PROCEDIMENTO PARA INGRESSO DE NOVOS BOLSISTAS NO LABEEE – Referente ao uso dos cartões de acesso (crachá).

1. Criar um currículo Lattes em: https://wwws.cnpq.br/cvlattesweb/pkg_cv_estr.inicio

2. Ler as instruções sobre a política de uso da internet (anexo)

3. Preencher o cadastro online na página do LabEEE em: http://www.labeee.ufsc.br/user/register

4. Preencher o formulário “Termo de Compromisso” (anexo) e solicitar a assinatura do orientador.

5. Entregar o formulário e retirar o crachá.

Política de segurança

LabEEE - Laboratório de Eficiência Energética em Edificações

Kathia Jucá
Coordenadora de Segurança da Informação (NPD-UFSC)

Prof. Roberto Lamberts
Coordenador do LabEEE

6 de agosto de 2010

Estas Instruções Reguladoras têm por finalidade regular as condições de acesso e utilização dos recursos da Internet em proveito da Instituição, em consonância com a Portaria GSI/PR n_ 16, de 22.01.2001, Decreto n_ 3.505, de 13.06.2000. São objetivos destas Instruções:

1. Utilização dos Recursos Computacionais
2. Gerenciamento de Web Sites
3. Normas de Utilização do Correio Eletrônico
4. Normas de Segurança para Utilização da Internet
5. Privacidade de mensagens Eletrônicas e Arquivos de Computador

1 Utilização dos Recursos Computacionais

Recursos Computacionais do Laboratóncia Energética em Edificações da Universidade Federal de Santa Catarina são os equipamentos, instalações e recursos de informação direta ou indiretamente administrados, mantidos ou operados pelo Laboratorio, tais como:

- computadores e terminais de qualquer espécie;
- impressora;
- redes, incluindo equipamentos de telecomunicações;
- recursos de informação que incluem todas as informações eletrônicas, serviço de correio eletrônico, mensagens eletrônicas, documentos,executados ou transmitidos através dos computadores, redes ou outros sistema de informação.
- Todos os equipamentos de terceiros, conectados à rede Instituição estão sujeitos às mesmas políticas.

1.1 Diretrizes e Regulamentações

Usuário é qualquer pessoa, autorizada ou não, que utiliza, de qualquer forma, algum Recurso Computacional do LabEEE, incluindo pessoas físicas ou jurídicas que acessam os recursos via uma rede de comunicação ou em salas de computadores e aquelas que utilizam qualquer rede da Instituição para conectar uma máquina pessoal e qualquer outro sistema ou serviço. Definição das figuras mencionadas no texto:

- SeTIC – Superintendência de Governança Eletrônica e Tecnologia da Informação e Comunicação
- Administrador da Rede: O Administrador de Rede é designado e tem como atribuição principal o gerenciamento da rede , bem como dos recursos computacionais da Unidade à ela conectados direta ou indiretamente.

1.2 Política

- É política da Instituição 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. É política da Instituição que as fontes de Informação sejam utilizadas pelos membros da comunidade dentro do respeito e da ética.
- Fundamental para o uso apropriado e responsável é a premissa que, em geral, os recursos computacionais devem ser utilizados de maneira responsável, consistente com os objetivos educacionais, de pesquisa e administrativos da Instituição.
- O uso deve também estar de acordo com os objetivos específicos do projeto ou tarefa para a qual o uso foi autorizado. Todas as utilizações que não estão de acordo com estes objetivos são consideradas inapropriadas e podem colocar em risco os demais acessos a serviços.
- Os recursos computacionais *não* podem ser utilizados para constranger, assediar, ameaçar ou perseguir qualquer pessoa. Esses recursos não podem ser usados para alterar ou destruir recursos computacionais de outra instituições.
- 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 qual, a seu critério, e sem prejuízo de outras sanções, poderá determinar a imediata suspensão temporária da conta de onde parte a interferência.

O acesso à infra-estrutura de tecnologias de informação e comunicação, o compartilhamento de informações e a segurança da produção intelectual da comunidade, exigem que cada um dos usuários assuma a responsabilidade de proteger os direitos da comunidade. O acesso aos recursos computacionais da Instituição deve ser considerado um privilégio e como tal deve ser tratado por todos os seus usuários. Adotando esta política, a Instituição 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.

1.3 Responsabilidades

Esta política estabelece a expectativa de uso de maneira ética dos recursos computacionais da Instituição. No entanto, a utilização dos recursos computacionais é altamente complexa podendo evoluir e incorrer em riscos. Esta seção tem o objetivo de especificar as responsabilidades dos usuários de acordo com esta política e promover o uso ético, legal e seguro dos recursos computacionais para a proteção de todos os membros da comunidade.

1.3.1 Responsabilidades do Usuário

Constituem responsabilidades do Usuário relativamente ao uso dos Recursos Computacionais:

1. Respeitar todas as políticas e procedimentos da Instituição incluindo, mas não limitado, às normas de uso apropriado dos recursos de informação e tecnologias da informação e comunicação, aquisição, uso e descarte de equipamentos de propriedade da Instituição, de uso de equipamentos de telecomunicação e de uso legal e ético de software e de dados corporativos. O usuário é responsável por conhecer e obedecer às políticas específicas estabelecidas para o sistema e para a rede que ele acessa.

2. Respeitar os direitos de outros usuários, incluindo os direitos garantidos em outras políticas da Instituição para alunos, docentes e funcionários; estes direitos incluem, mas não estão limitados, a privacidade e liberdade de expressão.

3. Utilizar qualquer Recurso Computacional 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. Os usuários devem comprovar seu vínculo com a Instituição ou autorização especial ao pessoal responsável, sempre que solicitado durante a utilização dos recursos, sob pena de imediata suspensão da conexão.

4. Respeitar a integridade de sua autorização de acesso ou conta. Os usuários são responsáveis por qualquer atividade desenvolvida com o auxílio dos recursos computacionais e pelos eventuais prejuízos dela decorrentes. Os usuários são responsáveis pela 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. Os usuários devem relatar imediatamente ao Grupo de Segurança de Recursos Computacionais qualquer suspeita de tentativa de violação de segurança.

5. Não permitir ou colaborar com o acesso aos Recursos Computacionais por parte de pessoas não autorizadas.

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

7. Respeitar a integridade dos recursos computacionais. 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 Instituição, de sua propriedade ou de qualquer outra pessoa ou instituição. Essas alterações incluem, mas não se limitam, a alteração de dados, reconfiguração de chaves de controle ou parâmetros, ou mudanças no software embutido.

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

9. Respeitar os direitos de propriedade intelectual, em particular a lei de direitos autorais de software. É de responsabilidade do usuário utilizar apenas produtos de software com as licenças de uso válidas.

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

11. Comunicar ao Administrador da rede local ou ao Grupo de Segurança de Recursos Computacionais qualquer evidência de violação das normas em vigor, não podendo acobertar, esconder ou ajudar a esconder violações de terceiros.

12. Não distribuir arquivos do tipo correntes ou manifestos, pois esses causam excessivo tráfego na rede.

13. Somente acessar outro computador conectado à rede se possuir autorização para tal ou se o serviço alvo permitir acesso público;

14. Não utilizar ou disponibilizar para fins particulares ou de recreação, serviços que sobrecarreguem as redes de computadores e ainda,que possam ir contra a ética, a moral e os bons costumes, tais como:

    - escuta de rádio,
    - páginas de animação,
    - jogos,
    - pedofilia,
    - pornografia,
    - músicas,
    - vídeo,
    - filmes,
    - software comercial ou

    outro que comprometa a imagem da Universidade.

15. Quando utilizar alguma rede de dados externa o usuário deve observar as suas normas.

16. Não interceptar ou tentar interceptar a transmissão de dados através da rede, exceto quando autorizado explicitamente pelo superior hierárquico, com prévio conhecimento do SeTIC.

17. Não desenvolver, manter, usar ou divulgar meios que possibilitem a violação da rede de computadores da Universidade.

18. Não colocar um hub ou switch em um ponto de rede para ampliar o número de pontos de rede da sala ou laboratório.

1.3.2 Responsabilidades do Administrador de Sistemas e Rede

Administradores de Rede e Sistemas têm a responsabilidade de proteger os direitos dos usuários, fixar políticas consistentes com estes direitos e levar ao conhecimento dos usuários estas políticas. Eles têm autoridade para controlar ou recusar acesso a qualquer um que violar estas políticas ou ameaçar os direitos de outros usuários; os administradores devem, sempre que possível, notificar os usuários afetados pelas suas decisões. Administradores de Redes e Sistemas são também usuários, e como tais, estão sujeitos às políticas estabelecidas pelo Laboratorio. Compete ao Administrador de Redes decidir sobre procedimentos locais referentes a:

- Espaço para armazenamento das mensagens recebidas
- Espaço para armazenamento das mensagens em folders pessoais
- Mensagens não lidas na caixa de entrada (mbox)

- Acúmulo de mensagens em conta
- Retenção de mensagens enviadas (sent) e mensagens descartadas (trash).
- Caso haja necessidade eminente, fazer uso de ferramentas para monitorar a rede da Unidade.
- Comunicar imediatamente ao SeTIC a ocorrência de invasões (hackers, lammers, crackers, etc), tomando as medidas de desconexão da rede e correção das falhas.
- Proteger os serviços de rede utilizando ferramentas apropriadas, como firewall, Proxy, Sistemas de Detecção de Intrusão, etc, desde que não seja no backbone redeUFSC, pois neste caso deve haver a prévia consulta SeTIC.
- Sugere-se que o administrador divida as redes muito grandes em subredes, cada uma protegida por um perímetro de segurança.
- Comunicar ao SeTIC a instalação ou adoção de redes Wireless.
- Consultar a SeTIC sobre a criação de VPNs.
- Bloquear os serviços desnecessários que possam comprometer o desempenho ou ir contra o código de ética ou qualquer item desta norma.
- Fazer a atualização de patches e erratas nos equipamentos de rede (switches, hubs e roteadores).
- Não fornecer a empresas ou instituições informações sobre número IP ou nome de usuários em caso de reclamação ou denúncia; a solicitação deve sempre ser feita por vias formais (ofícios, protocolados, etc).
- Limitar ao máximo a divulgação de informações de roteamento, faixa de IP, servidores, equipamentos de rede, entre outros, a terceiros.
- Não é permitido desenvolver, manter, usar ou divulgar meios que possibilitem a violação de rede de computadores da Universidade.

1.4 Regulamentação

A Instituição caracteriza como não ético e inaceitável e considera como motivo de ação disciplinar qualquer atividade através da qual um indivíduo:

1. Viole questões tais como direitos autorais ou proteção de patentes e autorizações da Instituição ou de terceiros, como também licenças de uso e outros contratos.
2. Interfira no uso correto dos recursos de informação.
3. Tente conseguir ou consiga acesso não autorizado a recursos de informação.
4. Sem autorização, destrói, altera, desmonta, desconfigura, impede o acesso de direito ou interfere na integridade dos recursos computacionais.
5. Sem autorização, invade a privacidade de indivíduos ou entidades que são autores, criadores, usuários ou responsáveis pelos recursos computacionais.
6. Remova dos recursos computacionais, algum documento de propriedade da Instituição ou por ela administrado, sem uma autorização específica.
7. Se faça passar por outra pessoa ou camufle sua identidade na utilização dos Recursos Computacionais com exceção dos casos em que o acesso anônimo é explicitamente permitido.
8. Viole ou tente violar os sistemas de segurança dos recursos computacionais, como quebrar ou tentar adivinhar identificação ou senhas de terceiros.
9. Intercepte ou tente interceptar transmissão de dados não destinados ao seu próprio acesso.

10. 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. As penalidades a serem aplicadas por infração a estas normas, sem prejuízo de outras aplicáveis previstas em normas e leis maiores, são redução ou eliminação, temporárias ou permanentes, de privilégios de acesso, tanto aos Recursos Computacionais, quanto às redes, salas de computadores e outros serviços ou facilidades.

Qualquer violação ou suspeita de violação dessas normas deve ser comunicada imediatamente ao responsável direto pelo recurso computacional no local onde o fato tenha ocorrido. Sempre que julgar necessário para a preservação da integridade dos Recursos Computacionais, dos serviços aos usuários ou dos dados, o Administrador de Redes poderá suspender temporariamente qualquer conta, seja o responsável pela conta suspeito de alguma violação, ou não.

O usuário suspeito de violação dessas normas deverá ser notificado da acusação e a ele cabe o direito de enviar o seu relato sobre os fatos até cinco dias após ser notificado da violação pelo representante da Unidade em que ocorreu o incidente. Ao ser notificado, o usuário deve ser informado desse direito.

2 Gerenciamento de Web Sites

A popularização da Internet, como meio de aquisição, tramitação e disseminação de informações, trouxe, além de inúmeros benefícios, a vulnerabilidade a ataques, invasões e intercepções, tanto em nível individual como em nível corporativo. Um intruso, ao invadir remotamente uma organização, poderá obter informações sensíveis e produzir danos irreparáveis, sem deixar vestígios. As publicações WEB são sem nenhuma duvida a mais importante maneira para a Instituição, publicar informação, interagir com seus usuários. Entretanto, caso não seja adotado regras rigorosas para configurar e operacionalizar estes site Web públicos, a Instituição torna-se vulnerável a uma grande variedade riscos de segurança. O estabelecimento de um ambiente propício e adequado à Segurança da Informação, vai muito além da simples aquisição de equipamentos e sistemas criptográficos. Depende, prioritariamente, da conscientização do público interno, que deve ter comportamento e atitudes favoráveis à segurança.

2.1 Elaboração de Páginas Eletrônicas

Cada departamento, laboratório ou grupo de pesquisa pode dispor de um Web Site na Internet, a fim de disponibilizar naquela rede, para o público interno e, quando for o caso, para o público em geral, informações e serviços por meio de um endereço eletrônico e da página eletrônica correspondente. Na elaboração de página eletrônica, a unidade institucional que cria o sítio Internet é responsável pela coerência, exatidão e pertinência das informações difundidas, bem como pela observância dos aspectos de segurança. Em nenhuma hipótese devem estar disponíveis, por meio de páginas eletrônicas, dados ou informações que possam comprometer a segurança orgânica , ou denegrir a imagem da Instituição ou deste departamento. Devem ser utilizados apenas programas aplicativos (“softwares”) adquiridos ou desenvolvidos pela unidade institucional, licenciados de acordo com a legislação vigente ou de domínio público, desde que homologados pelo SeTIC. Os seguintes passos são necessários para restringir o acesso para o conteúdo de um sítio na Internet e devem ser implementados pelo Administrador de Rede:

1. Dedicar um servidor (hardware) para hospedar o conteúdo do Web Site na Internet. Neste servidor dedicar um disco rígido, ou partição lógica para armazenar os arquivos do servidor Web, incluindo gráficos, imagens mas excluindo scripts e outros programas.

2. Definir um diretório exclusivo para todos os scripts externos ou programas executados como parte do conteúdo de uma página Web isto é CGI’s, Active Server Page (ASP), Hypertext Preprocessor (PHP).

3. Desabilitar a execução de scripts que não estejam exclusivamente sob o controle de contas administrativas.

4. Desabilitar o use de ligações simbólicas (hard , symbolic links).

5. Definir um conjunto de regras de acesso ao conteúdo Web, identificando a que diretórios e arquivos o conteúdo Web deve restringir-se e quais serão acessíveis pelos seus responsáveis.

3 Normas de Utilização do Correio Eletrônico

Esta publicação esclarece a aplicabilidade da lei e de outras políticas da Instituição referentes a correio eletrônico ou mensagens eletrônicas. Também define novos procedimentos onde as políticas já existentes não cobrem questões específicas relacionadas com correio eletrônico. Os serviços de correio eletrônico são oferecidos como um recurso profissional para apoiar alunos, docentes e funcionários no cumprimento de seus objetivos as áreas de educação, pesquisa, comunicação e serviços. O uso pessoal é permitido 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 política vigente na Instituição. Cada usuário é responsável por utilizar os serviços de correio eletrônico de maneira profissional, ética e legal. Material obtido de forma fraudulenta, racista, profano, obsceno, intimidador, difamatório, ilegal, ofensivo, abusivo ou inapropriado não pode ser enviado via correio eletrônico ou através de qualquer outra forma de comunicação eletrônica.

A Instituição, em geral, não pode e não tem por objetivo ser o árbitro do conteúdo de mensagens eletrônicas. Da mesma forma a Instituição não pode, em geral, impedir que os usuários recebam mensagens ofensivas. No entanto, os membros da comunidade são encorajados a utilizar no serviço de correio eletrônico, em acordo com a mesma ética aplicada a outras formas de comunicação.

3.1 Política

1. Convenção de identificação de mensagens Todos os usuários que possuírem uma conta de correio eletrônico possuem um nome padrão no formato "identificação_do_usuário@labeee.ufsc.br".

2. Representação Os usuários de mensagens eletrônicas não devem dar a impressão que estão representando, dando opiniões ou fazendo declarações em nome da Instituição ou qualquer outro Órgão da Instituição a menos que autorizado, implícita ou explicitamente. Onde apropriado, uma declaração explícita deve ser incluída, a menos que já esteja claro a partir do contexto, indicando que o autor não está representando a Instituição.

3. Mensagens sem identificação ou com identificação falsa (spoofing) Usuários não devem falsificar sua identidade ou o seu nome de usuário (username) ao utilizar o sistema de mensagens ou alterar a linha de origem da mensagem (From:) ou qualquer outra indicação da origem da mensagem. Comportamentos deste tipo violam a política de uso apropriado dos recursos computacionais.

4. Correntes de mensagens (chain letters) Usuários não devem iniciar ou reenviar mensagens encadeadas.

5. Listas de discussão Listas são criadas sob demanda sem a necessidade de consultar os usuários inseridos nas mesmas. No entanto, deve ser facultada ao usuário a opção de se desligar posteriormente.

6. Envio de mensagens inapropriadas (spamming) Usuários não devem enviar mensagens não solicitadas ou que não se referem a assuntos universitários, a pessoas com as quais não tenham relacionamentos pessoais.

7. Prevenção contra vírus Todo servidor deve ter um sistema de anti-vírus que deve ser mantido atualizado pelo administrador do servidor.

8. Privacidade de mensagens As mensagens transferidas para arquivos em computadores de uso pessoal ou para sistemas de mensagens, externos à Instituição, são cobertos por outras políticas e procedimentos.

9. Bloqueio de recebimento de mensagens O Administrador de Redes pode, sob certas circunstâncias, bloquear o recebimento de mensagens (por exemplo, spams). A inconveniência e possível ameaça contida em mensagens indesejáveis, provenientes de fontes comerciais ou não (bulk e-mail), pode

levar o Administrador de Redes a bloquear a recepção de mensagens provenientes de alguns locais da rede. Não é permitido o uso do conteúdo da mensagem ou da sua linha referente ao "assunto" (subject) para bloquear ou redirecionar a entrega de qualquer mensagem, exceto no caso de spams, ameaça de vírus ou outro conteúdo igualmente destrutivo.

10. Privacidade no acesso às mensagens As mensagens endereçadas para uma conta são entregues numa caixa de correio que pode ser acessada através de diversos programas (como Outlook, Webmail, Netscape, Eudora) sob o controle da senha da conta correspondente. O usuário é responsável por manter a confidencialidade desta senha, de acordo com as Normas de Uso Apropriado dos Recursos Computacionais.

11. Uso pessoal Os serviços de correio eletrônico podem ser utilizados episodicamente para propósitos pessoais desde que, além do que está exposto nesta política, tal uso não:

    - interfira direta ou indiretamente nas operações dos recursos computacionais e serviços de correio eletrônico da Instituição;
    - incorra em gastos adicionais para a Instituição;
    - interfira nas obrigações internas e externas da Instituição; ou
    - interfira na produtividade das atividades funcionais da Instituição.

3.2 Política

Na Instituição , mensagens eletrônicas e arquivos de computador são considerados de uso privativo e confidencial na forma permitida em lei. Primordialmente, o acesso a mensagens eletrônicas ou arquivos de computador requer permissão por parte do remetente da mensagem ou do dono do arquivo (a pessoa para a qual a identificação da conta está assinalada), de uma ordem judicial ou quaisquer outras ações definidas por lei. No caso de uma investigação da Instituição em função de acusações de má conduta de algum usuário, mensagens e arquivos podem ser bloqueados ou copiados para impedir a destruição ou perda de informações.

Os Administradores de Redes em suas Unidades poderão, sempre que necessário para preservar provas de usos indevidos ou diagnosticar problemas nos sistemas, efetuar cópias de segurança de arquivos de dados pessoais ou corporativos e investigar informações de caráter técnico como o percurso percorrido pela informação na Internet. Fica vedada a leitura do conteúdo, a não ser que efetuada com autorização judicial específica.

3.3 Regulamentação

A fim de preservar provas de eventuais usos indevidos dos recursos computacionais , os Administradores de Redes nas Unidades poderão fazer cópias de segurança de mensagens eletrônicas e arquivos em casos suspeitos sem, contudo, analisar os seus conteúdos. Poderão ser lidas apenas as informações que acompanham o invólucro da mensagem ou arquivo tais como remetente, horário de envio e trajeto percorrido.

Cabe também a este grupo, rastrear o trajeto de mensagens eletrônicas consideradas ofensivas ou abusivas pela instituição, a fim de determinar o ponto de origem da qual foi enviada.

4 REFERÊCIAS

LEIS: Legislação Pertinente Segurança da Informação. Disponível em:http://dsic.planalto.gov.br/documentos/quadro_legislacao.htm.
TIC-01: Normas de Uso Apropriado dos Recursos Computacionais na Instituição Estadual de Campinas.
TIC-04 : Privacidade de mensagens eletrônicas e arquivos de computador(UNICAMP).
TIC-05: Gerenciamento de Dados Corporativos(UNICAMP).
TIC-06: Correio Eletrônico (UNICAMP).
Portaria N° 121- EME, DE 12 DE Novembro DE 2001- exército Brasileiro.
PSEG00: Normas de Uso Apropriado dos Recursos Computacionais de Uso Apropriado dos Recursos Computacionais na Unives idade de São Paulo. Disponível em:http://www.security.usp.br/normas_pseg00.html.

TERMO DE COMPROMISSO

Eu, _____, portador do **CPF:** _____, declaro que recebi uma chave eletrônica (crachá) da sala do LabEEE (Laboratório de Eficiência Energética em Edificações), sala 112, do bloco B do departamento de engenharia civil da UFSC, no **dia** ____ de _____de _____.

Declaro estar ciente da responsabilidade de zelar pelo patrimônio abrigado dentro do laboratório, incluindo equipamentos de pesquisa e informática, além de móveis e materiais de consumo, e estou disposto a arcar com as devidas conseqüências no caso de danos provocados pelo mau uso das instalações do LabEEE. Também estou ciente da política de acesso a internet e das penalidades para utilização indevida da rede de computadores da UFSC.

Declaro também que as chaves confiadas a mim serão apenas por mim utilizadas, para fins de pesquisa relacionada ao meu plano de trabalho ou projeto de pesquisa vinculado ao laboratório, sob orientação do **professor** _____.

DADOS DO ALUNO

Endereço atual:

Rua: _____nº_____

Bairro: _____ Cidade: _____CEP: _____-___

Telefones para contato: (cel)_____(res)_____

Email:_____

Matrícula da UFSC: _____

Assinatura do aluno: _____

Assinatura do orientador: _____

Florianópolis, ___ de _____ de _____.

Crachá nº: _____