

DTI – ANIMA Educação

Política de Segurança de Informações e uso de recursos computacionais

Normas e procedimentos de utilização de recursos tecnológicos

Acadêmico



2010

POLÍTIAS DO DEPARTAMENTO DE TECNOLOGIA		
 <p>Ănima E D U C A Ç Ã O</p>	<p>Segurança de Informações e Utilização de Recursos Computacionais</p>	<p>Elaborado em: 28/04/2010</p> <p>Revisado em: 26/07/2010</p> <p>Aprovado em: 16/08/2010</p>
<p>Elaborado por:</p> <p>DTI:</p> <ul style="list-style-type: none">• Edson Eduardo S. Santos (DTI ĂNIMA)• Tiago Campos Carrusca (DTI ĂNIMA)		
<p>Revisado por:</p> <ul style="list-style-type: none">• Heleno Carlos Fernandes (jurídico ĂNIMA)• Maria Elisabeth Ferraz (Diretoria Acadêmica ĂNIMA)		
<p>Aprovado por:</p> <ul style="list-style-type: none">• Bruno Henrique de Macedo Machado (DTI ĂNIMA)• Cristiane Lima Gatti Guimarães (Gestão de Pessoas UNA)• Elisete Helena Goncalves (Gestão de Pessoas UNIMONTE)• Flavio Korn (Diretor de Serviços ĂNIMA)• Lícia Boechat Assbú Janones (Gestão de Pessoas ĂNIMA)• Luis Alberto Rocha Benfica (Jurídico ĂNIMA)• Manoella Vasconcellos Costa (Gestão de Pessoas UNIBH)		

Sumário

I.	Introdução.....	
	a) Por que é necessária a segurança de informações.....	
II.	Objetivo.....	4
III.	Aplicação.....	4
IV.	Princípios.....	4
V.	Responsabilidades.....	5
	Dos alunos, professores, coordenadores, visitantes e prestadores de serviço que utilizam recursos de informática.....	5
	O Departamento de Tecnologia deverá.....	5
	O Departamento Jurídico deverá.....	6
VI.	Diretrizes de Segurança da Informação e utilização de recursos computacionais.....	6
	Quanto à solicitação de equipamentos, softwares e serviços de informática.....	6
	Quanto ao uso dos laboratórios de informática.....	7
	Quanto ao uso das impressoras e copiadoras.....	12
	Quanto ao acesso a rede corporativa e seus serviços.....	12
	Quanto ao uso e seleção de senhas.....	13
	Quanto à utilização de softwares.....	14
	Quanto à realização de backup, cópia de segurança e restauração de dados.....	14
	Quanto à manutenção e administração do ambiente.....	14
	Quanto ao uso dos recursos audiovisuais.....	14
VII.	Disposições Gerais.....	15
VIII.	Referências.....	16

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ANIMA EDUCAÇÃO

Garantir a **informação** como bem essencial da companhia, respeitando sua confidencialidade, assegurando sua continuidade e a usando de maneira ética.

INTRODUÇÃO

As informações, resumidamente são dados que, tratados adequadamente modificam quantitativamente e qualitativamente os ativos de uma organização. Essas informações portanto agregam valores, e por sua vez, devem ser protegidas, tendo em vista a quantidade de ameaças a que estão sujeitas (NBR ISO/IEC 17799:2000, pág. VI).

A informação pode existir de diversas formas, ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de meio eletrônico, mostrada em filmes ou falada em conversas. Seja qual for a forma apresentada ou meio através do qual a informação é compartilhada ou armazenada, é recomendado que seja sempre protegida adequadamente. (NBR ISO/IEC 17799, setembro 2001).

Desde o surgimento da internet e conseqüentemente a unificação da rede mundial, as organizações e seus sistemas de informações e redes se deparam frequentemente com constantes e crescentes ameaças como: invasão, hackers, vírus, spam, espionagem, vandalismo, etc.

A Segurança de Informações protege as informações por meio de normas, políticas, práticas, procedimentos, conscientização, treinamentos, estruturas e softwares, agindo diretamente sobre essas ameaças. (NBR ISO/IEC 17799:2000, pág. VI).

Este documento foi elaborado fundamentado nos principais agentes da Segurança de Informações, citados acima.

I. OBJETIVO

O objetivo desta política é orientar os alunos, professores, coordenadores, e prestadores de serviços sobre as diretrizes referentes à Segurança de Informações e Uso de Recursos Computacionais implantadas nas empresas que compõem o Grupo ANIMA, para proteger ativos da informação de sua propriedade ou sob sua custódia, contra ameaças internas ou externas, deliberadas ou acidentais.

II. APLICAÇÃO

Esta política aplica-se a todos os usuários dos sistemas e dos recursos computacionais das empresas que compõem o Grupo ANIMA e das Instituições de Ensino a ele vinculados, sendo estes os alunos, professores, terceiros ou visitantes.

III. PRINCÍPIOS

A segurança da informação é baseada na preservação dos seguintes princípios:

- ✓ **Confidencialidade:** garantia de que o acesso à informação é restrito às pessoas autorizadas, ou seja, proteger a informação privada contra leitura e/ou cópia por alguém que não tenha sido explicitamente autorizado pelo proprietário daquela informação;
- ✓ **Integridade:** A integridade consiste em evitar que dados sejam apagados ou de alguma forma alterados, sem a permissão do proprietário da informação. O conceito de integridade está relacionado com o fato de assegurar que os dados não foram modificados por pessoas não autorizadas;
- ✓ **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos necessários sempre que for preciso, para isso, é de extrema importância que os serviços prestados pelo sistema sejam protegidos de forma que não sejam degradados ou se tornem indisponíveis sem autorização;
- ✓ **Autenticidade:** está associada com a identificação de um usuário ou computador, a autenticidade é a medida de proteção de um serviço/informação contra a personificação por intrusos;

IV. RESPONSABILIDADES

Dos alunos, professores, coordenadores, visitantes e prestadores de serviços que utilizam recursos de informática:

1. Conhecer e agir conforme o conteúdo contido nesta política e nas documentações normativas relacionadas às suas atividades;

O Departamento de Tecnologia deverá:

1. Prover a infraestrutura e os recursos de tecnologia da informação necessários ao cumprimento desta política;
2. Analisar criticamente as causas de incidentes de segurança da informação e suportar planos de ação para a melhoria da Gestão da Segurança da Informação com o gestor de segurança de informação;
3. Analisar por meio de relatórios técnicos todos os dados estatísticos sobre ataques ou qualquer outra ameaça à infraestrutura de tecnologia da informação das empresas que compõem o Grupo ANIMA e das Instituições de Ensino a elas vinculadas;
4. Executar programas de inventário, a fim de identificar softwares sem licenciamento ou danosos à rede;
5. Analisar e averiguar a rede corporativa, a fim de detectar fluxo indevido de informações, intrusos e ataques aos sistemas e serviços de rede;
6. Aplicar filtros na rede corporativa, de qualquer natureza, para minimizar riscos aos ativos de informação da Instituição;
7. Instalar ferramentas de gerenciamento de rede, a fim de manter o controle e disponibilidade das atividades institucionais;
8. Executar aplicativos na estação de trabalho para sincronizar dados com servidores, bem como configurar aplicativos automaticamente;

9. Criar regras de bloqueio de sites que possuam conteúdos indevidos a fim de gerenciar o uso da ferramenta;
10. Personalizar o acesso à internet, solicitando login e senha aos usuários, a fim de gerenciar o uso da ferramenta;
11. Limitar o uso da banda de internet e, de acordo com as políticas da Instituição;
12. Interromper os serviços de internet quando necessário;
13. Solicitar, quando necessário, a troca de senhas de rede, de sistemas, de Internet e exigir senhas complexas;
14. Excluir o acesso à rede acadêmica aos alunos que se desvincularem da Instituição por trancamento de matrícula, abandono, solicitação de transferência externa ou desligamento;

O Departamento Jurídico deverá:

1. Avaliar, quando solicitado, as normas e os Procedimentos de Segurança da Informação elaborados pelo DTI.
2. Representar e defender judicialmente a Instituição, se necessário, em caso de transgressão das normas, por parte de alunos, professores, colaboradores e etc.

V. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO E UTILIZAÇÃO DE RECURSOS COMPUTACIONAIS

Quanto à solicitação de equipamentos, softwares e serviços de informática pelo Corpo Docente:

1. Toda solicitação de equipamentos, softwares ou serviços deverá ser feita ao Departamento de Tecnologia e Informação (DTI) por meio do sistema de chamados (Help Desk), devendo as reservas de recursos audiovisuais serem realizadas através do sistema de agendamento disponível no acesso restrito do professor;

2. Definem-se como equipamentos de informática quaisquer artigos do tipo hardware utilizados na Instituição e gerenciados pelo Departamento de Tecnologia, tais como computadores (servidores e desktops), notebooks, pockets, palmtops, discos rígidos, memórias, cabos específicos, mouses, teclados, webcams, kits multimídia, gravadoras de CD-ROM e/ou DVD, leitoras de CD-ROM e/ou DVD, monitores, impressoras, scanners, ativos de rede, Datashows, retroprojetores, televisores etc.;
3. Definem-se como softwares, todo e qualquer programa instalado nos computadores da Instituição, seja por tempo determinado ou não, independentemente de sua finalidade e/ou setor no qual estará sendo utilizado;
4. Define-se como serviço relacionado todo e qualquer serviço referente a cabeamento estruturado (ponto de rede), manutenção, consultoria ou assessoria nos equipamentos ou softwares da Instituição;

Quanto ao uso dos laboratórios de informática:

1. Os usuários são responsáveis diretos pela utilização dos recursos computacionais a eles confiados, em concordância com as diretrizes deste regulamento, sendo considerados recursos computacionais o conjunto formado por gabinete CPU, monitor, teclado, mouse, sistema operacional e sistemas em geral;
2. Os usuários deverão informar imediatamente à equipe do NSI (Núcleo de Suporte à Informática) caso ocorra qualquer ocorrência relacionada aos equipamentos de informática (quebra, falha, mau funcionamento, incidente, desaparecimento);
3. Do acesso:
 - a. Os laboratórios de informática são administrados pelo Departamento de Tecnologia e Informação (DTI);
 - b. São destinados ao uso acadêmico de alunos e professores da Instituição, utilizados prioritariamente para reserva de aulas;
 - c. Para obter acesso aos laboratórios de informática, cada aluno, professor ou funcionário deverá possuir login e senha;
 - d. São considerados alunos, estudantes regularmente matriculados na Instituição, e professores, os docentes contratados para ministrar horas/aula ou outras atividades acadêmicas na Instituição;

- e. Poderão ser concedidos acessos especiais, desde que devidamente autorizados pelo Departamento de Tecnologia;
 - f. Os usuários terão acesso aos recursos dos laboratórios de informática de acordo com o seu perfil, curso ou departamento, respeitando as diretrizes estabelecidas pela Instituição;
 - g. Todo usuário tem a obrigação de conhecer as normas e os regulamentos que regem o funcionamento dos laboratórios de informática da Instituição, disponíveis no seu acesso restrito do site;
 - h. Quando o cadastramento não ocorrer de forma automática, o usuário deverá se dirigir ao Núcleo de Suporte à Informática (NSI) do seu campus e requisitar o login e senha;
 - i. Será permitido aos alunos, professores, coordenadores e funcionários o uso de notebooks pessoais no âmbito dos laboratórios sob a responsabilidade dos mesmos;
4. Dos horários de funcionamento:
- a. O horário de funcionamento dos laboratórios de informática é de segunda a sexta-feira, das 7:20h às 22:35h e aos sábados, sob demanda, acordada com a coordenação de cursos;
 - b. Os usuários deverão respeitar os horários de funcionamento dos laboratórios de informática, visto que os equipamentos deverão ser desligados no horário previsto para encerramento;
5. Da estrutura, da impressão e do armazenamento de dados:
- a. Os laboratórios de informática dispõem de computadores com softwares licenciados instalados, rede local, serviço de impressão a laser, acesso à internet e serviço técnico especializado;
 - b. O uso das impressoras é restrito à reprodução de material estritamente acadêmico.

- c. O prazo para os usuários retirarem a impressão em um dos totens é de até 6 (seis) horas, contados após comando de impressão; findo esse tempo, o documento será excluído da fila de impressão, sem ônus para o aluno;
 - d. A impressão deve ser retirada pelo aluno em um dos totens ou nas lojas da copiadora, mediante a inserção de login e senha no sistema;
6. Das reservas de recursos audiovisuais pelo Corpo Docente:
- a. As solicitações de uso de laboratórios de informática para aulas deverão ser feitas a partir do acesso online do professor, disponível no site da Instituição;
 - b. As reservas dependem da disponibilidade dos laboratórios de informática, bem como dos recursos audiovisuais;
 - c. Somente professores, coordenadores de curso ou supervisores de laboratórios poderão efetuar reservas para aulas eventuais (agendadas para datas específicas), e para aulas regulares (ministradas regularmente em todas as semanas do semestre);
 - d. Eventuais cancelamentos de reserva devem ser feitos pelo professor, coordenador de curso ou supervisor de laboratório com pelo menos 1 (um) dia de antecedência pelo sistema de reserva, por telefone ou e-mail publicados no sistema;
 - e. Após 15 (quinze) minutos da hora marcada para o início da aula, sendo constatada a ausência do professor para a aula determinada, a reserva será automaticamente cancelada e o laboratório de informática será disponibilizado para o uso geral;
 - f. É vedado ministrar aulas nos laboratórios de informática sem a devida reserva de horário, assim como reservar laboratório de informática para uma turma de alunos sem a presença de um professor;
7. Das instalações de softwares:
- a. Pedidos de instalação de softwares para aulas eventuais ou regulares deverão ser feitos apenas pelo coordenador de curso, por meio do sistema de chamados;
 - b. A necessidade da realização de configurações especiais nos computadores dos laboratórios de informática deverá ser comunicada no ato da reserva.

- c. Os prazos para a instalação de softwares ou configurações especiais deverão ser acordados, no ato da solicitação, com o responsável do NSI do campus respectivo;
 - d. A instalação somente será feita após obtenção da licença do software, devidamente regularizada;
 - e. Depois de instalado, os testes de configuração do software deverão ser realizados pelo solicitante;
8. Da utilização de internet:
- a. A internet deverá ser utilizada exclusivamente para conteúdos acadêmicos. Qualquer site da internet que estiver bloqueado para uso, por ser a princípio considerado de uso não acadêmico, pode ser desbloqueado a pedido dos professores ou coordenadores, por meio do sistema de chamados;
9. Das responsabilidades dos usuários:
- a. O usuário responderá por danos físicos ou lógicos causados aos equipamentos, a título de dolo ou culpa, ressarcindo, monetariamente a Instituição e ficando ainda sujeito às penalidades disciplinares constantes nas Normas e no Regimento Interno desta;
 - b. O Departamento de Tecnologia não se responsabiliza por informações e/ou dados armazenados em diretórios locais, sendo de inteira responsabilidade do usuário a manutenção de cópias de segurança de seus arquivos. Quando necessário, poderá ser realizados backup, desde que solicitado antecipadamente;
 - c. Utilizar e controlar seu login e senha, não podendo permitir o acesso a recursos computacionais dos laboratórios de informática por pessoas não autorizadas, ou colaborar com tais procedimentos;
 - d. Comunicar ao funcionário ou estagiário dos laboratórios de informática qualquer problema, defeito ou evidência de violação das normas em vigor, não podendo omitir ou acobertar tais fatos;
 - e. Efetuar, após utilizar qualquer computador, o procedimento de logoff;
10. Das restrições e dos atos administrativos preventivos:

É vedado ao usuário:

- a. Executar comandos que levem à criação, alteração ou destruição de dados informatizados;
- b. Fumar ou consumir qualquer tipo de alimento nas dependências dos laboratórios de informática;
- c. Promover encontros e reuniões de caráter pessoal ou que não estejam relacionados com as atividades acadêmicas;
- d. Escutar música sem fone de ouvido;
- e. Colocar os pés sobre as mesas ou cadeiras, assentar em mesas ou fazer qualquer utilização inadequada de móveis e equipamentos;
- f. Falar em tom alto ou promover algazarras nos laboratórios de informática;
- g. Praticar jogos de qualquer natureza;
- h. Acessar a internet para fins não acadêmicos (ex. pornografias);
- i. Baixar arquivos como avi, mpeg, mpg, mp3, mid e wav, entre outros, com conteúdo não acadêmico;
- j. Instalar programas de qualquer natureza;
- k. Usar aparelhos celulares que perturbem a concentração dos demais usuários do laboratório;
- l. Alterar configurações de computadores;
- m. Invadir as dependências do NSI ou usar computadores administrativos;
- n. Afixar cartazes, panfletos ou anúncios de qualquer gênero nas dependências dos laboratórios de informática sem permissão previa da infraestrutura do campus;
- o. Emprestar login a aluno que estiver com sua conta bloqueada, ou a usuários externos;
- p. Remover documentos que não sejam de sua exclusiva propriedade;
- q. Camuflar a própria identidade, salvo no caso em que o acesso anônimo seja explicitamente permitido;
- r. Ler mensagens de terceiros, ou documentos confidenciais ou não autorizados.
- s. Interceptar transmissão de dados ou monitorar-se via barramento por meio da rede;

- t. Interferir em serviços de outros usuários, bloqueá-los ou congestionar a rede de qualquer forma;
- u. Permanecer nos laboratórios de informática sem autorização do professor, em horário reservado à aula da qual o aluno não está participando;
- v. Desrespeitar os funcionários ou os estagiários dos laboratórios de informática;
- w. Quebrar senhas, violar fechaduras eletrônicas ou sistemas de alarme;
- x. Abrir, desmontar ou carregar qualquer computador, equipamentos ou qualquer patrimônio da Instituição;

Quanto ao uso das impressoras e copiadoras:

1. Os laboratórios de informática dispõem de computadores com programas de diversas categorias instalados e sistemas multimídia, acesso a mídias magnéticas e ópticas, rede local, serviço de impressão a laser, acesso à internet e serviço técnico especializado;
2. O uso das impressoras é restrito à reprodução de material estritamente acadêmico.
3. O prazo para os usuários retirarem materiais impressos em um dos totens é de até 6 (seis) horas, contada a partir do comando de impressão. Findo esse tempo, o documento será excluído da fila de impressão.
4. A impressão deve ser retirada pelo aluno em um dos totens ou nas lojas da copiadora, mediante a inserção de login e senha no sistema;

Quanto ao acesso à rede corporativa e seus serviços:

1. O acesso ao ambiente informatizado deverá ser concedido unicamente por meio de identificação (conta ou login) e de senha associada;
2. É dever do usuário proteger suas credenciais de acesso ao sistemas de informação. O detentor da conta e senha deverá assumir a responsabilidade pela guarda, descrição ou sigilo das operações decorrentes do seu uso;
3. A implantação de perfis de acesso será realizada com base no princípio de privilégio mínimo;

4. É vedado ao usuário:
 - a. Acessar sites de conteúdo criminoso, apostas ou pornografia. O Departamento de Tecnologia irá restringir os acessos a sites que considerar alheios aos objetivos do grupo, e monitorar consultas de usuários, com objetivo de garantir segurança e adequação do uso deste recurso;
 - b. Revelar a terceiros sua identificação de usuário e senha de acesso à rede, ou a qualquer sistema da Instituição;
 - c. Alterar qualquer configuração de rede de computadores;
 - d. Burlar ou tentar burlar os dispositivos de segurança da rede;
 - e. Capturar dados na rede corporativa, que coloquem em risco a confidencialidade dos documentos, arquivos e o fluxo de dados entre as estações;
 - f. Utilizar a Internet para atividades ilícitas, contrárias aos interesses legítimos da Instituição, ou fora do contexto das atividades acadêmicas, ou em violação às regras fixadas neste documento;
 - g. Fazer download de arquivos executáveis ou de multimídia, mesmo que estejam compactados, sem autorização prévia do Departamento de Tecnologia;
5. Rede Wireless
 - a. As configurações de acesso à rede wireless serão realizadas somente pela equipe do NSI especializada e responsável por essa tarefa;
 - b. É de responsabilidade da equipe de Redes a configuração de qualquer Access Point, localizado em quaisquer campi;

Quanto ao uso e seleção de senhas:

1. Senhas são de uso pessoal e intransferível, sendo sua manutenção e confidencialidade responsabilidade de seu proprietário;
2. Senhas não devem ser registradas em papel, ou em qualquer meio sem controle, ou caracterizado como de acesso público;
3. Senhas devem ser alteradas pelos usuários sempre que houver qualquer indicação de possível comprometimento do sistema ou das próprias senhas. Recomenda-se a mudança de senha mensalmente;

4. É recomendável a utilização de letras, números e caracteres especiais na elaboração de senhas, tornando-as menos vulneráveis e susceptíveis à fraudes;

Quanto à utilização de softwares:

1. Os equipamentos de informática funcionarão somente com softwares regularmente adquiridos e licenciados junto a seus fornecedores ou representantes, ou ainda com aqueles desenvolvidos pelo quadro de funcionários da Instituição.
2. A área de Tecnologia, periodicamente, irá efetuar auditoria nas estações objetivando manter o padrão corporativo de softwares nos equipamentos.
3. Todos os servidores corporativos e estações serão protegidos pelo software de antivírus homologado, que deve estar sempre ativo e atualizado, seguindo as configurações definidas pela área de Tecnologia. O software de antivírus somente poderá ser removido das estações de trabalho e servidores pelos Administradores de Rede;

Quanto à realização de backup, cópia de segurança e restauração de dados:

1. Não será realizado, pela área de Tecnologia, Backup ou Cópia de Segurança de nenhuma informação ou arquivo armazenado nas estações de trabalho.

Quanto à manutenção e administração do ambiente:

1. O Departamento de Tecnologia poderá padronizar a configuração das estações com a utilização de papéis de parede, protetores de tela, menus de navegação, etc.

Quanto ao uso dos recursos audiovisuais:

1. Entendem-se como recursos audiovisuais: datashow, caixas de som, mesa de som, notebooks, vídeo cassete, DVD Player, TV's, retroprojektor, fone de ouvido, Cdplayer, microfone, robô (TV, DVD, Computador e Datashow), datatv (computador e TV), datatv DVD (computador com DVD e TV);
2. Agendamento de recursos para sala de aula:
 - a. Os recursos devem ser agendados por meio do sistema de agendamentos;
 - b. A reserva pode ser realizada por professores, coordenadores de curso, funcionários administrativos e funcionários do NSI, sendo que:

- i. O prazo mínimo para a realização da reserva pelos professores é de 6 horas e o máximo é de 240 horas ou 10 (dez) dias;
 - ii. O prazo mínimo para realização da reserva pelos coordenadores de curso é de 6 horas e o máximo de 1 semestre;
 - iii. O prazo mínimo para realização da reserva pelos funcionários administrativos é de 6 horas e o máximo de é de 240 horas ou 10 (dez) dias;
 - iv. O prazo mínimo para a realização da reserva pelos funcionários do NSI é de 6 horas e o máximo de 1 semestre;
- c. A reserva dos equipamentos de audiovisual está sujeita à disponibilidade dos mesmos;
 - d. Ficam sob responsabilidade dos solicitantes os equipamentos móveis listados a seguir, que forem disponibilizados pela Instituição: notebooks, datashow salvo os instalados em suporte fixo de teto, caixas de som, DVD Player, fones de ouvido, CD Player.

VI. DISPOSIÇÕES GERAIS

1. Nos casos em que houver violação desta Política de Segurança de Informações e uso de recursos computacionais, sanções administrativas e/ou legais poderão ser adotadas, podendo culminar com o desligamento do infrator e eventuais processos criminais, se aplicáveis.

VII. REFERÊNCIAS

1. NBR ISO/IEC 17799:2000.