado pelas ações de outros se, desrespeitando o item anterior, deliberadamente, compartilhar sua senha e/ou acesso.

§ 3º – Senhas devem ser trocadas periodicamente, em prazo a ser definido em Instrução Normativa específica.

§ 4º – Senhas devem conter no mínimo oito caracteres escolhidos entre dígitos, letras e símbolos especiais.

§ 5º – Usuários devem trocar suas senhas imediatamente após suspeitarem que foram violadas.

§ 6º – Senha temporária é uma senha gerada pelos Administradores de Sistemas e de Redes para um



Administrador de Sistemas e Rede para um usuário. Até esta senha seja utilizada pelo usuário na primeira autenticação, ela é considerada como temporária.

§ 6º – Senhas temporárias podem ser entregues ao titular, ou a outrem por procuração registrada em cartório.

§ 7º – Em caso de esquecimento da senha, uma senha temporária pode ser fornecida via rede após o solicitante fornecer informações de caráter pessoal e não públicas.

§ 8º – A troca de senha temporária é obrigatória na primeira autenticação.

§ 9º – Cabe ao Administrador de Sistemas e Rede adotar procedimentos de administração de senhas específicos para o seu ambiente computacional, observando os critérios gerais acima.

### CAPÍTULO III

#### Da Gestão de Software Proprietário

Artigo 46 – O Programa de Computador ou Software é propriedade intelectual, protegida pela Lei n.º 9.609, de 19 de fevereiro de 1998, que dispõe sobre a proteção da propriedade intelectual de programa de computador, e pela Lei n.º 9.610, de 19 de fevereiro de 1998, que trata dos direitos autorais.

Artigo 47 – A política de uso de software proprietário na Unicamp estabelece, fundamentada na Lei de Direitos Autorais e na Lei de Software, que nenhum membro de sua comunidade se envolva em qualquer atividade que viole leis federais, estaduais ou locais relacionadas a direitos de propriedade intelectual referentes a licenças de software ou qualquer outra política relacionada a software de computador ou conteúdos em formato digital.

Artigo 48 – Copiar software para distribuição para outros ou usar uma versão mono-usuário em diversos

usuário e que só é válida até o primeiro acesso autenticado bem sucedido do respectivo usuário.

§ 7º – Senhas temporárias podem ser entregues ao titular, ao Representante de Usuários do Órgão ou a outrem por procuração registrada em cartório.

§ 8º – Em caso de esquecimento da senha, uma senha temporária pode ser fornecida via rede após o solicitante fornecer informações de caráter pessoal e não públicas que permitam sua autenticação.

§ 9º – A troca de senha temporária é obrigatória na primeira autenticação bem sucedida.

§ 10º – Cabe aos Administradores de Sistemas e de Redes adotar procedimentos de administração de senhas específicos para o seu ambiente computacional, observando estas normas.

### CAPÍTULO VII

#### Da Gestão de Software Proprietário

Artigo 61 – O Programa de Computador ou Software é propriedade intelectual, protegida pela Lei n.º 9.609, de 19 de fevereiro de 1998, que dispõe sobre a proteção da propriedade intelectual de programa de computador, e pela Lei n.º 9.610, de 19 de fevereiro de 1998, que trata dos direitos autorais.

Parágrafo Único – O software produzido no âmbito da UNICAMP por qualquer dos integrantes de sua comunidade é regido pela Deliberação CONSU-A-016/2010, de 30/11/2010, que estabelece a Política Institucional de Propriedade Intelectual da Universidade Estadual de Campinas.

Artigo 62 – A política de uso de software proprietário na Unicamp, fundamentada na Lei de Direitos Autorais e na Lei de Software, estabelece que nenhum membro de sua comunidade se envolva em qualquer atividade que viole leis federais, estaduais ou locais relacionadas a direitos de propriedade intelectual referentes a licenças de software ou qualquer outra política relacionada a software de computador ou conteúdos em formato digital.

Artigo 63 – Copiar software proprietário para distribuição para outros ou usar uma versão mono-usuário em diversos computadores em rede, caso tal

computadores em rede, caso tal hipótese não seja contemplada na sua licença, é ilegal e viola as leis de software e de direitos autorais.

Artigo 49 – Fica estabelecido que para qualquer software de propriedade ou licenciado pela Unicamp e hardware ou sistemas computacionais de propriedade ou operados pela Unicamp, os seus usuários, sejam eles docentes, funcionários ou alunos:

I. devem concordar com todos os termos do acordo de licença de software;

II. devem estar cientes que todos os softwares são protegidos por direitos autorais, a menos que explicitamente rotulados de Domínio Público;

III. Não podem copiar software para qualquer propósito com exceção daqueles permitidos no acordo de licença;

IV. Não podem tornar o software disponível para outras pessoas usarem ou copiarem, se tal procedimento estiver em desacordo com os termos da licença de software e/ou procedimentos adotados pela Unicamp;

V. Não podem aceitar software não licenciado de terceiros;

VI. Não podem instalar, nem permitir ou induzir outros a instalarem, cópias ilegais de software, ou software sem as devidas licenças, em qualquer recurso computacional de propriedade ou operado pela Unicamp.

Artigo 50 – Toda aquisição de equipamento computacional deve incluir necessariamente a aquisição de licenças do software básico mínimo apropriado para o seu uso final.

Artigo 51 – Toda licença de software, de qualquer natureza, adquirida pela Unicamp deve ser obrigatoriamente registrada, assim como também às licenças de software incluídas na aquisição do equipamento.

Artigo 52 – A instalação de software nos equipamentos computacionais da Unicamp somente é autorizada mediante as formalizações de registro e arquivamento da licença de uso, em sistema

hipótese não seja contemplada na sua licença, é ilegal e viola as leis de software e de direitos autorais.

Artigo 64 – Para todo software de propriedade da Unicamp, ou por ela licenciado, e para todo hardware ou sistema computacional de propriedade ou operado pela Unicamp, fica estabelecido que seus usuários:

I – devem concordar com todos os termos do acordo de licença de software;

II – devem estar cientes que os softwares são protegidos por direitos autorais e por licenças de uso e cessão que devem ser observados, mesmo naqueles rotulados como Domínio Público;

III – não podem copiar software para qualquer propósito com exceção daqueles cuja cópia é permitida no acordo de licença;

IV – não podem tornar o software disponível para outras pessoas usarem ou copiarem, se tal procedimento estiver em desacordo com os termos da licença de software e/ou procedimentos adotados pela Unicamp;

V – não podem aceitar software não licenciado de terceiros;

VI – não podem instalar, permitir que instalem ou induzir outros a instalarem cópias ilegais de software ou software sem as devidas licenças, em qualquer recurso computacional de propriedade da, ou operado pela, Unicamp.

Artigo 65 – Toda aquisição de equipamento computacional deve contemplar necessariamente a obtenção de licenças do software básico mínimo apropriado para o seu uso final.

Artigo 66 – Toda licença de software, de qualquer natureza, adquirida pela Unicamp deve ser obrigatoriamente registrada, assim como também às licenças de software incluídas na aquisição do equipamento.

Artigo 67 – A instalação de software nos equipamentos computacionais da Unicamp só pode ser realizada mediante as formalizações de registro e arquivamento da licença de uso no Órgão responsável pelo equipamento, excluídos os softwares de domínio

centralizado no Órgão responsável pelo equipamento, excluídos os softwares abertos ou de uso gratuito.

Parágrafo Único – As disposições deste artigo se aplicam também aos equipamentos e licenças de software doados ou adquiridos por convênios ou projetos de pesquisa vinculados à Unicamp.

## CAPÍTULO V

### Da Gestão de Dados Corporativos

Artigo 55 – Este Capítulo aplica-se a:

I. Todos os dados em todos os formatos que dão suporte às necessidades administrativas, acadêmicas e operacionais da Universidade.

II. Todos os softwares, aplicações e sistemas operacionais utilizados para o gerenciamento destes dados.

III. Atividades de processamento de dados relacionadas a atividades de pesquisa.

Artigo 56 – Considera-se:

I. Dado: Informação sobre fatos, incluindo medidas, declarações e estatísticas.

II. Acesso: permissão, privilégio ou capacidade de ler, registrar, atualizar, gerenciar ou administrar a consulta e/ou a manipulação do acervo de dados e informações da Unicamp. O acesso é autorizado pelo Responsável pela Custódia do Dado e é dependente do dado em questão e da função exercida pelo solicitante.

III. Dado de uso corporativo ou institucional: todos os dados capturados e utilizados nas operações de serviço e administrativas da Unicamp são considerados dados corporativos. Embora os dados corporativos residam em diferentes sistemas de gerenciamento de dados, incluindo planilhas, e estejam em diferentes locais físicos, eles constituem um único banco de dados corporativo.

Dados corporativos incluem, mas não estão restritos a:

a) dados de recursos humanos;

público e os que não possuam ou dispensam tal licença.

Parágrafo Único – As disposições deste Artigo se aplicam também aos equipamentos e licenças de software doados ou adquiridos por convênios ou projetos de pesquisa vinculados à Unicamp.

## CAPÍTULO VIII

### Da Gestão de Dados Corporativos

Artigo 68 – Este Capítulo aplica-se a:

I – todos os dados em todos os formatos que dão suporte às necessidades administrativas, acadêmicas e operacionais da Universidade;

II – todos os softwares, aplicações e sistemas operacionais utilizados para o gerenciamento destes dados;

III – atividades de processamento de dados relacionadas a atividades de pesquisa.

Artigo 69 – Considera-se:

I – Dado: informação sobre fatos, incluindo medidas, declarações e estatísticas.

II – Acesso: permissão, privilégio ou capacidade de ler, registrar, atualizar, gerenciar ou administrar a consulta e/ou a manipulação do acervo de dados e informações da Unicamp. O acesso é autorizado pelo Responsável pela Custódia do Dado e é dependente do dado em questão e da função exercida pelo solicitante.

III – Dados Corporativos: dados de uso corporativo ou institucional capturados e utilizados nas operações de serviço e administrativas da Unicamp, que residam em diferentes sistemas de gerenciamento de dados, incluindo planilhas, e estejam em diferentes locais físicos, constituindo um único banco de dados corporativo.

IV – Dados Corporativos incluem, mas não estão restritos a:

a) dados de recursos humanos;

b) dados financeiros;

- b) dados financeiros;
- c) dados de equipamentos de qualquer natureza;
- d) dados de alunos;
- e) dados de cursos, disciplinas, entre outros;
- f) políticas, procedimentos e manuais;
- g) páginas Web.

IV. Agente: qualquer pessoa ou conjunto de pessoas autorizadas pela Unicamp para o acesso e/ou tratamento dos dados corporativos: docentes, funcionários, alunos e terceirizados.

X. Usuário de dados: agente autorizado a ler, registrar, e/ou atualizar dados, com as seguintes responsabilidades:

- a) acessar os dados conforme a autorização dada pelo Responsável pela Custódia do Dado;
- b) garantir que os mecanismos de proteção física dos dados estão instalados e operando de forma satisfatória;
- c) não poder divulgar dados sem a permissão dos responsáveis pela custódia destes dados.

V. Informação: dados estruturados.

VI. Fonte primária de dado:

- a) Existe uma única fonte primária para cada item de dado que é identificada pelo Responsável pela Custódia do Dado.
- b) Esta fonte primária é o registro oficial da Unicamp para este item de dado.

VII. Fonte secundária de dado:

- a) Existem circunstâncias onde fontes secundárias ou alternativas existem para um item de dado.
- b) Elas podem estar em um banco de dados separado ou numa cópia da fonte primária.
- c) Fontes secundárias podem ser utilizadas, ao invés da fonte primária, apenas em situações aprovadas pelo Responsável pela Custódia do Dado.

VIII. Responsável pela custódia do dado: agente da Unicamp a quem foi delegado a responsabilidade por uma parte dos dados em nome da Unicamp, com o objetivo de

garantir a sua integridade e precisão, com as seguintes responsabilidades:

- c) dados de equipamentos de qualquer natureza;
- d) dados de alunos;
- e) dados de cursos, disciplinas, turmas, matrículas;
- f) políticas, procedimentos e manuais.
- ~~g) páginas Web.~~

V – Agente: qualquer pessoa ou conjunto de pessoas autorizadas pela Unicamp para o acesso e/ou tratamento dos dados corporativos com as seguintes responsabilidades:

~~X. Usuário de dados: agente autorizado a ler, registrar, e/ou atualizar dados, com as seguintes responsabilidades:~~

a) acessar os dados conforme a autorização dada pelo Responsável pela Custódia dos Dados;

~~b) garantir que os mecanismos de proteção física dos dados estão instalados e operando de forma satisfatória;~~

~~b) não divulgar dados sem a permissão do responsável pela custódia dos mesmos.~~

VI – Informação: conjunto de dados estruturados.

VII – Fonte Primária de Dados: fonte principal oficial para Dados Corporativos, a qual é definida pelo Responsável pela Custódia dos Dados.

VIII. Fonte Secundária de Dados: fonte alternativa oficial para Dados Corporativos, a qual é definida e tem seu uso autorizado pelo Responsável pela Custódia dos Dados.

IX – Responsável pela Custódia dos Dados: Agente a quem são delegadas as seguintes responsabilidades sobre um determinado conjunto de Dados Corporativos:

a) buscar garantir a integridade, consistência e precisão de sua parte dos Dados Corporativos;

b) definir a Fonte Primária de Dados e as Fontes

- a) identificar os itens de dados corporativos e a sua fonte primária;
- b) identificar e documentar a quem é permitido o acesso ao dado e o nível de acesso;
- c) autorizar acesso aos dados;
- d) especificar os requisitos de segurança de acesso;
- e) estabelecer procedimentos para a obtenção de autorização para acesso aos dados;
- f) implementar processos que mantenham a integridade, precisão, temporalidade, consistência, padronização e o valor do dado;
- g) garantir através de procedimentos que o dado seja captado e utilizado de forma adequada;
- h) monitorar as atividades de acesso aos dados e notificar as tentativas ou violações de acesso a Equipe de Segurança de Recursos Computacionais da Unicamp.

IX. Responsável pelo Gerenciamento dos Dados: agente da Unicamp que fornece serviços de processamento de dados como suporte aos usuários dos dados com as seguintes responsabilidades:

- a) implementar a segurança de acesso aos dados como especificado pelo Responsável pela Custódia do Dado, assim como de acordo com os padrões e orientação de acesso aos dados;
- b) prover acesso aos dados pelos usuários como especificado pelo Responsável pela Custódia do Dado;
- c) garantir que os mecanismos de proteção física dos dados estão instalados e operando de forma satisfatória;
- d) monitorar a efetividade dos controles implantados contra tentativas de acesso não autorizado;
- e) acessar os dados, da forma autorizada pelo Responsável pela Custódia do Dado, para a execução das tarefas necessárias para garantir a disponibilidade e acessibilidade;
- f) garantir que todos os dados possuem um

Secundárias de Dados, se houver;

- c) identificar e documentar os Agentes aos quais é permitido o acesso aos dados e o nível deste acesso;
- d) autorizar o acesso aos dados;
- e) especificar os requisitos de segurança de acesso;
- f) estabelecer procedimentos para a obtenção de autorização de acesso aos dados;
- g) implementar processos que mantenham a integridade, precisão, temporalidade, consistência, padronização e o valor do dado;
- h) garantir através de procedimentos que o dado seja captado e utilizado de forma adequada;
- i) monitorar as atividades de acesso aos dados e notificar as tentativas ou violações de acesso ao CCUEC.

X – Responsável pelo Gerenciamento dos Dados: Agente que fornece serviços de processamento de dados e suporte aos usuários dos dados com as seguintes responsabilidades:

- a) implementar a segurança de acesso aos dados como especificado pelo Responsável pela Custódia dos Dados;
- b) prover acesso aos dados pelos usuários como especificado pelo Responsável pela Custódia dos Dados;
- c) garantir que os mecanismos de proteção física e lógica dos dados estão instalados e operando de forma satisfatória;
- d) monitorar a efetividade dos controles implantados contra tentativas de acesso não autorizado;
- e) acessar os dados, da forma autorizada pelo Responsável pela Custódia dos Dados, para a execução das tarefas necessárias para garantir a disponibilidade dos mesmos;
- f) garantir que todos os dados possuam um responsável pela sua custódia;



responsável pela sua custódia;

g) prover e dar suporte aos sistemas e aplicações necessárias para atender às especificações dos Responsáveis pela Custódia do Dado para a manutenção e disseminação dos dados;

h) proteger os dados contra destruição, modificações ou acessos durante as transferências eletrônicas ou físicas de um local para outro;

i) documentar e promover o valor do dado para os objetivos da Unicamp e facilitar o compartilhamento e a integração dos dados;

j) gerenciar o uso de padrões comuns de definição de dados em toda a Unicamp.

XI. Dono do dado: a Unicamp é proprietária de todos os seus dados corporativos e detém os direitos autorais de todas as políticas, manuais e compilações destes dados.

XII. Comissão Diretora de Informática – CDI: órgão deliberativo da Reitoria, que estabelece políticas e programas na área de informática de acordo com propostas encaminhadas pela Coordenadoria Geral de Informática – CGI, que tem como competência:

a) rever, recomendar e aprovar políticas e procedimentos relacionadas ao uso e acesso a informações corporativas;

b) resolver conflitos e disputas que ocorram em função da implementação ou administração desta política.

Artigo 57 – É política da Unicamp manter os dados corporativos integrados e íntegros através de todos os seus Órgãos, permitindo que os seus administradores acessem as informações que necessitam, dentro de um ambiente controlado.

Artigo 58 – Os novos sistemas desenvolvidos ou adquiridos de terceiros devem se integrar com os sistemas corporativos existentes, atendendo requisitos técnicos para esta integração.

Parágrafo único – A Unicamp delegará funções e responsabilidades para o gerenciamento dos seus dados corporativos.

Artigo 59 – Funcionários, terceirizados, alunos,

g) **prover suporte** aos sistemas e aplicações necessárias para atender às especificações dos Responsáveis pela Custódia dos Dados para a manutenção, **acesso e segurança** dos dados;

h) proteger os dados contra destruição, modificações ou acessos **indevidos** durante as transferências eletrônicas ou físicas de um local para outro;

~~i) documentar e promover o valor do dado para os objetivos da Unicamp e facilitar o compartilhamento e a integração dos dados;~~

j) **promover** o uso de padrões comuns de definição e **gerenciamento** de dados em toda a Unicamp.

~~XI – Dono dos Dados: a Unicamp é proprietária de todos os seus dados corporativos e detém os direitos autorais de todas as políticas, manuais e compilações destes dados.~~

~~XII. Comissão Diretora de Informática – CDI: órgão deliberativo da Reitoria, que estabelece políticas e programas na área de informática de acordo com propostas encaminhadas pela Coordenadoria Geral de Informática – CGI, que tem como competência:~~

**Artigo 70 – Cabe ao ConTIC** rever, recomendar e aprovar políticas e procedimentos relacionadas ao uso e acesso a **Dados Corporativos, bem como** resolver conflitos e disputas que ocorram em função da implementação ou administração **destas políticas e procedimentos.**

**Artigo 71 – É política da Unicamp** manter **seus Dados Corporativos** integrados e íntegros através de todos os seus Órgãos, **buscando permitir** que os **Agentes** acessem as informações que necessitam dentro de um ambiente controlado.

**Artigo 72 – Os novos sistemas desenvolvidos ou adquiridos de terceiros** devem se integrar com os **sistemas corporativos existentes.**

~~Parágrafo único. A Unicamp delegará funções e responsabilidades para o gerenciamento dos seus dados corporativos.~~

~~Artigo 85 – Funcionários, terceirizados, alunos, docentes ou outros agentes que geram dados ou são~~

docentes ou outros agentes que geram dados ou são usuários de dados e que, intencionalmente e sem autorização, acessem ou publiquem, modifiquem ou destruam dados e informações corporativas estão violando diretamente esta Norma.

## CAPÍTULO VIII

### Do Uso da Tecnologia Web

Artigo 73 – A Unicamp reconhece o escopo e a importância da tecnologia Web na disseminação das informações internas e externas e está comprometida com o desenvolvimento e com o suporte ao conteúdo de qualidade através dos servidores Web.

Artigo 74 – A Unicamp reconhece a importância e a utilidade de publicações eletrônicas através da Internet, principalmente as páginas pessoais, que podem prover informações relevantes sobre o papel de cada indivíduo dentro da Universidade.

§ 1º – Considerando que as páginas pessoais são documentos públicos disponíveis para qualquer pessoa em qualquer lugar, torna-se necessário o estabelecimento de critérios para a elaboração das mesmas, visto que, mesmo sendo de caráter pessoal, as informações colocadas nos servidores Web da Unicamp podem influir na formação de sua imagem e reputação frente à comunidade.

§ 2º – Dado o elevado número de páginas pessoais e a dinâmica inerente à criação e publicação destas páginas, a Unicamp considera inviável a revisão das informações publicadas eletronicamente por seus membros – professores, funcionários e alunos – e descarta esta prática.

§ 3º – Os autores de páginas pessoais assumem toda a responsabilidade pelo conteúdo de suas páginas e devem estar cientes das responsabilidades e consequências inerentes a estas publicações, prevalecendo a assinatura colhida por ocasião da abertura da conta.

Artigo 75 – Este Capítulo estabelece as seguintes regras básicas para as páginas pessoais residentes em servidores da Unicamp:

I. Páginas pessoais devem ser elaboradas considerando as portarias, normas e regulamentos da Unicamp, regulamentações externas e a legislação

~~usuários de dados e que, intencionalmente e sem autorização, acessem ou publiquem, modifiquem ou destruam dados e informações corporativas estão violando diretamente esta norma.~~

## CAPÍTULO IX

### Do Uso da Tecnologia Web

Artigo 73 – A Unicamp reconhece o escopo e a importância da tecnologia Web na disseminação das informações internas e externas e está comprometida com o desenvolvimento e com o suporte ao conteúdo de qualidade através dos servidores Web.

Artigo 74 – A Unicamp reconhece a importância e a utilidade de publicações eletrônicas através da Internet, principalmente as páginas pessoais, que podem prover informações relevantes sobre o papel de cada indivíduo dentro da Universidade.

§ 1º – Considerando que as páginas pessoais são documentos públicos disponíveis para qualquer pessoa em qualquer lugar, torna-se necessário o estabelecimento de critérios para a elaboração das mesmas, visto que, mesmo sendo de caráter pessoal, as informações colocadas nos servidores Web da Unicamp podem influir na formação de sua imagem e reputação frente à comunidade.

§ 2º – Dado o elevado número de páginas pessoais e a dinâmica inerente à criação e publicação destas páginas, a Unicamp considera inviável a revisão das informações publicadas eletronicamente por seus membros – professores, funcionários e alunos – e descarta esta prática.

~~§ 3º – Os autores de páginas pessoais assumem toda a responsabilidade pelo conteúdo de suas páginas e devem estar cientes das responsabilidades e consequências inerentes a estas publicações.~~

~~Artigo 75 – São regras básicas para as páginas pessoais residentes em servidores Web da Unicamp:~~

~~I – páginas pessoais devem ser elaboradas considerando as portarias, normas e regulamentos da Unicamp, regulamentações externas e a legislação vigente;~~



vigente.

II. O conteúdo das páginas deve refletir o papel de seu autor, os interesses e os padrões correntes na Unicamp e não deve constituir material questionável sob os aspectos legais, éticos e morais.

III. Páginas pessoais não devem dar a impressão de que representam a posição da Unicamp ou que emitem posições e declarações em nome desta.

IV. Páginas pessoais devem incluir uma declaração explícita de que seu conteúdo representa a opinião e pontos de vista individuais do autor e não necessariamente aqueles da Unicamp.

V. Sugere-se o uso da seguinte declaração: "Esta página não é uma publicação oficial da Unicamp, seu conteúdo não foi examinado e/ou editado por esta instituição. A responsabilidade por seu conteúdo é exclusivamente do autor."

VI. É proibida a inclusão e a criação de referências a:

a) material com conteúdo comercial de caráter publicitário;

b) empresas ou entidades externas com objetivos comerciais;

c) material calunioso ou difamatório;

d) material que infrinja a legislação sobre direitos autorais;

e) material ofensivo ou que faça uso de linguagem ofensiva;

f) material que incite a qualquer tipo de discriminação;

g) material que incite à violência;

h) material pornográfico de qualquer natureza;

i) imagens ou dados que possam ser considerados abusivos, profanos, incômodos,

j) ameaçadores ou sexualmente ofensivos a uma pessoa comum, considerados os padrões éticos e morais correntes na comunidade.

VII. O uso do logotipo da Unicamp em páginas

II – o conteúdo das páginas deve refletir o papel de seu autor, os interesses e os padrões correntes na Unicamp e não deve constituir material questionável sob os aspectos legais, éticos e morais.

III – páginas pessoais não devem dar a impressão de que representam a posição da Unicamp ou que emitem posições e declarações em nome desta;

IV – páginas pessoais devem incluir uma declaração explícita de que seu conteúdo representa a opinião e pontos de vista individuais do autor e não necessariamente aqueles da Unicamp;

V – sugere-se o uso da seguinte declaração: "Esta página não é uma publicação oficial da Unicamp, seu conteúdo não foi examinado e/ou editado por esta instituição. A responsabilidade por seu conteúdo é exclusivamente do autor."

VI – é proibida a inclusão e a criação de referências a:

a) material com conteúdo comercial de caráter publicitário;

b) empresas ou entidades externas com objetivos comerciais;

c) material calunioso ou difamatório;

d) material que infrinja a legislação sobre direitos autorais;

e) material ofensivo ou que faça uso de linguagem ofensiva;

f) material que incite a qualquer tipo de discriminação;

g) material que incite à violência;

h) material pornográfico de qualquer natureza;

i) imagens ou dados que possam ser considerados abusivos, profanos, **incômodos**, **ameaçadores** ou sexualmente ofensivos a uma pessoa comum, considerados os padrões éticos e morais correntes na comunidade.

VII – o uso do logotipo da Unicamp em páginas pessoais está regulamentado pela Portaria GR 193/90;

pessoais está regulamentado pela Portaria GR 193/90.

VIII. Toda página deve incluir o nome do autor, a data da última atualização e uma forma de contato.

IX. Os autores devem assumir explicitamente toda a responsabilidade pela informação contida em suas páginas pessoais.

Parágrafo único – Eventuais ocorrências não previstas neste documento serão analisadas pelos órgãos competentes da Unicamp.

Artigo 76 – O Portal da Unicamp é um repositório de informações sobre a Unicamp, disponibilizadas para a comunidade universitária e para o público em geral. O Portal foi projetado para promover a experiência da Unicamp através da publicação periódica de estudos, trabalhos, eventos e informações institucionais de forma geral. Também tem a finalidade de servir como veículo de apresentação da comunidade universitária e seus recursos.

Artigo 77 – A Assessoria de Comunicação e Imprensa da Unicamp – ASCOM é responsável pela divulgação na página principal do Portal.

Artigo 78 – Os visitantes do Portal Unicamp estão livres para divulgar, recomendar e utilizar apontadores e referências do Portal, imagens e textos e outras referências aqui contidas para quaisquer finalidades não comerciais.

Artigo 79 – Os colaboradores do Portal Unicamp estão proibidos de postar ou transmitir de ou para este sítio qualquer material ilegal, ameaçador, caluniador, difamatório, pornográfico ou qualquer outro que possa violar alguma lei.

Artigo 80 – A Unicamp tem a propriedade intelectual sobre os conteúdos publicados no Portal, creditados aos responsáveis pela produção dos documentos. A autoria está nas citações de rodapé em cada arquivo.

Os conteúdos podem ser utilizados sob os seguintes termos:

I. Os Documentos de Autoria, publicados no Portal

VIII – toda página deve incluir o nome do autor, a data da última atualização e uma forma de contato;

IX – os autores devem assumir explicitamente toda a responsabilidade pela informação contida em suas páginas pessoais.

Parágrafo Único – Eventuais ocorrências **que infringjam ou que não são** previstas nesta **norma** serão analisadas pelos órgãos competentes da Unicamp.

Artigo 76 – O Portal da Unicamp é um repositório de informações sobre a Unicamp, disponibilizadas para a comunidade universitária e para o público em geral, **projetado** para promover a experiência da Unicamp através da publicação periódica de estudos, trabalhos, eventos e informações institucionais de forma geral, **além de ter** a finalidade de servir como veículo de apresentação da comunidade universitária e seus recursos.

Artigo 77 – A Assessoria de Comunicação e Imprensa da Unicamp – ASCOM é responsável **pelo conteúdo divulgado no Portal.**

~~Artigo 78 – Os visitantes do Portal Unicamp estão livres para divulgar, recomendar e utilizar apontadores e referências do Portal, imagens e textos e outras referências aqui contidas para quaisquer finalidades não comerciais.~~

~~Artigo 79 – Os colaboradores do Portal Unicamp estão proibidos de postar ou transmitir de ou para este sítio qualquer material ilegal, ameaçador, caluniador, difamatório, pornográfico ou qualquer outro que possa violar alguma lei.~~

Artigo 78 – A Unicamp detém a propriedade intelectual sobre os conteúdos publicados no Portal, **de acordo com a Deliberação CONSU-A-016/2010, de 30/11/2010.**

§ 1º – A Unicamp não assume qualquer responsabilidade sobre o uso indevido das informações contidas no Portal.

§ 2º – Os conteúdos publicados no Portal podem ser utilizados sob os seguintes termos:

I – os documentos produzidos no âmbito da **Universidade** e publicados no Portal Unicamp podem

Unicamp podem ser reproduzidos e distribuídos, no todo ou em parte, em qualquer meio físico ou eletrônico, desde que os termos desta licença sejam obedecidos, e que esta licença ou referência a ela seja exibida na reprodução.

Toda reprodução deverá ser referenciada como "Portal Unicamp – Universidade Estadual de Campinas" e a seus responsáveis e autores.

II. A redistribuição comercial destes documentos não é permitida.

Qualquer intenção de publicação, na forma impressa, deve obrigatoriamente submeter consulta aos Editores do Portal que dará encaminhamento.

Caso a publicação seja autorizada, citar, nas páginas externas, sua origem e atribuições de direito autoral (A Universidade Estadual de Campinas, Instituto/Faculdade ou órgão responsável e seu Autor).

III. A licença de uso e redistribuição dos documentos é oferecida, sem nenhuma garantia de qualquer tipo, expressa ou implícita, quanto à sua adequação a qualquer finalidade.

IV. Adicionalmente, devem ser observadas as seguintes restrições:

a) A versão "modificada" – traduzida ou derivada, deve ser identificada como tal.

b) Versões modificadas não contam com o endosso dos autores originais, salvo autorização fornecida por escrito.

c) O responsável pelas modificações deve ser identificado e as modificações datadas.

d) O reconhecimento da fonte original do documento deve figurar explicitado.

e) A localização da fonte original deve ser citada.

A Unicamp não assume qualquer responsabilidade sobre o uso indevido das informações contidas no Portal.

ser reproduzidos e distribuídos, no todo ou em parte, em qualquer meio físico ou eletrônico, desde que os termos **deste Artigo sejam obedecidos e desde que este Artigo ou uma referência a ele sejam exibidos na reprodução;**

**II – toda reprodução deste conteúdo deverá fazer referência ao Portal, a seus responsáveis e autores;**

**III – o uso e/ou a redistribuição comercial deste conteúdo não são permitidos;**

**IV – qualquer iniciativa de publicação deste conteúdo na forma impressa deve obrigatoriamente ser precedida de autorização explícita do responsável pelo Portal;**

~~**caso a publicação seja autorizada, deverão ser indicadas, nas páginas externas, sua origem e as atribuições de direito autoral (à Universidade Estadual de Campinas, Instituto/Faculdade ou órgão responsável e seu Autor);**~~

**V – a licença de uso e redistribuição dos documentos é oferecida sem nenhuma garantia de qualquer tipo, expressa ou implícita, quanto à sua adequação a qualquer finalidade;**

**VI – devem ser observadas as seguintes restrições:**

a) **uma versão modificada** – traduzida ou derivada – deve ser identificada como tal;

b) **versões modificadas** não contam com o endosso dos autores originais, salvo autorização fornecida por escrito;

c) **o responsável** pelas modificações deve ser identificado e as modificações datadas;

d) **o reconhecimento** da fonte original do documento deve figurar explicitado;

e) **a localização** da fonte original deve ser citada.

~~**A Unicamp não assume qualquer responsabilidade sobre o uso indevido das informações contidas no Portal.**~~

**Artigo 79 – As informações pessoais dos usuários,**

Artigo 81 – As informações enviadas pelos usuários e identificadas como "pessoal", inseridas nos formulários de captura de dados, bem como todo e qualquer material, informação na forma de dados ou artigos ou outra comunicação transmitida ou postada para este Portal será considerada confidencial.

§ 1º – O Portal Unicamp não publicará nenhum conteúdo, exceto nos casos de prévia autorização pelo autor/proprietário.

Porém, nada impedirá que a informação publicada no Portal possa ser reproduzida por algum visitante, ficando, portanto, a critério do autor a livre decisão de acioná-lo legalmente.

§ 2º – Não será publicado nenhum conteúdo de sugestão e/ou avaliação emitida a partir do preenchimento de formulários, no entanto poderão ser publicados resultados de apurações estatísticas.

## CAPÍTULO X

### Do Acesso a Sistemas e Serviços Informatizados Institucionais

Artigo 84 – Considerando o tamanho e a variedade do parque computacional, a necessidade de viabilizar um maior uso de software livre, bem como a preservação dos investimentos já feitos pela Unicamp em tecnologias da informação e comunicação, ficam estabelecidas as seguintes normas:

a) Os mecanismos de acesso a sistemas e serviços eletrônicos institucionais não devem impor uma plataforma (hardware e software) particular aos usuários finais.

b) Caso o acesso se dê através da Web, então ele deve ser possível via os diversos navegadores em uso pela Unicamp.

c) Se houver necessidade de software cliente nos equipamentos dos usuários finais, o seu uso não deve onerar as Unidades e Órgãos que interagem com sistemas e servidores de informação da Unicamp.

d) Eventuais ferramentas complementares requeridas por sistemas ou serviços eletrônicos da Unicamp devem ser ferramentas sem custo.

Parágrafo único – Sistemas e serviços da Unicamp em

bem como dados, artigos ou outras informações coletadas pelo Portal Unicamp serão consideradas confidenciais.

§ 1º – O Portal Unicamp não publicará nenhum conteúdo considerado confidencial, exceto nos casos de prévia autorização pelo autor ou responsável pelos dados.

~~Porém, nada impedirá que a informação publicada no Portal possa ser reproduzida por algum visitante, ficando, portanto, a critério do autor a livre decisão de acioná-lo legalmente.~~

§ 2º – O Portal Unicamp poderá publicar os resultados da apuração de dados estatísticos obtidos a partir dos dados fornecidos pelos usuários.

## CAPÍTULO X

### Do Acesso a Sistemas e Serviços Informatizados Institucionais

Artigo 80 – Considerando o tamanho e a variedade do parque computacional, **as vantagens** de viabilizar um maior uso de software livre, bem como a preservação dos investimentos já feitos pela Unicamp em **Tecnologias da Informação e Comunicação**, ficam estabelecidas as seguintes normas:

**I – os** mecanismos de acesso a sistemas e serviços eletrônicos institucionais **devem evitar** impor uma plataforma (hardware e software) particular aos usuários finais;

**II – caso** o acesso se dê através da Web, então ele deve ser **viável a partir de pelo menos dois dentre os** navegadores **mais usados na Internet**;

**III – se** houver necessidade de software cliente nos equipamentos **dos usuários**, sua instalação e uso não devem onerar **os Órgãos responsáveis por tais equipamentos**;

~~**IV – eventuais ferramentas complementares requeridas por sistemas ou serviços eletrônicos da Unicamp devem ser ferramentas sem custo.**~~

~~**Parágrafo único. Sistemas e Serviços Informatizados Institucionais da Unicamp em desacordo com as**~~

desacordo com as normas acima, terão um prazo de 30 (trinta) meses, a partir da publicação destas Normas para entrarem em conformidade com o estabelecido no caput deste artigo.

~~normas acima, terão um prazo de 30 (trinta) meses, a partir da publicação desta Resolução, para entrarem em conformidade com o estabelecido no caput deste artigo.~~

## CAPÍTULO XI

### Da Adoção de Formatos Abertos para Documentos Digitais

Artigo 81 – É recomendada a adoção de formatos digitais abertos para intercâmbio e preservação de documentos produzidos pela Unicamp.

Artigo 82 – A recomendação do Artigo anterior se aplica à edição e distribuição de documentos digitais oficiais na forma de textos formatados, formulários, planilhas, figuras ou apresentações (slides) que sejam produzidos pela Unicamp para uso interno ou externo.

Artigo 83 – Os formatos digitais abertos a serem adotados são:

I. Open Document Format (ODF), padronizado pela Associação Brasileira de Normas Técnicas (ABNT) como NBR ISO/IEC26300:2008 – Formato aberto de documento para aplicações de escritório (Open Document) v1.0 e posteriores, e

II. Portable Document Format (PDF), padronizado como ISO 32000-1:2008 – “*Document management—Portable document format—Part 1: PDF 1.7*” e, futuramente, como ABNT NBR ISO/IEC32000-1.

§ 1º – Considerando a maior disponibilidade de softwares para edição de arquivos no formato ODF, o uso deste formato deverá ser priorizado nas fases de criação, edição e distribuição de documentos não finalizados, como formulários, por exemplo.

§ 2º – Considerando a maior portabilidade do formato PDF para visualização de documentos, este formato deverá ser adotado preferencialmente na distribuição de documentos já finalizados.

§ 3º – Caso outros formatos digitais sejam eventualmente empregados, um dos formatos definidos no caput também deverá ser usado no armazenamento e distribuição do documento.

Artigo 84 – Com o objetivo de facilitar a adoção dos formatos definidos no Artigo 83, a CTIC deverá

promover iniciativas de capacitação no uso de programas de computador que suportem estes formatos e que façam a conversão de documentos para os mesmos.

Artigo 85 – Os órgãos responsáveis por sistemas de TI corporativos da Unicamp deverão realizar a adequação destes sistemas para que deem suporte aos formatos definidos no Artigo 83.

## CAPÍTULO XII

### Da Instalação e Uso de Equipamentos de Comunicação de Dados Sem Fio

Artigo 86 – A implantação e uso de redes de dados sem fio nos campi da Unicamp deverão ser regidas pela presente norma de acordo com os seguintes conceitos:

a) 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;

b) Cliente – equipamento da rede sem fio que é operado pelo usuário final; é qualquer dispositivo com interface de rádio apropriada para viabilizar a comunicação com um AP;

c) 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;

d) 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.);

e) ISM – bandas de rádio não licenciadas e reservadas para uso industrial, científico e médico (Industrial, Scientific and Medical radio bands);

f) Redes sem fio – redes de comunicação de dados que fazem uso de ondas de rádio para estabelecer os enlaces de comunicação entre os componentes;

g) Wi-Fi – termo utilizado para descrever redes locais sem fio baseadas nos padrões IEEE 802.11;



h) Rede sem fio Unicamp – é a rede sem fio com administração e autenticação centralizadas e que tem como objetivo oferecer acesso à rede da Universidade e à Internet;

i) Rede sem fio do Órgão – é a rede sem fio com administração e/ou autenticação localizadas no Órgão em que está instalada e que tem como objetivo oferecer acesso aos serviços de rede disponíveis no Órgão, estendendo e complementando sua rede cabeada;

j) 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;

k) Rede sem fio de permissionários – é a rede sem fio com administração e autenticação feitas pelo permissionário de serviços na 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 87 – Todos os APs, antenas e componentes de transmissão de uma infraestrutura de rede sem fio nos campi da Unicamp devem estar registrados junto a CTIC.

Parágrafo Único – O registro deve ser renovado quando houver alteração de informações ou quando for solicitado pela CTIC.

Artigo 88 – Cabe ao Órgão fiscalizar e 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 (equipamentos com Bluetooth, telefones sem fio, fornos de microondas etc.).

§ 1º – Um equipamento, seja de rede sem fio ou não, que venha 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.