REGULAMENTO GERAL PARA USO E ADMINISTRAÇÃO DE COMPUTADORES E REDES DA UNESP

Versão 1.0

Referência: RG–AI.00.01.01
Data: 07/Jan/1998

Assessoria de Informática

Janeiro de 1998

Alameda Santos, 647 - 13º andar – CEP 01419-901 – São Paulo, SP – Tel. (11) 252-0415 – http://www.unesp.br/ai

REGULAMENTO GERAL PARA USO E ADMINISTRAÇÃO DE COMPUTADORES E REDES DA UNESP

Referência: RG–AI.00.01.01
Data: 07/01/1998

1.INTRODUÇÃO

Este documento pretende levar em consideração o uso apropriado dos recursos de computação e redes, a proteção e a privacidade efetiva aos usuários, e a própria administração desses recursos na UNESP. Estas regras visam a complementar e não substituir leis já existentes que se apliquem a estes serviços.

As Unidades Universitárias, Núcleos e Centros de Pesquisa, Fundações Associadas, Departamentos, Laboratórios, Diretorias, Seções, Setores e congêneres - doravante **denominados genericamente de "Unidades"** - da UNESP, que operam seus próprios computadores e redes podem acrescentar, com a autorização do Diretor da Unidade ou de seu órgão assessor (Comissão Local de Informática - CLI), regras próprias para complementar este regulamento, sem a intenção de abrandá-lo. Qualquer ato no sentido de suplantar ou desautorizar este regulamento será considerado sem efeito.

1.1. Fundamento Principal

O uso de computadores e redes deve estar relacionado ao ensino, ao estudo independente, à pesquisa autorizada, à pesquisa independente, ao acesso e à disseminação de informações de interesse da UNESP, e ao trabalho das Unidades.

2.DEFINIÇÕES

2.1. Autorização de uso:

Autoriza-se o uso dos recursos de computação e de redes pertencentes à UNESP, ou operados pela mesma, para fins de educação, pesquisa, prestação de serviços e outras atividades que estiverem de acordo com os regulamentos desta Universidade.

2.2. Usuários autorizados

São considerados usuários autorizados dos sistemas de computação da

UNESP: corpo docente, servidores técnicos e administrativos e alunos em situação regular junto às Unidades. As Unidades podem ceder autorizações especiais de uso ou acesso, por tempo determinado, desde que esta utilização esteja de acordo com o item 1.1 acima.

3.RESPONSABILIDADES INDIVIDUAIS

3.1. Acesso a informações

Nenhum usuário pode ter acesso, copiar, alterar ou remover arquivos de terceiros sem autorização explícita, ressalvados casos especiais protegidos por lei ou regulamento.

3.2. Propriedade intelectual

Todos os usuários têm o dever de reconhecer e honrar a propriedade intelectual e os direitos autorais.

3.3. Molestamento

Nenhum membro da comunidade de usuários pode, sob quaisquer circunstâncias, usar computadores e redes da UNESP para difamar, caluniar ou molestar outras pessoas.

3.3.1. Situações de molestamento

Entende-se por molestamento o uso intencional dos computadores ou redes para:

- Perturbar, amedrontar, ameaçar ou ofender pessoas usando linguagem ou qualquer outro mecanismo ou material para fazer ameaças que comprometam a integridade física ou moral do receptor ou de sua família;
- Contatar alguém várias vezes com a intenção de perturbá-la, enviando ou não mensagens, seja quando não existe uma proposta de comunicação ou quando o receptor expressa o desejo de finalizar a comunicação;
- Indisponibilizar recursos computacionais de forma intencional;
- Causar danos ou prejudicar as pesquisas ou a administração acadêmica;
- Invadir a privacidade da Unidade, da UNESP ou de outros.

3.4. Responsabilidade no uso dos recursos

Os usuários devem estar cientes das regras e normas de uso dos recursos de informática (que podem ser setoriais), evitando, desse modo, os procedimentos que prejudicam ou impedem outras pessoas de terem

acesso a esses recursos ou de usá-los de acordo com o que é determinado. Os usuários não podem, deliberadamente, sobrecarregar os recursos computacionais ou de rede.

3.5. A Integridade e confiabilidade das informações

É dever do usuário estar ciente do potencial e das possíveis conseqüências da manipulação de informações, especialmente em forma eletrônica, e assim entender a natureza mutante de informações armazenadas eletronicamente, além de verificar a integridade e a completitude das informações que acessa ou usa. O usuário não deve confiar em informações que contrariem suas expectativas, sem antes verificá-las diretamente junto ao possível remetente da mensagem, do arquivo ou de qualquer tipo de dado.

3.6. O uso de sistemas

O usuário é responsável pela segurança e integridade das informações da UNESP armazenadas nos computadores sob sua responsabilidade. Essa responsabilidade inclui proceder regularmente cópias de segurança de seus dados, controlar o acesso à rede, às suas senhas e às máquinas sob seu uso, e usar programas de proteção contra vírus. Deve-se evitar armazenar senhas ou outras informações que possam ser usadas para o acesso a recursos de computação da Unidade.

3.7. Acesso às instalações e informações

3.7.1. Proibição de acesso compartilhado

O usuário é inteiramente responsável pelo uso de sua conta de acesso à rede, senha e outros tipos de autorização, que são de uso individual e intransferível, e não podem ser compartilhados com terceiros. Contas de acesso à rede devem ser individuais e não-compartilhadas, salvo em situações especiais que a Unidade julgar necessárias, e dentro de prazos curtos e pré-determinados.

3.7.2. Usuários não-autorizados

Não é permitido executar ou configurar software ou hardware com a intenção de facilitar o acesso a usuários não-autorizados.

3.7.3. Obrigatoriedade do uso de senhas seguras

O usuário é responsável pela manutenção de senhas seguras, devendo seguir normas e procedimentos padronizados e divulgados publicamente pelos órgãos de informática da UNESP. O usuário é totalmente responsável por ações indevidas

que venham a ser efetuadas a partir de sua conta de acesso à rede, caso alguém obtenha o acesso à sua conta devido à não utilização de senhas seguras.

3.7.4. Uso de acesso privilegiado pelos administradores dos sistemas

O acesso especial a senhas, informações ou outros privilégios só pode ser usado para o exercício de tarefas oficiais. Informações obtidas por meio de direitos especiais e privilégios devem ser tratadas como privativas e totalmente confidenciais pelos administradores, que responderão por qualquer uso indevido.

3.7.5.Cancelamento do acesso

Ao deixar de ser membro da comunidade da UNESP (graduar-se, terminar suas atividades ou demitir-se), ou ao ser nomeado para assumir uma nova função e/ou novas responsabilidades para com a UNESP, o usuário deverá ter sua autorização de acesso revista e não poderá fazer uso de benefícios, contas, senhas de acesso, direitos especiais ou informações aos quais não está autorizado em sua nova situação. Privilégios especiais não são incorporados permanentemente aos direitos dos usuários.

3.7.6. Acesso de computadores à rede

Computadores mono e multiusuário e servidores de rede ou similares, de qualquer espécie, não podem ser conectados à rede de computadores da Unidade ou da UNESP sem notificação e autorização dos administradores, assim como dos supervisores responsáveis pela rede na Unidade. Todos os computadores conectados devem obedecer os procedimentos padronizados de segurança estabelecidos pela Unidade ou por órgãos superiores da UNESP e devem seguir este regulamento. Deve ser facultado acesso dos administradores a todos os equipamentos ligados à rede, de forma a ser possível a realização de procedimentos de auditoria, controle e segurança que se fizerem necessários.

3.8. Autorização de uso de mecanismos de auditoria e segurança

Os responsáveis pela administração dos sistemas possuem autorização para utilizar o sistema de segurança ou qualquer mecanismo que julgarem mais adequado para a realização de auditoria e o controle dos computadores e redes.

3.9. Acessos, operações e ações proibidas aos usuários

3.9.1. Decodificação e acesso ao controle de informações

Os Usuários não podem utilizar qualquer software ou outro dispositivo para interceptar ou decodificar senhas ou similares.

3.9.2. Atividades perniciosas

É proibida toda e qualquer tentativa deliberada de retirar o acesso à rede ou a qualquer computador da UNESP, ou de prejudicar o seu rendimento. Procedimentos considerados graves:

- Criar ou propagar vírus, danificar serviços e arquivos;
- Destruir ou estragar intencionalmente equipamentos, software ou dados pertencentes à UNESP ou a outros usuários;
- Obter acesso a qualquer recurso não-autorizado;
- Destituir os direitos de outros usuários;
- Obter acesso não-autorizado aos sistemas.

As ações acima são proibidas mesmo com o uso dos seguintes expedientes:

- Senhas especiais obtidas por quaisquer meios;
- Falhas nos sistemas de segurança dos computadores e redes;
- Senhas de terceiros obtidas por quaisquer meios;
- Direitos especiais de acesso já extintos com o término do período de ocupação de cargo ou função na UNESP.

3.9.3. Monitoramento não-autorizado

Os recursos de computação não podem ser utilizados para o monitoramento não-autorizado de mensagens eletrônicas ou de qualquer transmissão de dados.

3.9.4. Uso de informações e materiais protegidos por copyright

Não é permitido ao usuário servir-se dos recursos de informática da UNESP para usar, examinar, copiar ou armazenar qualquer material protegido por *copyright*, sem que possua licença ou autorização específica para tal.

3.9.5. Propagandas e campanhas políticas

É proibido o uso de computadores e redes da UNESP em campanhas políticas ou propaganda de qualquer espécie. A veiculação de nomes de empresas, instituições ou pessoas junto aos sistemas de informação da UNESP só poderá ser realizada se houver o estabelecimento oficial e reconhecido de convênios de cooperação ou parceria acadêmica, técnica ou científica.

3.9.6. Uso dos recursos da UNESP em atividades particulares

Computadores, redes e outros serviços de informática não podem ser usados para trabalhos particulares, ou em benefício de organizações que não tenham relação com a UNESP e em acordo com o item 1.1. acima.

3.9.7. Uso excessivo

O uso individual dos recursos computacionais, tais como mensagens eletrônicas, acesso à Internet, o armazenamento de dados em computadores ou a impressão de arquivos, não devem ser excessivos nem interferir na utilização e acesso a outros usuários a estes recursos.

3.9.8. Inatividade do acesso à conta

O tempo máximo de inatividade de uma conta é de 6 meses. O usuário será avisado após 4 meses de inatividade da conta e quando da extinção da mesma. Cabe ao Administrador de Rede Local providenciar mecanismos para esse controle.

4.PRIVILÉGIOS DAS UNIDADES

4.1. Controle do acesso a informações

As Unidades devem controlar o acesso a suas informações e a suas formas de armazenamento, a manipulação e a transmissão de acordo com as normas superiores da UNESP, de conformidade com as leis estaduais e federais.

4.2. Imposição de sanções

As Unidades devem impor sanções e penas aos que violarem este regulamento.

4.3. Acesso de supervisores e administradores ao sistema

O supervisor ou administrador (responsável pelas operações técnicas de

determinada máquina ou rede) pode ter acesso a arquivos de outros usuários para garantir a segurança, manutenção e conservação de redes, computadores e sistemas armazenados. No entanto, todos os privilégios individuais e direitos de privacidade dos usuários deverão ser preservados.

4.4. Monitoramento de uso, inspeção de arquivos e auditoria

As Unidades da UNESP responsáveis pelas operações de informática que, freqüentemente, operam computadores e redes podem monitorar e registrar dados como início e fim de conexão à rede, tempo de CPU, utilização de discos feita por cada usuário, registros de auditoria, carga de rede, dentre outros. Os supervisores ou administradores responsáveis pelas redes e recursos computacionais devem rever e observar periodicamente essas informações, certificando-se de que não houve a violação de leis nem de regulamentos, ou para outros fins.

Se houver evidência de atividade que possa comprometer a segurança da rede ou dos computadores, estes supervisores podem monitorar todas as atividades de um determinado usuário, além de inspecionar seus arquivos nos computadores e redes, a bem do interesse da UNESP. As ações de auditoria são restritas aos supervisores responsáveis pelo gerenciamento da rede em questão. O supervisor que acreditar que tal monitoramento ou inspeção é necessária, deve notificar seu superior imediato para realizar esta operação. Ao utilizar os recursos de informática da UNESP, o usuário concorda com esta norma e autoriza implicitamente as ações de auditoria eventualmente necessárias.

4.5. Suspensão de privilégios individuais

As Unidades podem suspender todos os privilégios de determinado usuário em relação ao uso de redes e computadores sob sua responsabilidade, por razões ligadas à segurança física e ao bem estar do usuário, ou por razões disciplinares ou relacionadas à segurança e ao bem-estar dos outros membros da Unidade ou da UNESP.

4.5.1. Possibilidade de novo acesso

O acesso será prontamente restabelecido quando a segurança e o bem-estar puderem ser assegurados; a suspensão do acesso pode continuar se for resultado de uma ação disciplinar imposta pelos órgãos assessores da Unidade ou instâncias superiores.

5.RESPONSABILIDADES DAS UNIDADES

5.1. Medidas de segurança

A Unidade e seus órgãos encarregados da administração dos recursos computacionais são responsáveis pelas medidas de segurança necessárias

para garantir a integridade de informações relativas à Unidade e a cada usuário, independentemente da maneira pela qual estejam armazenadas, e impor as penalidades cabíveis quando qualquer norma for desrespeitada.

5.2. Defesa de direitos autorais e de licenças

A Unidade defenderá os direitos autorais (*copyright*), as leis que regulamentam o acesso e o uso de informações e as regras de organizações que fornecem informações aos membros da comunidade (por exemplo, regras ou procedimentos para o uso da Internet ou outras redes).

5.3. Deveres de cada Unidade

Cabe a cada Unidade a responsabilidade de:

- Assegurar o cumprimento deste regulamento;
- Manter fichas cadastrais com os dados de todos os usuários autorizados, inclusive com a assinatura do termo de compromisso ratificando o conhecimento e a concordância deste e de outros regulamentos, conforme modelo no anexo I;
- Manter, na Unidade, um registro das ocorrências de violação dos regulamentos;
- Garantir a segurança de suas áreas;
- Controlar o acesso físico aos equipamentos sob sua responsabilidade;
- Não permitir que softwares licenciados para uso da UNESP sejam copiados por terceiros ou instalados em computadores não autorizados.

Por responder pela importância e a sensibilidade das informações armazenadas e processadas em suas instalações, o setor responsável pelos recursos de informática da Unidade (Pólo Computacional ou similar) e seus administradores, gerentes ou coordenadores terão a responsabilidade de :

- Designar funcionários para administração dos sistemas;
- Fazer cópias de segurança e verificar sua integridade;
- Adotar medidas apropriadas de segurança em relação a software e rotinas;
- Preservar informações confidenciais como, por exemplo, arquivos de usuário e códigos de acesso ao sistema;
- Administrar devidamente o acesso, regularizar de maneira rápida e precisa as permissões de acesso para usuários transferidos ou que tiveram seu acesso cancelado (ver item 3.7.5);
- Controlar, gravar software e mudar de configuração os sistemas de rede e similares ;
- Monitorar os *logins* , acessos e registros de auditoria dos sistemas para controlar tentativas de violação e quebra de segurança;

- Manter as conexões e o roteamento de transmissão de dados em funcionamento;
- Respeitar e seguir os procedimentos padronizados para a administração de recursos de informática e redes definidos pelos órgãos superiores da UNESP.

5.4. Serviços de informação ao público

As Unidades e seus responsáveis podem, com permissão do Diretor ou de seu órgão assessor, configurar sistemas para fornecer serviços de busca de informações à comunidade externa (os exemplos atuais incluem serviços de "*anonymous ftp*", "*listservers*" e "WWW").

5.4.1. Sobrecarga

A extensão desses serviços ao público não poderá provocar sobrecarga nos computadores e redes, prejudicando assim outros serviços, e respeitará incondicionalmente este regulamento.

6.PROCEDIMENTOS E SANÇÕES

6.1. Conhecimento e concordância deste regulamento

Todo interessado, ao se cadastrar como usuário de recursos de informática da UNESP, deve preencher e assinar uma ficha cadastral e um termo de compromisso elaborado pela Unidade, o qual manifesta conhecimento e concordância, comprometendo-se a respeitar este regulamento e as normas específicas de uso e acesso de cada Unidade (vide anexo I). Esta ficha cadastral deverá ser mantida sob o controle da Unidade em caráter confidencial e as informações presentes não poderão ser utilizadas para qualquer finalidade não relacionada ao controle, à segurança e à integridade dos sistemas.

6.2. Respondendo pela segurança e incidentes

Todos os usuários e administradores têm o dever de denunciar qualquer tentativa de acesso não-autorizado ou qualquer outro uso indevido de computadores e redes da UNESP. Ao testemunhar ou tomar conhecimento (por quaisquer meios) de problemas relacionados à segurança ou ao uso abusivo de computadores e redes, incluindo o desrespeito a este regulamento, o usuário deve tomar imediatamente as providências necessárias que estiverem a seu alcance, para garantir a segurança e a conservação dos recursos e notificar as seguintes pessoas:

- O administrador ou coordenador do sistema em questão;

- Seu chefe imediato ou o presidente da Comissão Local de Informática.

6.3. Incidentes e suas conseqüências

O primeiro incidente, considerado não grave, envolvendo um usuário será julgado em nível de Unidade pela CLI, a qual deverá impor as sanções cabíveis, com posterior registro da ocorrência.

Reincidências e incidentes considerados graves deverão ser tratados pela CLI, a qual encaminhará o caso ao Diretor da Unidade, para determinação das sanções a serem impostas, com posterior registro da ocorrência.

6.4. Penalidades a serem aplicadas

6.4.1. Penalidades nível I (não grave)

A violação das normas descritas referente aos itens 3.6 e 3.9.5 resultará na suspensão temporária de privilégios de acesso por, no mínimo, 7 dias e, no máximo, 3 meses.

6.4.2. Penalidades nível II (intermediário)

A violação das normas descritas referente aos itens 3.1, 3.2, 3.4, 3.7.1, 3.7.3, 3.9.4 e 3.9.6 resultará na suspensão temporária de privilégios de acesso por, no mínimo, 7 dias e, no máximo, 6 meses.

6.4.3. Penalidades nível III (grave e reincidências)

A violação das normas descritas referente aos itens 3.3, 3.7.2, 3.7.4, 3.7.5, 3.7.6, 3.9.1, 3.9.2 e 3.9.3 resultará na suspensão temporária de privilégios de acesso por, no mínimo, 30 dias e, no máximo, 1 ano.

6.4.4. Outras situações

Todas as demais violações das normas, ainda que não expressamente descritas, serão punidas com suspensão temporária ou permanente de privilégios de acesso aos recursos computacionais, após avaliação da gravidade da infração.
Qualquer que seja o tipo de infração, dependendo de sua gravidade, as penalidades aqui fixadas poderão ser substituídas pela penalidade de suspensão permanente de privilégios de acesso aos recursos computacionais.

Caso as infrações às normas de segurança impliquem também em falta disciplinar, o assunto será objeto de apuração e solução

mediante a aplicação das normas já existentes na Universidade de acordo com o Regimento Geral da UNESP.

6.5. A extensão das sanções disciplinares

Os alunos e servidores da UNESP que desrespeitarem este regulamento, além das sanções anteriormente descritas, estão sujeitos a ações disciplinares ou demissão a bem do serviço público. As sanções impostas pela Unidade não isentam o responsável de outras ações legais. Os incidentes envolvendo telecomunicações ou transmissão de dados que forem considerados crimes, de acordo com as leis estaduais ou federais, deverão ser denunciados pela Unidade às autoridades competentes.

O possível desconhecimento desse regulamento por parte do usuário não o isenta das responsabilidades e das sanções aplicáveis, nem pode minimizar as medidas cabíveis.

7.CASOS OMISSOS A ESTE REGULAMENTO

Casos omissos a este regulamento serão tratados pela Comissão Local de Informática e pelo Diretor da Unidade, cabendo recurso à Comissão de Informática da Reitoria.

São Paulo, 07 de janeiro de 1998
UNESP - Reitoria
Assessoria de Informática

ANEXO I

MODELO DE FICHA DE CADASTRO PARA USO DE RECURSOS COMPUTACIONAIS E ACESSO À REDE DE COMPUTADORES

(Pode ser adaptada para atender necessidades e exigências locais)

Nome_____
_____

Vínculo com a UNESP:
( )Servidor ( )Aluno ( )Outros _____

Unidade – Órgão _____

Documento de Identificação (R.G. ou passaporte)_____

Endereço
completo_____
_____

Telefone res./com. _____

Máquina – Domínio _____

Nome da conta (username) _____

Data do término da validade (definida pelo responsável pela autorização da conta) _____/_____/_____.

TERMO DE COMPROMISSO

Declaro ser responsável pela conta acima solicitada, sendo conhecedor(a) das determinações contidas no Regulamento Geral para Uso e Administração de Computadores e Redes da UNESP (http://www.unesp.br/ai/pdf/rg-ai.00.01.01.pdf). Comprometo-me a respeitar as normas da Universidade relativas ao assunto, assumindo as conseqüências administrativas, cíveis e penais decorrentes do desvio de finalidade e do desrespeito às normas de uso de contas. Comprometo-me, ainda, a aceitar eventuais alterações e regulamentações futuras, assim como de comunicar meu desligamento da Universidade, a qualquer título, para a regularização da conta.

Por ser verdade, firmo a presente.

_____
Usuário

Local_____/_____/_____.