



Faculdade
Politécnica

POLÍTICA DE SEGURANÇA DA
INFORMAÇÃO
FACULDADE POLITÉCNICA

Autor: José Roberto Brasil
Uberlândia – fevereiro 2009

ÍNDICE

Resumo	02
1 Introdução.....	03
2 Objetivos da política de segurança	03
3 Política de segurança da estrutura de informática.....	04
4 Política de utilização da rede	04
4.1 Regras gerais e básicas de segurança	04
4.2 Regras para funcionários.....	05
4.3 Regras para alunos.....	06
5 Política de administração de contas.....	06
5.1 Regras gerais.....	06
5.2 Regras para funcionários.....	06
5.3 Regras para alunos.....	07
6 Política de senhas.....	08
6.1 Regras gerais.....	08
7 Política de utilização de e-mail e antivírus.....	09
7.1 Regras gerais.....	09
7.2 Regras para funcionários.....	10
8 Política de acesso a Internet	10
8.1 Regras gerais.....	10
8.2 Regras para funcionários.....	11
9 Política de uso das estações de trabalho	11
9.1 Regras gerais.....	11
10 Política de uso de impressoras	12
10.1 Regras gerais.....	12
11 Política de segurança física	12
11.1 Política de controle de acesso.....	12
11.2 Regras gerais.....	13
12 Política de mesa limpa e tela limpa.....	13
12.1 Regras gerais.....	13
13 Política de utilização de laboratórios de informática.....	14
13.1 Regras gerais.....	14
14 Termo de compromisso.....	14
15 Verificação da utilização da política.....	15
16 Violação da política, advertência e punições.....	15
16.1 Regras para funcionários.....	15
16.2 Regras para alunos.....	16
17 Anexos.....	16

RESUMO

Este trabalho aborda um estudo sobre política de segurança da informação, uma das principais medidas de segurança adotadas pelas organizações. Atualmente, algumas metodologias e melhores práticas em segurança da informação têm sido aplicadas, dentre elas, a NBR ISO 17799, tradução da BS7799. A referida norma foi utilizada neste projeto, pela qual será possível verificar o que devemos seguir para a elaboração de uma política de segurança da informação. Há necessidade de envolvimento de toda a Instituição, pois esta proposta de política de segurança da informação atenderá todos os setores da Faculdade Politécnica.

1- INTRODUÇÃO

O presente trabalho tem como objetivo fazer um estudo aprofundado sobre segurança da informação, detalhando este estudo sobre uma das medidas de segurança que é a política de segurança da informação.

Atualmente, a informação tornou-se o ativo mais valioso das grandes empresas, ao mesmo tempo que passou a exigir uma proteção mais adequada.

De forma assustadoramente crescente, os sistemas de informações e as redes de computadores das organizações apresentam-se diante de uma série de ameaças, ameaças estas que podem resultar em prejuízos para as empresas e continuidade do negócio.

Esta segurança é obtida a partir da implementação de uma série de controles, que podem ser políticas, práticas e procedimentos, os quais precisam ser estabelecidos para garantir que os objetivos de segurança específicos da organização sejam atendidos.

A dificuldade de entender a importância da segurança da informação ainda é muito grande. Muitas empresas começam a pensar na implantação de medidas de segurança após terem sofrido prejuízos decorrente de algum tipo de incidente relacionado à segurança.

A política de segurança de uma empresa é, por certo, o documento mais importante em um sistema de gerenciamento de segurança da informação. Seu objetivo é normatizar as práticas e procedimentos de segurança da empresa. Isso significa que deve ser simples, objetiva, de fácil compreensão e aplicação. Os controles de segurança, de um modo geral, e a política, em particular, devem ser definidos para garantir um nível de segurança coerente com o negócio da empresa. Esta política pode trazer ao ambiente de uma instituição de ensino regras e procedimentos que devem ser seguidos para a garantia da segurança da informação. É importante que as informações da política de segurança sejam divulgadas para todos os membros da Instituição, sejam alunos, e/ou funcionários, conscientizando-os da importância do seguimento desta política.

2- OBJETIVOS DA POLÍTICA DE SEGURANÇA

O objetivo é garantir que os recursos de informática e a informação estarão sendo usados de maneira adequada. O usuário deve conhecer todas as regras para utilização da informação de forma segura, evitando a exposição de qualquer informação que possa prejudicar a Instituição de Ensino, os funcionários e/ou alunos.

3 - POLÍTICA DE SEGURANÇA DA ESTRUTURA DE INFORMÁTICA

A Política de Segurança da estrutura de informática abrange itens relacionados à segurança da informação e à utilização desta estrutura, sendo contempladas: política de utilização da rede, administração de contas, senhas, e-mail, antivírus, acesso à Internet, uso das estações de trabalho, e utilização de impressoras.

4 - POLÍTICA DE UTILIZAÇÃO DA REDE

Esse tópico visa definir as normas de utilização da rede que abrange o login, manutenção de arquivos no servidor e tentativas não autorizadas de acesso. Esses itens serão abordados para orientação a todos os usuários dos sistemas e da rede de computadores da Faculdade Politécnica.

4.1 REGRAS GERAIS E BÁSICAS DE SEGURANÇA

- Não são permitidas tentativas de obter acesso não autorizado, tais como, tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta. Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se a servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes.
- Não são permitidas tentativas de interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques, tentativas de provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de "quebrar" (invadir) um servidor.
- Antes de ausentar-se do local de trabalho, o usuário deverá bloquear sua estação de trabalho.
- O usuário deve fazer manutenção no diretório pessoal, evitando acúmulo de arquivos desnecessários.
- Material de natureza pornográfica e racista não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede.
- Jogos ou qualquer tipo de software/aplicativo não podem ser gravados ou instalados no diretório pessoal do usuário, no computador local e em qualquer outro diretório da rede; podem ser utilizados apenas os softwares previamente instalados no computador.
- Não é permitido criar e/ou remover arquivos fora da área alocada ao usuário e/ou que venham a comprometer o desempenho e funcionamento dos sistemas. As áreas de armazenamento de arquivos são designadas conforme mostra a tabela abaixo:

Compartilhamento	Utilização
Diretório pessoal (Z:)	Arquivos pessoais de responsabilidade do usuário, dono deste diretório pessoal.
Diretório público (X:)	Arquivos de compartilhamento geral, para todos os funcionários.

- A pasta PÚBLICA ou similar não deverá ser utilizada para armazenamento de arquivos que contenham assuntos sigilosos; devem ser armazenadas apenas informações comuns a todos.
- Não é permitido gravar arquivos de vídeo e áudio no servidor de arquivos. Isso tanto no servidor administrativo, quanto no laboratório.
- Haverá limpeza semestral dos arquivos armazenados na pasta PÚBLICO, para que não haja acúmulo desnecessário de arquivos.
- É proibida a instalação ou remoção de softwares que não for devidamente acompanhada pelo departamento técnico, através de solicitação via e-mail, e deve conter autorização do coordenador da área do solicitante.
- Não são permitidas alterações das configurações de rede e inicialização das máquinas, bem como modificações que possam trazer algum problema futuro.

GLOSSÁRIO

Cracking: é o nome dado a ações de modificações no funcionamento de um sistema, de maneira geralmente ilegal, para que determinados usuários ganhem algo com isso.

4.2 REGRAS PARA FUNCIONÁRIOS

- É obrigatório armazenar os arquivos inerentes à empresa no servidor de arquivos, para garantir a cópia de segurança dos mesmos.
- É proibida a abertura de computadores para qualquer tipo de reparo, seja isso feito em departamentos ou laboratórios de informática. O reparo só pode se dar através do departamento técnico.
- A utilização de equipamentos de informática particulares deverá ser comunicada pelo funcionário à coordenação de seu departamento.
- Quando um funcionário é transferido entre departamentos, o coordenador deve informar a equipe de TI, e se informar sobre qual modificação necessária que deverá ser feita para sua nova função.
- Quando ocorrer a demissão do funcionário, o coordenador responsável deve informar a equipe técnica para a imediata desativação dos acessos do usuário a

qualquer recurso da rede. Deve-se verificar a necessidade de troca de senhas de contas de uso comum ao departamento, evitando o acesso às informações.

4.3 REGRAS PARA ALUNOS

Semestralmente, todo o conteúdo das contas de usuário do domínio LABPOLI é deletado.

A cada final de semestre, o(s) aluno(s) e/ou professor(es) (que) desejar(em) manter suas informações, deverá(ão) providenciar a cópia dos arquivos, eis que todo o conteúdo das contas de usuário do domínio LABPOLI será deletado.

5- POLÍTICA DE ADMINISTRAÇÃO DE CONTAS

Este tópico visa definir as normas de administração das contas, abrangendo: criação, manutenção e desativação da conta. Esta política será dividida por usuários para facilitar o entendimento de todos.

5.1 REGRAS GERAIS

Desativação da conta:

- É reservado o direito de desativar uma conta de usuário, por parte da equipe de TI da Faculdade Politécnica, caso se verifique a ocorrência de algum dos critérios abaixo especificado:

- ✓ Incidentes suspeitos de quebra de segurança nas contas dos usuários.
- ✓ Mau uso do computador de trabalho.

Ex: Acessar sites pornográficos, navegar na Internet constantemente.

5.2 REGRAS PARA FUNCIONÁRIOS

Todo funcionário da Faculdade Politécnica poderá ter uma conta para acesso aos recursos da rede nos computadores da Instituição. Os acessos a demais sistemas devem ser informados pelo coordenador da área no momento da solicitação da conta do usuário. Para solicitação da conta para novos funcionários, os coordenadores devem proceder da maneira detalhada abaixo.

Criação de contas:

- A solicitação para criação da conta é de competência do coordenador de departamento a que o funcionário estiver vinculado e deverá ser formalizada pelo e-mail ti@facpoli.edu.br, contendo:
- o nome, função e os acessos que serão necessários para este usuário;

- criação de uma conta para acesso ao domínio ADMPOLI, acesso ao sistema de ERP – RM Sistemas, e criação da conta de email.

Administração da conta:

Criada a conta, o funcionário, individualmente, terá um espaço no servidor para gravar seus arquivos pessoais, sendo copiados, diariamente, os arquivos do servidor do domínio ADMPOLI.

- As contas podem ser monitoradas pela equipe de TI, com o objetivo de verificar possíveis irregularidades no armazenamento, ou manutenção dos arquivos nos diretórios pessoais.

5.3 REGRAS PARA ALUNOS

Todo aluno da Faculdade Politécnica poderá ter uma conta para acesso aos recursos da rede de computadores, sendo que usará o domínio LABPOLI, com limite de armazenamento de arquivos em seu diretório pessoal.

A necessidade de um espaço maior para armazenamento dos arquivos nos diretórios pessoais deve ser informada pelo professor à equipe de TI.

Criação de contas:

- A criação da conta do aluno é de responsabilidade do administrador de redes. A cada semestre, as informações das contas dos alunos são deletadas e criados os usuários dos alunos matriculados na Instituição.
- A criação de conta de acesso à rede de computadores deverá ser requerida pelo aluno, diretamente, à equipe de TI .
- No momento da abertura da conta, a equipe de TI criará a senha dos alunos. Esta senha poderá ser alterada quando o usuário utilizar sua conta, sendo importante seguir as regras para criação de senhas que estão detalhadas neste documento.

Administração da conta:

- Cada aluno que tiver sua conta terá um espaço no servidor para gravar seus arquivos pessoais;
- As contas podem ser monitoradas pela equipe de TI, com o objetivo de verificar possíveis irregularidades no armazenamento, ou manutenção dos arquivos nos diretórios pessoais.
- Diariamente, será emitida cópia de segurança dos arquivos do servidor do domínio LABPOLI.

6- POLÍTICA DE SENHAS

As senhas são utilizadas pela grande maioria dos sistemas, e necessárias como meio de autenticação. Porém, elas são consideradas perigosas, pois dependem do usuário, que pode, por exemplo, escolher senhas óbvias e fáceis de serem descobertas, ou ainda compartilhá-las com seus amigos.

6.1 REGRAS GERAIS

- A senha deve ser redefinida a cada três meses, para os usuários. As senhas devem ser bloqueadas após 5 tentativas sem sucesso, devendo o administrador de redes e o usuário serem notificados sobre estas tentativas.
- As responsabilidades do administrador do sistema incluem o cuidado na criação e alteração das senhas dos usuários, além de manter atualizados os dados dos mesmos.
- As responsabilidades do usuário incluem, principalmente, os cuidados para a manutenção da segurança dos recursos, tais como, sigilo da senha e o monitoramento de sua conta, evitando sua utilização indevida. As senhas são sigilosas, individuais e intransferíveis, não podendo ser divulgadas em nenhuma hipótese.
- Tudo o que for executado com a sua senha de usuário da rede, ou de outro sistema será de inteira responsabilidade do usuário, por isso a necessidade de todo o cuidado de se manter a senha secreta.
- A Request for Comments (RFC) 2196, que é um guia para desenvolvimento de políticas de segurança de computador comenta sobre como selecionar e manter senhas.

As senhas são efetivas apenas quando usadas corretamente, e requerem alguns cuidados na sua escolha e uso, como:

- ✓ Não utilize informações pessoais fáceis de serem obtidas, como o número de telefone, nome da rua, nome do bairro, cidade, data de nascimento, etc.
- ✓ Não utilize senhas somente com dígitos ou com letras.
- ✓ Utilize senha com, pelo menos, oito caracteres.
- ✓ Misture caracteres maiúsculos e minúsculos.
- ✓ Misture números, letras e caracteres especiais.
- ✓ Utilize um método próprio para lembrar-se da senha, de modo que ela não precise ser escrita em nenhum local, em hipótese alguma.
- ✓ Não anote sua senha em papel, ou em outros meios de registro de fácil acesso.
- ✓ Não utilize o nome do usuário.
- ✓ Não utilize o primeiro nome, o nome do meio ou o sobrenome.

- ✓ Não utilize nomes de pessoas próximas, como do(a) esposo(a), dos filhos, de amigos.
- ✓ Não forneça sua senha para ninguém, por razão alguma.
- ✓ Utilize senhas que podem ser digitadas rapidamente, sem a necessidade de olhar para o teclado.

7- POLÍTICA DE UTILIZAÇÃO DE E-MAIL E ANTIVÍRUS

Esse tópico visa definir as normas de utilização de e-mail e antivírus que engloba o envio, recebimento e gerenciamento das contas de e-mail.

Todos os usuários de e-mail devem tomar ciência que a Internet opera em domínio público, que foge do controle da equipe técnica da Faculdade Politécnica. As mensagens podem estar sujeitas a demora e serviços potencialmente não confiáveis.

Grande parte da comunicação do dia-a-dia passa através de e-mails. Mas é importante lembrar que grande parte das pragas eletrônicas atuais chega por esse meio. Os vírus atuais são mandados automaticamente. Isso não significa que um e-mail de um cliente, parceiro ou amigo foi mandado necessariamente pelo mesmo. Nosso servidor de e-mail está protegido contra vírus e códigos maliciosos, mas algumas atitudes do usuário final são importantes. Para isso, é importante que algumas regras sejam obedecidas.

7.1 REGRAS GERAIS

- O e-mail deve ser utilizado de forma consciente, evitando qualquer tipo de perturbação a outras pessoas, seja através da linguagem utilizada, frequência ou tamanho das mensagens.
- É proibido o envio de grande quantidade de mensagens de e-mail (spam) que, de acordo com a capacidade técnica da rede, seja prejudicial ou gere reclamações de outros usuários.
- Evite mandar e-mail para mais de 10 (dez) pessoas de uma única vez. É proibido o envio de e-mail mal-intencionado, tais como, **mail bombing** ou sobrecarregar um usuário, site ou servidor com e-mail muito extenso ou numerosas partes de e-mail.
- É obrigatória a manutenção da caixa de e-mail, evitando acúmulo de e-mails e arquivos inúteis.
- É obrigatória a utilização do programa Outlook 2003, para ser o cliente de email.
- É obrigatória a utilização do programa Trend Office Scan, para ser o cliente de antivírus.
- Para certificar-se de que a mensagem foi recebida pelo destinatário, deve-se, se

necessário, utilizar procedimentos de controles extras para verificar a chegada da mensagem. Devem ser solicitadas notificações de recebimento e leitura.

Não execute ou abra arquivos anexados enviados por emitentes desconhecidos ou suspeitos.

- Não abra arquivos anexados com as extensões .bat, .exe, .src, .lnk e .com, se não tiver certeza absoluta de quem solicitou este email.
- Desconfie de todos os emails com assuntos estranhos e/ou em inglês. Alguns dos vírus mais terríveis dos últimos anos tinham assuntos como: ILOVEYOU, Branca de neve, pornô, etc.
- Evite anexos muito grandes.

GLOSSÁRIO

Mail bombing: Excesso de mensagens enviadas a uma caixa postal, a ponto de congestionar o tráfego do provedor. Mensagem enviada a uma caixa postal que, em consequência de sua grande extensão, trava o computador.

7.2 REGRAS PARA FUNCIONÁRIOS

- Não utilize o email da Faculdade Politécnica para fins pessoais.
- É obrigatória a utilização de assinatura nos e-mails, seguindo padrão a ser estabelecido pela Faculdade Politécnica.

8- POLÍTICA DE ACESSO A INTERNET

Esse tópico visa definir as normas de utilização da Internet, que engloba a navegação a sites, downloads e uploads de arquivos.

A Internet é uma ferramenta de trabalho e deve ser usada para este fim pelos funcionários e alunos da Faculdade Politécnica. Não é permitido o seu uso para fins recreativos durante o horário de trabalho ou de aula.

8.1 REGRAS GERAIS

- É proibida a divulgação de informações confidenciais da Faculdade Politécnica em grupos de discussão, listas ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida, sendo passível sofrer as penalidades previstas nas políticas de procedimentos internos e/ou na forma da lei.
- São bloqueados arquivos que comprometam o uso de banda ou perturbem o bom andamento dos trabalhos.
- São bloqueados domínios que comprometam o uso de banda ou perturbem o bom andamento dos trabalhos.

- É obrigatória a utilização do programa Internet Explorer para ser o cliente de navegação de Internet.
- Não será permitido software de comunicação instantânea, como Windows Messenger - MSN.
- Não será permitida a utilização de softwares peer-to-peer (P2P), tais como, Kazaa, Morpheus, LimeWire , entre outros.
- O acesso a sites com conteúdo pornográfico, jogos e bate-papo são bloqueados e as tentativas de acesso serão monitoradas.
- Não será permitida a utilização de serviços de streaming, tais como, rádios on-line, usina do som, entre outros.

8.2 REGRAS PARA FUNCIONÁRIOS

- Haverá geração de relatórios dos sites acessados por usuário, e, se necessário, a publicação desse relatório e prestação de contas dos acessos pelo usuário.
- Os funcionários com acesso à Internet podem baixar somente programas ligados diretamente às atividades da empresa e devem providenciar o que for necessário para regularizar a licença e o registro desses programas.

9-POLÍTICA DE USO DAS ESTAÇÕES DE TRABALHO

Cada estação de trabalho possui códigos internos, os quais permitem que ela seja identificada na rede. Sendo assim, tudo que for executado na estação de trabalho será de responsabilidade do usuário. Por isso, sempre que sair de frente da estação de trabalho, tenha certeza que efetuou o logoff ou bloqueou a estação de trabalho.

9.1 REGRAS GERAIS

- Não utilize nenhum tipo de software/hardware sem autorização da equipe técnica.
- Mantenha nas estações de trabalho somente o que for supérfluo ou pessoal. Todos os dados relativos à Faculdade Politécnica devem ser mantidos no servidor, onde existe sistema de backup diário e confiável.
- Não é permitido gravar, nas estações de trabalho, softwares com direitos autorais ou qualquer outro tipo que possa ser considerado pirataria.
- Os arquivos gravados em diretórios temporários das estações de trabalho podem ser acessados por todos os usuários que utilizarem a mesma, portanto não se pode garantir sua integridade e disponibilidade. Estes arquivos poderão ser alterados ou excluídos sem prévio aviso e por qualquer usuário que acessar a estação.

10- POLÍTICA DE USO DE IMPRESSORAS

Esse tópico visa definir as normas de utilização de impressoras disponíveis nos departamentos da Faculdade Politécnica. Esta política é aplicada somente a funcionários que utilizam impressoras em seus departamentos, visto que, nos laboratórios de informática, não existem impressoras instaladas.

10.1 REGRAS GERAIS

- Ao mandar imprimir, verifique na impressora se o que foi solicitado já está impresso.
- Se houver erro na impressão, reaproveite o papel na sua próxima tentativa, recolocando-o na bandeja de impressão. Se o papel servir para rascunho, leve para sua mesa. Se o papel não servir para mais nada, jogue no lixo.
- Não é permitido deixar impressões erradas na mesa das impressoras, na mesa das pessoas próximas a ela e tampouco sobre o gaveteiro.
- Se a impressora emitir alguma folha em branco, recoloque-a na bandeja.
- Se você notar que o papel de alguma das impressoras está no final, reabasteça-a. Isso evita que você e outras pessoas tenham seus pedidos de impressão prejudicados, e evita acúmulo de trabalhos na fila de impressão.
- Utilize a impressora colorida somente para versão final de trabalhos, e não para testes ou rascunhos.
- Não será permitida a impressão de documentos pessoais nas impressoras da instituição.

11- POLÍTICA DE SEGURANÇA FÍSICA

O objetivo desta política é prevenir o acesso não autorizado, dano e interferência às informações e instalações físicas da organização. A segurança física dos equipamentos de informática e das informações da empresa deve ser protegida de possíveis danos. Aqui será abordada a segurança física dos laboratórios de informática, das instalações de TI, dos equipamentos no geral e procedimentos para garantir a segurança física.

11.1 POLÍTICA DE CONTROLE DE ACESSO

Existem áreas que merecem maior atenção quanto ao controle da entrada de pessoas. Estas áreas são departamentos que contêm informações ou equipamentos que devem ser protegidos, como, por exemplo: sala de servidores, departamento financeiro, sala de coordenadores e diretores, entre outras.

As instalações da equipe de TI devem minimizar acesso público direto, riscos ao fornecimento de energia e serviços de telecomunicações.

11.2 REGRAS GERAIS

- Apenas pessoas autorizadas podem acessar as instalações da equipe de TI, devendo os funcionários usarem crachás de identificação.
- Nos departamentos que tratam com informações confidenciais de alunos, como, por exemplo, documentação, informações financeiras, acadêmicas, o acesso deve ser permitido somente para pessoas autorizadas.
- A temperatura, umidade e ventilação das instalações que abrigam equipamentos de informática e de comunicações devem estar de acordo com os padrões técnicos especificados pelos fabricantes dos equipamentos.
- Se acontecer a perda de chaves de departamentos ou laboratórios, a coordenação responsável deve ser informada imediatamente, para que possa providenciar a troca da fechadura e das cópias da chave perdida.

12- POLÍTICA DE MESA LIMPA E TELA LIMPA

A política de mesa limpa deve ser considerada para os departamentos e utilizada pelos funcionários da Faculdade Politécnica, de modo que papéis e mídias removíveis não fiquem expostos a acessos não autorizados.

A política de tela limpa deve considerar que, se o usuário não estiver utilizando a informação, ela não deve ficar exposta, reduzindo o risco de acesso não autorizado e evitando perda e danos à informação.

12.1 REGRAS GERAIS

- Os papéis ou mídias de computador não devem ser deixados sobre as mesas; quando não estiverem sendo usados, devem ser guardados de maneira adequada, de preferência, em gavetas ou armários trancados.
- O ambiente dos departamentos devem ser mantidos limpos, sem caixa ou qualquer outro material sobre o chão, de modo que possa facilitar o acesso de pessoas que estiverem no departamento.
- Sempre que não estiver utilizando o computador, não deixar nenhum arquivo aberto, de modo que as informações possam ser visualizadas por outras pessoas que estiverem no departamento.
- Agendas, livros ou qualquer material que possam ter informações sobre a empresa ou informações particulares devem sempre ser guardados em locais fechados, evitando o acesso de terceiros (ou pessoas não autorizadas).
- Chaves de gavetas, armários, de portas de acesso a departamentos, de laboratórios de informática devem ser guardadas em lugar adequado; não devem ser deixadas sobre a mesa ou guardadas com o professor/funcionário.

13- POLÍTICA DE UTILIZAÇÃO DE LABORATÓRIOS DE INFORMÁTICA

Para utilização de laboratórios e equipamentos de informática, algumas regras devem ser cumpridas, para que possa ser feito o uso correto das instalações, evitando qualquer tipo de dano a equipamentos em laboratórios que possam prejudicar a utilização dos mesmos.

13.1 REGRAS GERAIS

- O acesso a laboratórios de informática deve ser controlado, somente sendo permitido o uso dos mesmos com o acompanhamento de um funcionário responsável.
- É de responsabilidade do professor/funcionário que utilizou o laboratório zelar pela ordem das instalações. Sendo necessário qualquer tipo de manutenção, a equipe técnica deve ser informada.
- No momento em que entrar no laboratório, o funcionário responsável deve verificar se todos os computadores estão funcionando corretamente. Se detectado qualquer problema, a equipe técnica deve ser informada, para que a solução possa ser providenciada o mais rápido possível.
- Alimentos, bebidas, fumo e o uso de telefones celulares são proibidos nos laboratórios.
- As chaves dos laboratórios devem ficar guardadas em locais cujo acesso seja controlado.
- É necessária a reserva do laboratório para garantir sua disponibilidade.

14- TERMO DE COMPROMISSO

O termo de compromisso é utilizado para que os funcionários e alunos se comprometam formalmente a seguir a política de segurança, tomando ciência das punições impostas ao seu não cumprimento.

No termo de compromisso, serão reforçados os principais pontos da política de segurança. O documento deve ser assinado por todos os funcionários, e será renovado sempre que necessário. O anexo II é um modelo de termo de compromisso.

15- VERIFICAÇÃO DA UTILIZAÇÃO DA POLÍTICA

Para garantir as regras mencionadas acima, a Faculdade Politécnica se reserva no direito de:

- Implantar softwares e sistemas que podem monitorar e gravar todos os usos de Internet através da rede e das estações de trabalho da empresa.
- Inspeccionar qualquer arquivo armazenado na rede, tanto no disco local da estação ou nas áreas privadas da rede, visando assegurar o rígido cumprimento desta política.

- Foram instalados uma série de softwares e hardwares para protegerem a rede interna e garantir a integridade dos dados e programas, incluindo um firewall, que é a primeira, mas não a única barreira entre a rede interna e a Internet.

16- VIOLAÇÃO DA POLÍTICA, ADVERTÊNCIA E PUNIÇÕES

Ao detectar uma violação da política, o primeiro passo é determinar a sua razão, ou seja, verificar se a violação pode ter ocorrido por negligência, acidente ou erro, por desconhecimento da política ou por ação previamente determinada, ignorando a política estabelecida. Um processo de investigação deve determinar as circunstâncias da violação, como e porque ela ocorreu.

Nos termos da Política, a Faculdade Politécnica procederá ao bloqueio do acesso ou o cancelamento do usuário caso seja detectado uso em desconformidade com o que foi estabelecido ou de forma prejudicial à rede.

É recomendado o treinamento dos usuários em segurança da informação, como forma de conscientização e divulgação da política de segurança a ser seguida por todos. O programa de treinamento em segurança deve fazer parte do programa de integração de novos funcionários e do programa de integração de novos alunos (ao início de cada ano letivo), devendo ser feitos treinamentos de reciclagem para os funcionários mais antigos.

16.1 REGRAS PARA FUNCIONÁRIOS

Caso seja necessário advertir o funcionário, o departamento de Recursos Humanos será informado a fim de interagir e manter-se informado da situação.

O não cumprimento, pelo funcionário, das normas estabelecidas neste documento, seja isolada ou acumulativamente, poderá causar, de acordo com a infração cometida, as seguintes punições: Comunicação de descumprimento, Advertência ou suspensão, Demissão por justa causa.

Comunicação de descumprimento: Será encaminhado ao funcionário, por e-mail, comunicado informando o descumprimento da norma, com a indicação precisa da violação praticada. Cópia desse comunicado permanecerá arquivada junto ao Departamento de Recursos Humanos na respectiva pasta do funcionário.

Advertência ou suspensão: A pena de advertência ou suspensão será aplicada, por escrito, somente nos casos de natureza grave ou na hipótese de reincidência na prática de infrações de menor gravidade.

Demissão por justa causa: Nas hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, conforme anexo I.

Fica desde já estabelecido que a Diretoria, no uso do poder diretivo e disciplinar que lhe é atribuído, poderá aplicar a pena que entender devida.

16.2 REGRAS PARA ALUNOS

Caso seja necessário advertir o aluno, a coordenação de curso será informada para interagir e manter-se informada da situação.

O não cumprimento pelo aluno, das normas estabelecidas neste documento, seja isolada ou acumulativamente, poderá causar, de acordo com a infração cometida, as punições estabelecidas no **GUIA DE ORIENTAÇÃO ACADÊMICA PARA ALUNO**, disponível no site da faculdade <http://www.facpoli.edu.br>, e no **REGIMENTO ESCOLAR**, disponível na biblioteca.

17- ANEXOS

ANEXO I – ARTIGO 482 DA CLT

ANEXO II – MODELO TERMO DE COMPROMISSO

Anexo I – Artigo 482 da CLT (Consolidação das Leis do Trabalho)

Art. 482. Constituem justa causa para rescisão do contrato de trabalho pelo empregador:

- a) ato de improbidade.
- b) incontinência de conduta ou mau procedimento.
- c) negociação habitual por conta própria ou alheia sem permissão do empregador, e quando constituir ato de concorrência à empresa para a qual trabalha o empregado, ou for prejudicial ao serviço.
- d) condenação criminal do empregado, passada em julgado, caso não tenha havido suspensão da execução da pena.
- e) desídia no desempenho das respectivas funções.
- f) embriaguez habitual ou em serviço.
- g) violação de segredo da empresa.
- h) ato de indisciplina ou de insubordinação.
- i) abandono de emprego.
- j) ato lesivo da honra ou da boa fama praticado no serviço contra qualquer pessoa, ou ofensas físicas, nas mesmas condições, salvo em caso de legítima defesa, própria ou de outrem.
- k) ato lesivo da honra ou da boa fama ou ofensas físicas praticadas contra o empregador e superiores hierárquicos, salvo em caso de legítima defesa, própria ou de outrem.
- l) prática constante de jogos de azar.

Parágrafo único. Constitui igualmente justa causa para dispensa de empregado a prática, devidamente comprovada em inquérito administrativo, de atos atentatórios à segurança nacional.

Anexo II – Termo de Compromisso

TERMO DE COMPROMISSO

Identificação do Colaborador/Aluno

NOME:	
MATRÍCULA:	

Comprometo-me a:

1. Executar minhas tarefas de forma a cumprir com as orientações da Política de Segurança e com as Normas e Padrões vigentes.
2. Utilizar adequadamente os equipamentos da Instituição, evitando acessos indevidos aos ambientes computacionais aos quais estarei habilitado, e que possam comprometer a segurança das informações.
3. Não revelar, fora do âmbito profissional, fato ou informações de qualquer natureza de que tenha conhecimento devido às minhas atribuições, salvo em decorrência de decisão competente do superior hierárquico.
4. Acessar as informações somente por necessidade de serviço e por determinação expressa do superior hierárquico.
5. Manter cautela quando da exibição de informações sigilosas e confidenciais, em tela, impressoras ou outros meios eletrônicos.
6. Não me ausentar do local de trabalho sem encerrar a sessão de uso do computador ou sistema, evitando assim o acesso por pessoas não autorizadas.
7. Observar rigorosamente os procedimentos de segurança estabelecidos quanto à confidencialidade de minha senha, através dos quais posso efetuar operações a mim designadas nos recursos computacionais que acesso, assim procedendo:
 - a. Substituir a senha inicial gerada pelo sistema, por outra secreta, pessoal e intransferível.
 - b. Não divulgar a minha senha a outras pessoas.
 - c. Nunca escrever a minha senha, sempre memorizá-la.
 - d. De maneira alguma, ou sob qualquer pretexto, procurar descobrir as senhas de outras pessoas.
 - e. Somente utilizar o meu acesso para os fins designados, e para os quais estiver devidamente autorizado, em razão de minhas funções.

f. Responder em todas as instâncias pelas conseqüências das ações ou omissões de minha parte, que possam pôr em risco ou comprometer a exclusividade de conhecimento da minha senha ou das transações a que tenho acesso.

g. Reportar imediatamente ao superior imediato ou ao Administrador de Segurança em caso de violação, acidental ou não, da minha senha, e providenciar a sua substituição.

h. Solicitar o cancelamento de minha senha, quando não for mais de minha utilização.

Estou ciente da existência da "**Política de Segurança da Informação da Faculdade Politécnica**" e da minha responsabilidade em cumprir as normas e regras contidas nessa Política.

Uberlândia, _____ de _____ de _____.

Assinatura do Colaborador/Aluno