INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAZONAS

POLÍTICA DE USO DO SISTEMA DE TECNOLOGIA DA INFORMAÇÃO

MANAUS/AM
2012

POLÍTICA DE USO DO SISTEMA DE TECNOLOGIA DA INFORMAÇÃO DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAZONAS

TÍTULO I

REGRAS E DIRETRIZES

CAPÍTULO I

NORMA DE USO DO SERVIÇO

Art.1º O Instituto Federal de Educação, Ciência e Tecnologia do Amazonas (IFAM) possui uma rede local e remota com facilidades de conexão com a Internet e cujo domínio é www.ifam.edu.br. Todas as máquinas conectadas à rede do Instituto (tanto as das unidades administrativas como as dos laboratórios de alunos de todos os Campi) podem usufruir dos recursos da Internet como: acessar páginas www, ssh, entre outros.. Dentre as facilidades que são oferecidas aos servidores e alunos destacam-se o serviço de correio eletrônico e o servidor de páginas.

§ 1º. A utilização de qualquer computador do IFAM implica na aceitação e o respeito as regras de uso aqui definidas e amparadas pela Resolução nº 18/CONSUP/IFAM, de 15 de junho de 2012.

§ 2º. Os termos e as siglas utilizadas neste documento estão de acordo com a listagem apresentada no anexo I.

Art.2º A utilização de qualquer serviço deve ser norteada por um documento denominado norma de uso do serviço.

§ 1º. A norma de uso do serviço deve especificar o público alvo do serviço.

§ 2º. As instruções de funcionamento, bem como as limitações de um serviço devem ser fornecidas aos seus usuários.

§ 3º. A norma de uso do serviço deve estipular PROCEDIMENTOS ADMINISTRATIVOS – PA que deverão ser aplicados em caso de desvio na sua utilização.

§ 4º. A norma deverá ser amplamente divulgada para cada tipo de serviço oferecido.

§ 5º. A norma de uso do serviço deve definir regras de controle de acesso ao serviço.

§ 6º. A norma de uso do serviço deve definir um mecanismo de registro de acesso ao serviço (log).

§ 7º. Recomenda-se que os responsáveis pelos Laboratórios possuam um controle de acesso.

§ 8º. Serviços cuja informação é classificada como privativa e/ou confidencial devem fornecer métodos seguros de autenticação e autorização validados pelos órgãos centrais de administração de informática do Instituto.

§ 9º. Deverá ser disponibilizado um telefone e/ou e-mail para suporte aos usuários do serviço.

§ 10. Todo serviço deverá ter um responsável ou contato para ser acionado pelos CTI's (Coordenação de Tecnologia da Informação) em casos de incidentes de segurança ou de outros motivos relacionados ao serviço.

§ 11. Todo usuário que se utilizar de algum recurso computacional no IFAM deverá obrigatoriamente possuir um meio de autenticação.

§ 12. Os usuários devem procurar o DGTI (Diretoria de Gestão de Tecnologia da Informação) ou CTI's (Coordenação de Tecnologia da Informação) em caso de dúvidas e esclarecimentos sobre as regras e diretrizes.

CAPÍTULO II

REGRAS E DIRETRIZES GERAIS PARA SOFTWARES

Art.3º No Brasil, os direitos sobre software de computadores estão regulados pela Lei de Direitos Autorais (nº 9.610 de 29/02/1998) e da Lei do Software (nº 9.609 de 19/02/1998). A legislação sobre software estabelece que a violação dos direitos autorais de programas de computador é passível de ação criminal e civil podendo ser combinada a esta, a fixação de pena para o caso de transgressão daquele preceito legal. Além disso, o infrator fica sujeito à busca e apreensão de todas as cópias ilegalmente reproduzidas e utilizadas. Combinada, pois com a Lei do Direito Autoral, a Lei do Software permite que as perdas e danos do titular do programa sejam ressarcidos por valores que podem atingir até 3.000 vezes o dos programas ilegalmente reproduzidos. Além disso, o infrator fica sujeito à detenção de seis meses a dois anos pelo uso ilegal do programa.

Art.4º Todos os usuários (servidores, alunos e terceiros) da Rede IFAM devem atender as seguintes orientações:

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

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

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

IV. Não podem tornar o software disponível para outros usarem ou copiarem, se tal procedimento estiver em desacordo com os termos da licença de software;

V. Não podem aceitar software não licenciado de terceiros; e

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

Art.5º Cabe a DGTI e às Coordenações de TI dos Campi:

I. Especificar requisitos mínimos de hardware para aquisição dos softwares (Básico, Aplicativos e Utilitários);

II. Inspecionar se o hardware e software estão de acordo com a solicitação;

III. Instalar e Manter (Atualizar e Remover) os softwares (Básico, Aplicativos e Utilitários);

IV. Auditar os computadores da Rede IFAM; e

V. Fazer o gerenciamento de todas as licenças de *software* adquiridas pelo Instituto.

CAPÍTULO III

REGRAS E DIRETRIZES GERAIS PARA USUÁRIOS

Art.6º Cabe a DGTI e às Coordenações de TI dos Campi conhecerem as instruções, regras e PA's (Procedimento Administrativo) que implicam na utilização do serviço atendendo aos seguintes itens:

I. Não se fazer passar por outra pessoa ou dissimular sua identidade quando utilizar os recursos computacionais;

II. Responsabilizar-se pela sua identidade eletrônica, senha, credenciais de autenticação, autorização ou outro dispositivo de segurança, negando revelá-la a terceiros; e

III. Responder por mau uso dos recursos computacionais, bem como atos que violem as regras, estando, portanto, sujeito aos PA's (Procedimento Administrativo).

CAPÍTULO IV
REGRAS E DIRETRIZES GERAIS DESTINADAS AOS MANTENEDORES DOS SERVIÇOS

Art.7º As pessoas envolvidas no projeto, implementação e operação do serviço devem estar cientes da Política de Uso do Serviço, não podendo alegar desconhecimento. Assim, cabe aos mantenedores:

I. Cumprir as regras e diretrizes definidas nas normas;

II. Preservar a integridade e a segurança dos sistemas;

III. Manter os registros e logs de utilização dos serviços;

IV. Armazenar registros em outro computador, além do que hospeda o serviço, ou ainda offline (fita, CD, DVD, etc);

V. Manter registros por um período mínimo de 30 dias nos casos de acesso a Internet ou conforme a lei;

VI. Fornecer registros e logs mediante somente à solicitação por escrito da Diretoria Geral de cada Campus ou Reitor no caso da Reitoria e Diretorias de Campi;

VII. Movimentar os arquivos institucionais dos usuários somente quando for indispensável para manutenção do sistema ou em casos de falhas de segurança;

VIII. Gerenciar adequadamente os privilégios de grupos e usuários, as senhas de usuários, os procedimentos de logon, de desconexão de usuários por inatividade e de política de troca de senha;

IX. No caso de um incidente de segurança, identificar as pessoas responsáveis, notificando o DGTI; e

X. Interagir com os CTI's para troca de conhecimentos sobre ferramentas apropriadas a serem utilizadas para segurança e gerenciamento dos serviços.

CAPÍTULO V
VIOLAÇÃO DAS REGRAS

Art.8º Considera-se violação das regras o seguinte:

I. Mostrar, armazenar ou transmitir texto, imagens ou sons que possam ser considerados ofensivos ou abusivos conforme as Leis Federais;

II. Efetuar ou tentar qualquer tipo de acesso não autorizado aos recursos computacionais da Instituição;

III. Utilizar os recursos computacionais da rede IFAM para acesso não autorizado a Domínios de terceiros;

IV. Violar ou tentar violar os sistemas de segurança, quebrando ou tentando adivinhar a autenticação eletrônica de outro usuário, senhas ou outros dispositivos de segurança;

V. Interceptar ou tentar interceptar a transmissão de dados através de monitoração, exceto para fins de pesquisa da Instituição usando redes destinadas para essa finalidade, com prévio conhecimento do CTI local;

VI. Provocar interferência em serviços de outros usuários ou o seu bloqueio, provocando congestionamento da rede de dados, inserindo vírus ou tentando a apropriação indevida dos recursos computacionais da Instituição;

VII. Desenvolver, manter, utilizar ou divulgar dispositivos que possam causar danos aos sistemas e às informações armazenadas, tais como criação e propagação de vírus, trojans e worms, criação e utilização de sistemas de criptografia que causem ou tentem causar a indisponibilidade dos serviços ou

destruição de dados, e ainda, engajar-se em ações que possam ser caracterizadas como violação da segurança computacional;

VIII. Utilizar os recursos computacionais da rede IFAM para atividades direta ou indiretamente relacionadas ao desenvolvimento de malwares. Exceto para fins de Pesquisa na Instituição;

IX. Utilizar os recursos computacionais da rede IFAM para fins próprios, lucrativos e políticos;

X. Utilizar os recursos computacionais da rede IFAM para intimidar, assediar e difamar; e

XI. Utilizar de forma inadequada e fora dos padrões os recursos computacionais da rede IFAM.

CAPÍTULO VI

DISTRIBUIÇÃO DE INFORMAÇÃO IMPRÓPRIA

Art.9º O usuário não pode transmitir, difundir ou disponibilizar a terceiros, informações de qualquer natureza e classe material, de forma que:

I. Contrariem, menosprezem ou atentem contra os direitos fundamentais e as liberdades públicas reconhecidas constitucionalmente, nos tratados internacionais e no ordenamento jurídico como um todo;

II. Induzam, incitem ou promovam atos ilegais, denegridores, difamatórios, infames, violentos ou, em geral, contrários à lei, à moral e aos bons costumes geralmente aceitos ou à ordem pública;

III. Induzam, incitem ou promovam atos, atitudes ou idéias discriminatórias por causa de sexo, raça, religião, crenças, idade ou condição;

IV. Incorporem, ponham à disposição ou permitam acessar produtos, elementos, mensagens e/ou serviços ilegais, violentos, pornográficos, degradantes ou, em geral, contrários à lei, à moral e aos bons costumes geralmente aceitos ou à ordem pública;

V. Induzam ou possam induzir a um estado inaceitável de ansiedade ou temor;

VI. Induzam ou incitem a envolver-se em práticas perigosas, de risco ou nocivas à saúde ou equilíbrio psíquico;

VII. Sejam falsos, ambíguos, inexatos, exagerados ou extemporâneos, de forma que possam induzir a erro sobre seu objeto ou sobre as intenções ou propósitos do comunicante; sejam protegidos por quaisquer direitos de propriedade intelectual ou industrial pertencentes a terceiros, sem que o Usuário tenha obtido previamente dos seus titulares a autorização necessária para levar a cabo o uso que efetuar ou pretender efetuar; transgridam os segredos de terceiros;

VIII. Sejam contrários ao direito de honra, à intimidade pessoal e familiar ou à própria imagem das pessoas;

IX. Infrinjam as normas sobre segredo das comunicações;

X. Constituam publicidade ilícita, enganosa ou desleal;

XI. Incorporem vírus ou outros elementos físicos ou eletrônicos que possam causar dano ou impedir o normal funcionamento da rede, do sistema ou de equipamentos de informática (hardware e software) de terceiros, ou que possam causar dano aos documentos eletrônicos e arquivos armazenados nestes equipamentos;

XII. Provoquem, por suas características, dificuldades no normal funcionamento do Serviço;

XIII. Permitam a tentativa de acesso, ou o acesso a máquinas não autorizadas; e

XIV. Permitam a tentativa de quebra, ou a quebra de sigilo de códigos alheios, o acesso e modificação de arquivos pertencentes a outros usuários sem a sua autorização.

CAPÍTULO VII

RESPONSABILIDADES DOS USUÁRIOS

Art.10 O usuário é responsável por qualquer atividade a partir de sua conta e também por seus atos no uso dos recursos computacionais oferecidos. Assim, o mesmo responderá por qualquer ação legal apresentada à Instituição e que o envolva.

Parágrafo Único. No caso de violação às normas, serão tomadas ações previstas na mesma, se a violação infringir as leis federais, a Administração será informada.

TÍTULO II

IDENTIDADE DOS USUÁRIOS

CAPÍTULO I

OS ADMINISTRADORES DOS SISTEMAS COMPUTACIONAIS

Art.11 Entende-se por “perfil de administradores de sistemas computacionais” quaisquer pessoas dos quadros docente, técnico-administrativo, discente ou que tenha vínculo com a Instituição e possuam conhecimento autorizado do código de acesso e senha do super usuário, root ou função equivalente dos computadores em que estejam instalados esses sistemas computacionais, sejam eles de uso geral, de uso restrito a um Campus, Departamento ou grupo de pessoas, ou ainda de uso individual.

Art.12 Os administradores dos sistemas computacionais do IFAM devem zelar pela segurança dos sistemas e dos dados sob os seus cuidados, devendo observar as seguintes normas:

I. Não abrir contas de uso coletivo ou com senhas públicas;

II. Suspender contas que estejam inativas por períodos superiores a 120 dias, a não ser em casos justificados;

III. Cancelar contas de usuários que venham a se desligar do IFAM, tais como alunos formados, servidores públicos exonerados, após 180 dias do desligamento, para que o usuário possa preservar os seus dados e redirecionar a sua correspondência eletrônica para outro endereço;

IV. Dar conhecimento desta Política a todo usuário que mantenha conta em sistemas computacionais sob sua responsabilidade;

V. Desabilitar as contas e senhas associadas a setores cujo responsável venha a ser substituído ou ficar vagos, sendo essa informação oriunda do setor de Gestão de Pessoas;

VI. Em caso de desligamento com caráter punitivo ou litigioso uma vez informado por escrito pelo setor competente, a desativação das contas e senhas mencionadas no parágrafo anterior deve ser feita antes do comunicado do desligamento;

VII. Configurar os computadores ou sistemas para exigir senhas de difícil decodificação, comprimento mínimo de oito caracteres, utilizando letras e números; e

VIII. Não utilizar como servidores ou para armazenamento de informações, computadores cujos sistemas operacionais não dêem suporte às características exigidas nas normas de padronização;

Parágrafo único. Para os efeitos dos itens II e III, servidores aposentados pelo IFAM poderão manter conta de email ativa do IFAM, mediante requerimento por escrito.

CAPÍTULO II

O ACESSO À REDE DO IFAM

Art.13 Ao manter e usar uma conta em sistema computacional do IFAM, o usuário responsabiliza-se pela sua senha de acesso, obrigando-se a não revelá-la a terceiros, sejam pessoas vinculadas ao IFAM ou não.

§ 1º. Excepcionalmente, o acesso poderá ser repassado a pessoa vinculada ao IFAM, desde que esta assine um termo de responsabilidade, cujo modelo encontra-se no *site* www.dgti.ifam.edu.br.

§ 2º. Caso o acesso seja repassado sem adoção da medida prevista no parágrafo anterior, o titular da senha responderá pelo mau uso do sistema em qualquer circunstância, não podendo transferir responsabilidade a terceiros.

Art.14 As chefias imediatas e os órgãos de recursos humanos e acadêmicos, ao programar ou efetivar transferências e desligamentos de pessoal, deverão informar os fatos aos (Aos GT'S de seu Campus) de suas Unidades em 72 horas para que a conta seja desabilitada no tempo adequado, conforme o caso.

Art.15 Os sistemas computacionais devem ter um controle de uso, definido na sua norma, restrito às pessoas expressamente autorizadas por quem de direito. As Chefias devem orientar seus funcionários a respeito desse procedimento, por escrito e de forma clara.

§ 1º. O usuário ou administrador poderá transferir a responsabilidade a terceiros caso implemente mecanismos manuais ou automáticos ("logs") que permitam identificar, pelo os usuários dos computadores por intermédio dos quais seja possível causar incidentes.

§ 2º. O DGTI e os CTI's promoverão, quando necessário, cursos e palestras sobre assuntos relacionados a segurança da Rede IFAM, uso de recursos de informática.

§ 3º. Para evitar procedimentos inadequados ou incorretos que possam gerar problemas futuros à segurança de informações e dados deste Instituto, as chefias imediatas de funcionários que lidam com processos de informática, tais como abertura de contas e gerenciamento de usuários, devem manter um controle rígido dos procedimentos de segurança e realizar reuniões com seus funcionários para manter o sistema operando em conformidade com estas normas.

TÍTULO III

USO DE *LINKS* NO DOMÍNIO IFAM

Art.16 A inserção de referências a páginas eletrônicas de pessoas físicas e jurídicas, externas ao IFAM, nas páginas eletrônicas do IFAM, de suas Unidades, Campus e Órgãos, rege-se pelo disposto desta política.

Art.17 Não estão sujeitas a restrições as referências em páginas eletrônicas do IFAM:

I. As páginas cujo conteúdo seja da natureza e de interesse acadêmico; e

II. As instituições de utilidade pública, entidades da administração pública direta e indireta, fundações e outras instituições sem fins lucrativos, desde que os ser viços de tais entidades sejam julgados relevantes para a Instituição, no caso do Portal IFAM, e para as Unidades, Campus e Órgãos, em se tratando de suas páginas eletrônicas na Internet.

Parágrafo único. Para a inserção de referências não previstas nesta Política em página eletrônica, sob o Domínio IFAM, é necessário solicitação por escrito.

Art.18 Caberá ao Setor Comunicação do IFAM, o deferimento do pedido sobre a inserção das referências mencionadas no parágrafo 3.2.2 deste artigo no Portal do IFAM, no endereço http://www.ifam.edu.br.

Art.19 Caberá ao dirigente do Campus, a decisão sobre o mérito quando se tratar de inserções desse tipo em suas respectivas páginas eletrônicas.

Art.20 Cada Campus decidirá conforme a análise e oportunidade de permitir a inserção dessas referências nas suas páginas eletrônicas internas, nas condições estipuladas, autorizada pela respectiva diretoria.

Art.21 A inclusão de referências nas páginas internas do Portal do IFAM será decidida, pela Comunicação do IFAM.

Art.22 Caberá ao Setor de Comunicação do IFAM a verificação do cumprimento da norma referente ao uso de Links Institucionais nas páginas do Campus.

Art.23 Não serão admitidas referências a pessoas físicas e jurídicas, externas à Instituição, em suas páginas eletrônicas, nas seguintes situações:

Art.24 Mediante simples remuneração ou pagamento, sob pena de a referência as sumir a natureza de mera publicidade;

Art.25 Caberá a Comunicação do IFAM a verificação periódica do cumprimento deste artigo nas páginas das Unidades, Campus ou Órgãos.

Art.26 Os casos omissos serão decididos pelo DGTI e Comunicação do IFAM.

TÍTULO IV
REGISTROS DE DADOS INFORMATIZADOS

Art.27 A coleta, a inserção e a conservação, em registro informatizado, de dados pessoais devem estar sob a égide da voluntariedade, da privacidade e da confidencialidade, podendo ser utilizados para os fins propostos para sua coleta.

Art.28 Os Servidores Públicos e o Corpo Discente da Rede IFAM têm direito de acesso aos seus registros, mediante requerimento por escrito.

Art.29 O acesso e a utilização de informações relativas à vida acadêmica ou funcional de outrem, por qualquer usuário da Rede IFAM, dependem de:

I. Expressa autorização do titular do direito;

II. Ato administrativo motivado, em razão de objetivos acadêmicos ou funcionais, devidamente justificados;

III. Os recursos computacionais da Instituição destinam-se exclusivamente ao desenvolvimento de suas atividades de ensino, pesquisa e extensão. Não podendo ser usados para fins pessoais ou comercias de terceiros; e

IV. Arquivos computacionais:

a. Quando os arquivos forem institucionais gerados ou armazenados a partir de contas funcionais são de uso privativo do detentor da conta ou proprietário;

b. Quando os arquivos forem de caráter pessoal gerados ou armazenados a partir contas pessoais são de responsabilidade do detentor da conta ou proprietário;

c. Quando os arquivos forem armazenados em pastas públicas a partir de qualquer conta estão sujeitas a todas manipulações (alterar,consultar,excluir ou mover); e

d. Os administradores dos sistemas computacionais poderão mover os arquivos em casos de necessidade de manutenção ou falha de segurança.

TÍTULO V

REGISTRO DE SUB-DOMÍNIOS DA REDE IFAM

Art.30 A solicitação de registro de subdomínios da Rede IFAM deve ser feita por escrito pelo interessado ao Diretor de Gestão de Tecnologia da Informação.

Parágrafo Único. Em nenhuma hipótese serão registrados nomes considerados ofensivos, de baixo calão, preconceituosos ou manifestamente desvinculados dos objetivos e propósitos do IFAM.

Art.31 O registro de domínios IFAM fica na responsabilidade do DGTI, pois o mesmo gerencia a faixa de IP da Rede IFAM (200.129.168.0).

Art.32 Nomes obedecendo ao formato <ddd.ifam.edu.br/>, sem conter a Unidade, salvo exceções previstas no artigo 5º, só podem ser atribuídos a iniciativas da administração central, não vinculadas a um Campus. Exemplos: projetos.ifam.edu.br.

Art.33 Caberá a DGTI analisar e aprovar os domínios solicitados que se enquadrem nos itens 5.1 ou 5.3.

Art.34 Fundações, sociedades acadêmicas, científicas e culturais, e outras entidades oficialmente autorizadas a funcionar em campus do IFAM que possuam seus próprios CNPJ, ainda que recebam números IP atribuídos pelo IFAM, só podem requerer nomes de formato <ddd.org.br>. Exemplo: www.saci.org.br (Solidariedade, Apoio, Comunicação e Informação).

Parágrafo Único. Os nomes de domínios atualmente registrado serão revisados e os que deixarem de atender a qualquer ítem deste capítulo serão orientados a seguir o padrão definido nas normas, com prazo de até dois (2) anos para conviver em paralelo com o endereço antigo.

TÍTULO VI

POLÍTICA DE SEGURANÇA DA REDE IFAM

CAPÍTULO I

RESPONSÁVEIS PELA POLÍTICA DE SEGURANÇA

Art.35 A Rede Computacional do IFAM, deve permitir ao Instituto a possibilidade de se integrar a outros centros de ensino, pesquisa e extensão. Além disso, ela deve possuir recursos computacionais e de redes para acesso aos Sistemas de Informação Corporativos – SICs que permitam o tráfego de um grande volume de dados, tanto interno quanto externo de forma segura, mantendo a confidencialidade, a integridade a disponibilidade e a autenticidade da informação, independentemente de onde ela esteja, residente em memória de máquinas e dispositivos, armazenada em disco conforme a norma ou em trânsito, salvaguardando a exatidão e completeza da mesma, dos métodos de processamento e garantindo que usuários obtenham acesso à informação sempre que necessário e de acordo com a permissão atribuída a cada um.

Art.36 Os Órgãos, comissões, grupos e pessoas responsáveis pela Política de Segurança e suas respectivas atribuições são as seguintes:

I. Comissão de Política de Uso do Sistema de Tecnologia da Informação IFAM: Formular as políticas do IFAM na área de informática, constituída por um Chefe de Departamento ou Coordenação de TI presidida pelo Diretor de Tecnologia da Informação;

II. DGTI: Coordenar a execução dessas políticas pelos órgãos executivos (Departamentos ou Coordenações de Tecnologia da Informação – CTI's);
III. Coordenações de Tecnologia da Informação - CTI's: Auxiliar a DGTI ao formular as diretrizes gerais de informática e executar as políticas de informática formuladas pela Comissão;
IV. Unidades de Ensino e Pesquisa, campus, Museus e Órgãos da Administração Central: Formular políticas de informática em consonância com as políticas da DGTI e dos CTI's, e Coordenar a execução das políticas formuladas por seus Setores de Informática ou, na inexistência destes, com a Coordenadoria de Tecnologia da Informação mais próxima;
V. Consultoria Jurídica: Auxiliar ao DGTI, Unidades e Órgãos quanto aos aspectos legais, e avaliar os incidentes de segurança causados por servidores alunos e terceirizados do Instituto, recomendando as penalidades cabíveis; e
VI. Outros participantes da Política de Segurança:

a. Comissão Permanente de Segurança, criada pela portaria XXXX: Assessorar as Coordenações de Tecnologia da Informação no tratamento de questões de segurança; manter e aprimorar a Política de Segurança vigente visando à sustentação das atividades de proteção da informação eletrônica do Instituto; ser o canal de comunicação entre a CJ e as Comissões e CTIs dos Campi. Essa comissão deve ser formada por um representante de cada CTI e presidida pelo Diretor do DGTI;
b. Grupos de Segurança: Colaborar com a Comissão de Segurança da rede IFAM na promoção da Política de Segurança do Instituto e Demais atribuições conforme Portaria de criação;
c. Coordenador de Infra-Estrutura e Redes: Pessoa indicada pelo IFAM com a responsabilidade de zelar pelo cumprimento das Normas de segurança; e
d. Alunos, Servidores e demais pessoas que usam os recursos computacionais e de comunicação do Instituto.

CAPÍTULO II

SEGURANÇA DA INFORMAÇÃO

Art.37 Considera-se como segurança da informação a preservação da autenticidade, confidencialidade, integridade e autenticidade da informação do Instituto.

Art.38 A segurança pode ser enfocada sob dois aspectos:

I. Aspecto físico: adota-se como segurança física o relacionado à proteção de edificações, infra-estrutura e equipamentos, reduzindo as ameaças que possam colocar em risco o bom funcionamento dos sistemas; e

II. Aspecto lógico: como segurança lógica, entende-se a segurança dos dados do Instituto transmiti dos ou armazenados em servidores institucionais, tais como: servidores de E-mail, DNS, Web, e outros servidores.

Art.39 O Departamento ou Coordenações de Tecnologia da Informação do Instituto ou dos Campi deve monitorar o não cumprimento das normas de seguranças estabelecidas e aplicar as ações previstas para cada infração ocorrida.

CAPÍTULO III

NORMA DE SEGURANÇA DA REDE IFAM

Art.40 As Normas de Segurança para a rede IFAM têm o objetivo de fornecer um conjunto de Regras e Recomendações aos administradores de rede e usuários, visando a proteção e segurança dos equipamentos, dados, pessoas e instalações do IFAM, a saber:

I. Estabelecer procedimentos para a instalação e manutenção de ferramentas, hardware e software, visando à segurança dos sistemas computacionais e de comunicação da rede IFAM;

II. Orientar, por meio de suas diretrizes, todas as ações de segurança das Unidades de Ensino e Pesquisa, Campus, Centros de Informática e Órgãos de Administração para minimizar os riscos de segurança e garantir autenticidade, confidencialidade, integridade e disponibilidade da informação; e

III. Estabelecer procedimentos visando prevenir e responder a incidentes de segurança.

Art.41 Em conformidade com a Política de Segurança da rede IFAM, esta norma abrange os seguintes aspectos:

I. Segurança física dos dispositivos da rede IFAM e da infra-estrutura;

II. Segurança lógica dos equipamentos da rede IFAM;

III. Segurança da Informação;

IV. Segurança administrativa; e

V. Segurança do usuário.

CAPÍTULO IV

SEGURANÇA FÍSICA DAS INSTALAÇÕES DE INFRA-ESTRUTURA DE TI

Art.42 A Segurança Física tem como objetivos específicos:

I. Proteger edificações e equipamentos;

II. Prevenir perda, dano ou comprometimento dos ativos de rede;

III. Manter a continuidade das atividades dos negócios; e

IV. Prevenir as ameaças que coloquem em risco o bom funcionamento dos sistemas.

Art.43 Para o Sistema de Proteção contra Descargas Atmosféricas (SPDA) e Aterramento, recomenda-se que as edificações onde encontram-se instalações de Infra-Estrutura de TI, estejam protegidas por um sistema contra descargas atmosféricas (pára-raios) e possuam sistema de aterramento eficiente, observando-se o seguinte:

I. Todo sistema de proteção deve receber manutenção preventiva e inspeção anualmente;

II. O projeto, instalação e manutenção do sistema devem estar em conformidade com a norma NBR-5419-2000;

III. A função do pára-raio é proteger edificações e pessoas, não abrangendo necessariamente equipamentos eletro-eletrônicos; e

IV. Recomenda-se a utilização de protetores para os equipamentos considerados essenciais, tais como centelhadores a gás, varistores ou similares, adequados para cada tipo de equipamento.

Art.44 Os equipamentos devem estar protegidos contra falhas de alimentação elétrica, observando-se as especificações do fabricante do equipamento quanto ao fornecimento de energia:

I. É obrigatório o uso de no-break em equipamentos que suportam atividades críticas e para todos os componentes do *backbone* rede IFAM;

II. O uso de grupo-gerador em instalações estratégicas e áreas do núcleo e de distribuição da rede IFAM;

III. Para o caso dos ativos classificados com criticidade máxima o uso de Grupo-gerador é obrigatório;

IV. Para outros equipamentos em áreas sujeitos a corte do fornecimento de energia freqüentemente, sendo uma boa alternativa a aquisição de no-break com maior autonomia;

V. Para o grupo-gerador, convém que seja firmado um contrato de manutenção para que as peças e componentes do sistema estejam sempre em perfeito estado e de acordo com as recomendações do fabricante;

VI. Equipamento de rede classificado com criticidade máxima deverá dispor de N+1 fontes de alimentação, onde N é igual ao número mínimo de fontes para suportar a carga imposta pela configuração do equipamento. A fonte redundante deverá estar operacional, no modo *load sharing*, de modo que o *failover* de uma das fontes seja imperceptível;

VII. O equipamento com mais de uma fonte de alimentação recomenda-se alimentação múltipla de circuitos elétricos, de modo a evitar um único ponto de falha, correspondendo um circuito para cada fonte;

VIII.É importante que as salas de equipamentos do *backbone* da rede IFAM recebam alimentação de circuitos totalmente independentes, ou seja, diferentes dos circuitos que alimentam os prédios vizinhos. Esses circuitos devem estar interligados diretamente à rede elétrica primária do campus;

IX.Convém ainda que as salas contendo os equipamentos possuam iluminação de emergência e interruptores elétricos de emergência que permitam o desligamento em caso de necessidade; e

X. A instalação elétrica deve seguir a norma NBR-5410 "Instalações Elétricas de Baixa Tensão".

Art. 45 A segurança do cabeamento é tão importante quanto a segurança dos equipamentos de rede. Assim, é importante observar o seguinte:

I. O cabeamento de fibra óptica deve ser preferencialmente subterrâneo e, neste caso, o encaminhamento do mesmo deve ser através do sistema de dutos de uso exclusivo para este serviço;

II. A instalação de cabeamento de fibra óptica com gel em seu núcleo deve seguir as recomendações das normas vigentes;

III. O cabeamento de fibra óptica do núcleo do backbone da rede IFAM deve possuir proteção anti-roedor, sendo que a norma NBR 14773 deve ser consultada;

IV. As rotas do cabeamento de fibra óptica devem receber sinalização específica para evitar acidentes e/ou danos de terceiros. Cabe à Coordenação de Tecnologia da Informação local manter a relação e identificação das rotas dos cabos ópticos do backbone;

V. As caixas de passagem devem ser mantidas adequadas ao uso e possuir tampas de ferro com identificação; e

VI. A instalação de cabeamento, tanto em cobre quanto em fibra óptica, deve seguir as recomendações da norma NBR 14565, TIA/EIA 568-B.2-1.

Art.46 A Segurança Ambiental tem por objetivo adotar medidas que evitem risco às instalações e equipamentos por ocorrência dos seguintes fatores:

I. Incêndio;

II. Fumaça;

III. Poeira;

IV. Vibração;

V. Umidade; e

VI. Água.

Art.47 Em relação à Segurança Ambiental recomenda-se que:

I. Sensores de monitoria destes fatores estejam integrados a um sistema que permita a monitoração remota, assim como o disparo de alarme;

II. O uso de desumificador para Instalações de Infra-Estrutura de T;

III. Sejam adotados, ainda, procedimentos restringindo comida, bebida e fumo dentro das Instalações de Infra-Estrutura de TI; e

IV. De forma promover condições ao que se refere às Medidas de Segurança e Medicina do Trabalho, as seguintes normas também devem ser seguidas:

a. NR - 18 "Condições e Meio Ambiente do Trabalho na Indústria da Construção Civil"; e

b. NR – 10 “Instalações e Serviços em Eletricidade”.

Art.48 A Segurança das instalações, com relação ao acesso físico, tem como objetivos específicos:

I. Prevenir e controlar o acesso não autorizado a informações e instalações físicas do Departamento;

II. Prevenir perda, dano ou comprometimento dos ativos; e

III. Evitar a exposição ou roubo de informação e equipamento.

CAPÍTULO V

CONTROLE DE ACESSO

Art.49 As áreas restritas de Infra-Estrutura de TI devem ser equipadas com controles de entrada apropriados, de forma que somente pessoal autorizado tenha acesso liberado.

Art.50 O controle de acesso depende dos requisitos de segurança próprios da área considerada e pode ser através de:

I. Controle de entrada (métodos de acesso físico);

II. Crachás de identificação e procedimentos pelos quais o acesso é concedido, modificado ou negado;

III. Chaves e/ou cartão inteligente;

IV. Restrições de acesso baseadas no status do funcionário e horas de operação; e

V. Combinação dos itens anteriores.

CAPÍTULO VI

SEGURANÇA DO ACESSO FÍSICO AO DATA CENTER E PARA O SISTEMA DE TELEFONIA

Art. Recomenda-se que cada Departamento de Informática crie normas ou procedimentos que complementem os sistemas de segurança adotados e sugeridos:

I. Recomenda-se que o Controle de Acesso utilize como validação um sistema de cartão com PIN (*personal identification number*). Eventualmente, em locais mais críticos, pode-se optar também pela validação biométrica (impressão digital, por exemplo);

II. O fornecimento do acesso deve ser através do responsável pelo Setor;

III. O extravio ou roubo de cartões de acesso deve ser informado imediatamente à Administração do Campus para as devidas providencias;

IV. A credencial de acesso é pessoal e intransferível;

V. Mesmo durante o horário comercial o acesso com cartão é necessário para os funcionários;

V. Todas as portas externas são bloqueadas fora do horário de funcionamento;

VII. Qualquer pessoa dentro de uma área de segurança deverá dispor de identificação;

VIII. Os funcionários não podem permitir a estranhos o acesso aos *Data Centers*;

IX. Os visitantes ou funcionários sem permissão deverão pedir autorização para ter acesso e permanecer nos locais de segurança, devendo estar explícito qual o propósito de adentrar ao local, quais as atividades que serão desenvolvidas e a quais recursos estas pessoas terão acesso;

X. Serviços de terceiros no *Data Center* devem ser agendados previamente, deve ser fornecido o nome das pessoas que executarão o serviço, assim como o detalhamento da atividade a ser desenvolvida; e

XI. Tanto para o caso de terceiros quanto para visitantes, uma pessoa do Departamento deve sempre acompanhar o trabalho, de forma que um estranho nunca fique sozinho nas instalações.

Art.52 Adicionalmente convém que o Controle de Acesso utilize sistemas eletrônicos complementares:

I. Circuito Fechado de TV nas áreas consideradas estratégicas, havendo registro da imagem local por meio de câmeras de vídeo, que deverão estar sendo armazenadas em alguma mídia, de forma a poderem ser resgatadas em caso de alguma ocorrência ou auditoria; e

II. Alarme que envie alguma mensagem a uma estação de gerenciamento remota caso ocorra algum acesso não autorizado.

Art.53 Semelhante ao *Data Center*, o sistema de telefonia requer cuidados e procedimentos que visem a segurança:

I. O acesso físico ao hardware do sistema de telefonia e aos terminais de configuração de sistema é restritivo aos administradores do sistema de telefonia e ao pessoal da companhia provedora do serviço;

II. O sistema de telefonia deve estar em uma área segura que necessite de métodos de acesso especializados via chaves ou cartões eletrônicos; e

III. A instalação de novos modems deve ser coordenada pelo grupo responsável, a fim de fornecer a segurança necessária e infra-estrutura de rede para manter a segurança.

CAPÍTULO VII

ACESSO A INSTITUIÇÃO VIA CATRACA

Art.54 A Inserção, Alteração, Remoção de dados e fornecimento do acesso à Instituição via catraca será feito da seguinte forma:

I. No caso do Servidor Público deve ser através do responsável pelo Setor de Gestão de Pessoas;

II. No caso do Discente deve ser através do responsável pelo Departamento de Ensino; e

III. No caso do visitante deve ser através do responsável pelo Departamento de Administração e Manutenção.

Art.55 O extravio ou roubo de cartões de acesso deve ser informado imediatamente à Administração do Campus para as devidas providências.

Art.56 Cabe ao Departamento de Administração e Manutenção gerenciar a manutenção das Catracas.

Art.57 Cabe ao Departamento de Informática a inserção em Lote das credenciais, o fornecimento de infra-estrutura de rede e o treinamento da utilização da ferramenta.

CAPÍTULO VIII

SEGURANÇA E MANUTENÇÃO DOS EQUIPAMENTOS DE INFORMÁTICA

Art.58 A segurança dos equipamentos de informática está diretamente relacionada aos procedimentos de instalação e proteção, atentando-se ao seguinte:

I. A instalação de equipamentos deve seguir o procedimento recomendado pelo fabricante e normas específicas existentes, na falta destes, deverá ser consultado o setor responsável pela instalação elétrica da Unidade;

II. Os equipamentos devem ser instalados de modo a permitir fácil acesso à equipe de manutenção de rede;

III. A instalação deve garantir boa ventilação a seus componentes;

IV. Terminais públicos devem estar afixados via dispositivos de segurança;

V. Equipamento instalado fora das áreas de segurança deverá dispor de proteção física, como armário, gaiola, ou equivalente, com trava mecânica e/ou eletrônica, chave ou outro dispositivo que permita barrar o acesso de pessoas não autorizadas; e

VI. A instalação, manutenção e atualização de equipamentos no backbone da rede IFAM é de responsabilidade única e exclusiva do DGTI.

Art.59 Os equipamentos instalados fora dos limites da rede IFAM e interligados a ela, devem ter autorização expressa do responsável pela administração do backbone da rede IFAM para poder manter a conexão.

Art.60 Em relação à manutenção dos equipamentos deve-se observar o seguinte:

I. A manutenção de equipamentos deve ser de acordo com intervalos e especificações do fabricante. Se essas recomendações não forem conhecidas, procedimentos de manutenção devem ser elaborados e aplicados pelo Setor de Informática de cada Campus;

II. Apenas profissionais autorizados podem fazer manutenção nos equipamentos, empresas autorizadas e equipes dos Setores de Informática de cada Campus;

III. Deve ser realizado um plano de manutenção preventiva seguindo um cronograma estipulado por cada Setor de Informática;

IV. Devem ser mantidos registros de todas as falhas suspeitas ou ocorridas em toda manutenção preventiva e corretiva. É recomendado o uso de um sistema computacional com um banco de dados para estas informações, preferencialmente com acesso via web;

V. Equipamentos do Backbone enviados para manutenção de terceiros e que possuem meios de armazenamento (disco rígido, fitas, etc) devem ter seus itens checados para assegurar que toda informação sensível, sigilosa e software licenciado foi removido ou sobreposto antes da realocação do equipamento;

VI. Os demais equipamentos de Informática institucionais enviados para manutenção de terceiros devem ser devolvidos conforme suas características de configurações de hardware, software e acessórios. No caso da troca de algum item divergente, só será aceito se a configuração proposta for igual ou superior;

VII. Um hardware sobressalente deve estar disponível caso a criticidade do equipamento seja alta; e

VIII. Dispositivos de armazenamento danificados, assim como equipamentos, devem sofrer uma avaliação de riscos para verificar se eles devem ser destruídos, reparados ou descartados. Recomenda-se que cada ativo ou parte dele seja avaliado pelo Setor de Informática de cada Campus.

CAPÍTULO IX

SEGURANÇA LÓGICA OU SEGURANÇA DA INFORMAÇÃO

Art.61 Tão importante quanto a segurança física é a segurança da informação. Recomenda-se a adoção das seguintes medidas que visem proteger a integridade das informações da rede IFAM:

I. O acesso às mídias de *back/up* deve ser restrito ao pessoal autorizado;

II. O acesso ao aplicativo de *back/up* deve ser restrito ao pessoal autorizado;

III. Equipamentos, informações ou software não devem ser retirados da organização sem autorização;

IV. Toda informação registrada nos servidores de dados em mídia ou papel, deve ficar sempre guardada em locais apropriados e de acesso restrito;

V. É recomendado que uma outra cópia seja guardada fora do *backbone*, semanalmente, por meio do funcionário autorizado;

VI. Aconselha-se que seja feita uma vez por semana o back-up completo dos sistemas e, diariamente, de preferência à noite ou madrugada, a cópia incremental, ou seja, o que foi modificado; e

VII. A restauração deve ocorrer da última cópia completa até as cópias com as alterações incrementais (*layered over*), até o momento do evento.

Art.62 Sobre as contas de acesso ao sistema e a sua administração, segue:

I. Cada usuário deve possuir uma conta individual. Não deve haver contas compartilhadas por mais de um usuário, a não ser em situações específicas e prazos determinados;

II. O DGTI manterá um sistema unificado de contas dos usuários dos Sistemas integrantes da rede IFAM;

III. Novo funcionário da Instituição receberá uma conta única para acessar os sistemas necessários à execução de suas funções;

IV. A solicitação de abertura de contas em quaisquer dos sistemas se dará pelo preenchimento de um Termo de Identificação e Compromissos;

V. Após receber uma conta, cujas identificações foram criadas pelos administradores dos sistemas ou de redes, o proprietário da conta tem uma semana para alterar a seu critério essas identificações;

VI. A autorização e o nível da conta será concedido pelo proprietário e/ou administrador do sistema, ou se for o caso, pelo Setor de Informática de cada Campus;

VII. Contas de usuários que venham a se desligar da rede IFAM, tais como alunos formados, professores e funcionários, serão canceladas após um período de 180 dias da data do desligamento, salvo casos excepcionais que serão analisados pelo Setor de Informática de cada Campus;

VIII. A conta de Servidor Público deve ser composta por pelo menos um dos seus nomes Próprios. A conta deve identificar a pessoa, não podendo fazer referência a personagens fictícios, pseudônimos, pornografia e logomarcas;

IX. Toda conta de aluno sempre será identificada pela sua matricula; e

X. As penalidades, responsabilidades e atos considerados como infrações quanto ao uso das contas em quaisquer sistemas devem ser analisados pelo Setor de Informática de cada Campus aplicando as ações previstas nas normas.

Art.63 A segurança para a rede de dados sob o aspecto da segurança lógica deve considerar filtros e protocolos habilitados nos ativos:

I. Cabe ao DGTI implantar regras de proteção nos seus roteadores e firewall para proteger as redes de uma forma restritiva (método de exceção);

II. Para os roteadores do backbone da rede IFAM, os filtros e regras deverão ser obrigatórios e estudados para cada caso;

III. Para o link da RNP fornecido pelo Data Center as regras de bloqueios são gerenciadas pelo DGTI. Caso o Campus contrate um link separado ele terá total controle sobre esse link;

IV. O DGTI esta sujeito as regras do seu provedor de acesso, tanto no que tange a limitação de banda quanto à restrição a sites;

V. Os filtros e regras no firewall devem permitir apenas conexões entrantes para servidores WWW, de correio eletrônico e de nomes (DNS), sendo que exceções devem ser estudadas pelo DGTI;

VI. O acesso lógico aos equipamentos de rede (roteadores, switches, modems, servidores, ou outros) deve sempre ser protegido por senhas não-padrão (default ou inicial), quer para suporte, configuração ou gerenciamento e, preferencialmente, a partir de um número restrito de equipamentos;

VII. As senhas de acesso lógico aos equipamentos devem ser trocadas periodicamente, a cada 90 dias no máximo, ou quando o administrador ou funcionário que as detenha venha a se desligar da Instituição ou da função;

VIII. Sugerimos aos responsáveis manter um registro (log) para as alterações de configuração dos equipamentos de rede usando um software que possa realizar controle de versão;

IX. É recomendado o uso de aplicativos de gerenciamento para os equipamentos de rede e servidores, que notifiquem o administrador em casos de anomalias;

X. É recomendada a padronização das ferramentas de gerencia da rede, tendo a possibilidade de mudanças caso sejam aceitas novas ferramentas;

XI. Para o caso do gerenciamento SNMP, não deve estar habilitado se não estiver em uso, do contrário, garantir acesso estritamente aos administradores responsáveis;

XII. Também é recomendada a utilização de antivírus que monitorem as mensagens de correio eletrônico;

XIII. As informações de configuração dos equipamentos devem estar armazenadas em servidores administrativos, nunca em servidores públicos ou de produção;

XIV. Sempre que possível, os equipamentos de rede devem fazer back/up de sua configuração em servidores administrativos, buscando aumentar a segurança e confiabilidade; e

XV. Os equipamentos devem ter habilitados somente os protocolos necessários.

CAPÍTULO X

SEGURANÇA DE ACESSO REMOTO

Art.64 A permissão para o acesso remoto é fornecida pela DGTI, que deve preencher formulários, assinados pelos usuários deste serviço, atestando a ciência às normas.

Art.65 A autenticação deve ser necessariamente através de senhas, podendo estar combinada com recurso de identificação de conexão.

Art.66 A autenticação e o log de conexão de rede através de acesso remoto devem ser feitos via um sistema de relatório e autenticação centralizado.

Art.67 A utilização de fax modems, modem USB ou PCMCIA em computadores instalados na rede IFAM deve ser autorizada pela DGTI ou pelo CTI local de cada Campus. Não é recomendado o uso desses dispositivos por motivos de Segurança da Informação.

Art.68 O terminal público deve estar numa rede separada de acesso restrito, será provido apenas de um navegador de internet para disponibilizar acesso a sistemas e sites.

Art.69 Recomendamos que todos os terminais de pesquisa sejam gerenciados via software com base nas regras de negócios de cada Campus.

Art.70 Em relação à segurança para equipamentos portáteis:

I. Recomenda-se utilizar senhas de BIOS para evitar acesso não autorizado;

II. Os usuários jamais devem deixar sessões abertas, efetuando o logoff quando ele não estiver em uso;

III. Recomenda-se que dados importantes sejam protegidos por senhas e criptografia;

IV. É recomendado que o usuário utilize senhas fortes para os sistemas e equipamentos; e

V. Recomenda-se que estes equipamentos portáteis devem estar presos fisicamente através de cabos, correntes ou outro dispositivo de segurança, ou ainda, trancados em gavetas ou armários quando fora de uso.

CAPÍTULO XI

SEGURANÇA ADMINISTRATIVA

Art.71 Os usuários devem atender às seguintes diretivas básicas:

I. A utilização dos recursos de rede da Instituição só é concedida mediante a adesão dos usuários às normas e diretivas de segurança vigentes no termo adequado;

II. Os usuários devem estar cientes de auditorias, em conformidade com as diretivas de segurança; e

III. Cabe ao usuário informar ao CTI local, qualquer observação em relação a defeitos, acesso não autorizado, falhas de segurança ou afins.

Art.72 Os servidores devem ler e entender as seguintes diretrizes para lidar com incidentes:

I. Todos os incidentes de Segurança e suas soluções devem ficar registrados, sendo submetidos ao Coordenador do CTI Local;

II. O *Backbone* deve passar por um *check list* de Segurança antes de ser implantando e sua consistência deverá ser checado de 2 em 2 meses em conjunto com o Coordenador de cada Campus;

III. Cada alteração deverá ser documentada e informada ao DGTI; e

IV. O incidente deverá ser analisado entre os Coordenadores de Rede e Coordenador do Campus Local para identificar os pontos fracos da Unidade, visando prevenir incidentes futuros.

Art.73 Em relação aos ativos de rede deve-se observar o seguinte:

I. Sempre tentar identificar e documentar a causa e a solução do incidente;

II. Se uma invasão causar parada ou ruptura de serviços, a prioridade é restabelecer os serviços, porém sempre que possível, os coordenadores devem tentar identificar a origem do problema, preservando as evidências;

III. No caso de uma invasão é aconselhável rever as regras dos filtros dos roteadores, modificando-as para controlar os efeitos;

IV. Em caso de incidente que resulte em perda de dados armazenados nos servidores, o funcionário deve notificar ao Coordenador da rede imediatamente; e

V. Em caso de incidentes como falha de hardware, comprometimento do sistema ou invasões de um servidor ou outro ativo, deve-se removê-lo da rede e deixá-lo em seu estado atual a fim de permitir um trabalho de investigação eficiente.

CAPÍTULO XII

AUDITORIAS

Art.74 É importante que a Unidade adote um esquema de Auditorias. Neste caso, os servidores devem ter ciência e cooperar com os procedimentos e diretivas adotadas.

I. As auditorias serão realizadas principalmente em servidores e equipamentos de rede para assegurar a configuração e atualização adequadas;

II. Os auditores só podem ser servidores do CTI local ou DGTI;

III. Auditorias nas linhas telefônicas devem ocorrer regularmente para verificar a funcionalidade dos modems existentes e para identificar os não autorizados;

IV. As auditorias em sistemas de usuários seguirão as diretivas adotadas; e

V. As auditorias podem ser notificadas ou não.

Art.75 As auditorias notificadas são anunciadas previamente aos servidores, de modo que tenham tempo para preparar o ambiente e rever suas práticas. Seus propósitos são:

I. Analisar os sistemas em relação aos componentes de segurança;

II. Verificar se as práticas dos usuários são impróprias ou desafiam a segurança e se ocorrer notificar o Chefe Imediato; e

III. Assegurar que as informações são apropriadas e cumprem aos objetivos.

Art.76 As auditorias não anunciadas São aleatórias, buscando a identificação de vulnerabilidades e a constante conscientização com a segurança. Podem ser implementadas na forma de ataques simulados, desde que permaneçam no escopo da rede local.

TÍTULO VII

USO DAS CONTAS DE CORREIO ELETRÔNICO

CAPÍTULO I
REGRAS E DIRETRIZES PARA O USUÁRIO PARA USO DO CORREIO ELETRÔNICO

Art.77 A formatação de Contas do Correio Eletrônico deve obedecer as seguintes recomendações:

I. As contas dos setores devem estar de acordo com a ~~seguir a seguinte~~ formatação dada no exemplo: setor_siglacampus@ifam.edu.br;

II. As contas dos Servidores Públicos ativos e inativos devem estar de acordo com a seguinte formatação:

a. nome@ifam.edu.br;

b. partenome@ifam.edu.br;

c. sobrenome@ifam.edu.br; e

d. nome.sobrenome@ifam.edu.br.

III. As contas dos serviços devem identificar o serviço, utilizando como exemplos:

a. postmaster@ifam.edu.br;

b. mailerdaemon@ifam.edu.br;

c. webmaster@ifam.edu.br;

d. faleconosco_cmzl@ifam.edu.br; e

e. update_cmdi@ifam.edu.br.

IV. As contas de eventos temporários devem identificar o evento e ficarão validas por 365 dias após o término do mesmo, utilizando como exemplos:

a. volimpiadamat@ifam.edu.br; e

b. olimpiadamat5@ifam.edu.br.

V. As contas de prestação de serviço temporário deverão identificar a pessoa e serviço, ficarão ativas 180 dias após o término do vínculo e devem seguir a formatação como no exemplo: maria_ead@ifam.edu.br; e
VI. As contas de alunos devem ser suas matriculas de curso.

Art.78 São deveres dos usuários do correio eletrônico:

I. O Usuário deve evitar o uso do sistema de correio eletrônico para finalidades que não sejam do escopo da Instituição;

II. O Usuário não deve utilizar o sistema de correio eletrônico para *spam*;

III. O Usuário deve manter atualizados seus dados dentro da ferramenta de email;

IV. O Usuário não deve utilizar o sistema de correio eletrônico para enviar correntes, pirâmides, boatos, e outros;

V. O Usuário não deve utilizar o sistema de correio eletrônico para molestar, intimidar, assediar ou difamar outras pessoas;

VI. O Usuário deve evitar seu envolvimento em discussões ou polêmicas ("*flame wars*") com outros Usuários de correio eletrônico (internos ou externos);

Art.79 São responsabilidades dos usuários do correio eletrônico:

I. O titular da conta tem total responsabilidade pelo uso da mesma;

II. É de exclusiva responsabilidade do usuário o conteúdo do email e arquivos; e

III. É de responsabilidade da DGTI manter o sistema de email funcionando.

Art.80 São recomendações aos usuários do correio eletrônico:

I. Recomenda-se que o usuário no envio de emails com anexos, procure utilizar ferramentas de compactação de arquivos ou arquivos de formatos reduzidos. Exemplos: .zip, .rar, .pdf, .jpg, entre outros;

II. Recomenda-se que o usuário não responda e-mails incluindo os anexos recebidos;

III. Recomenda-se que o usuário não envie emails com arquivos anexos a listas de email; e

IV. Recomenda-se que o usuário apague emails desnecessários e, principalmente, os que possuam anexos.

CAPÍTULO II

REGRAS E DIRETRIZES PARA O COORDENADOR DE REDE

Art.81 São deveres do Coordenador de Rede

I. O Coordenador deve verificar periodicamente a conta *postmaster*, para detectar eventuais problemas que possam estar ocorrendo no servidor e na entrega de e-mail dos usuários;

II. É obrigatória a criação das contas "*security*" e "*abuse*" nos servidores de domínio;

III. Todo servidor de correio eletrônico deve ter nome e reverso configurado de maneira correta no DNS;

IV. O Administrador de um serviço oferecido pelo IFAM deve seguir as Orientações para Difusão de E-mails criada pela CCS, quando do envio de e-mails em grandes quantidades para docentes, servidores e alunos da Instituição;

V. O Administrador deve configurar o servidor de correio eletrônico de maneira a evitar problemas do tipo "*open-relay*", "*open-proxy*", "*formmail*" e outros;

VI. A leitura dos emails deve ser somente feita por mecanismos do tipo POP3, IMAP, HTTP (*Webmail*), de preferência utilizando as versões mais seguras desses protocolos APOP, SMTP-AUTH, POP com SSH, HTTPS;

VII. O Administrador não deve ler mensagens de seus usuários; e

VIII. O Administrador deve checar periodicamente o servidor de correio eletrônico para determinar se existem endereços de e-mail inválidos nas listas disponibilizadas pelo servidor. Se a lista for administrada por outra pessoa, o Administrador deve contatá-la para que seja feita a remoção desses endereços inválidos.

CAPÍTULO III

DAS LISTAS DE DISCUSSÃO E DE DISTRIBUIÇÃO

Art.82 Referentes às listas de discussão devem ser observados os seguintes itens:

I. O Administrador deve configurar um tamanho máximo para todas as mensagens que circulem através do servidor de listas;

II. O Administrador deve remover endereços inscritos em listas de discussão, caso eles estejam retornando;

III. O acesso a configuração do servidor de listas e principalmente aos seus inscritos deve ser rigorosamente controlado e limitado apenas ao Administrador (ou dono) da lista; e

IV. O Administrador deve configurar o servidor de listas para que em todos os emails que circulem por ela seja incluída informação ao usuário de como ele deve proceder para se descadastrar da lista, contactar um Administrador, receber outras informações, etc.

V. O Administrador do servidor de lista de discussão pode delegar a outras pessoas (Usuários que pertençam a Instituição) a administração de uma determinada lista. Essa pessoa ficará encarregada da sua manutenção (inclusão/remoção de usuários, moderação, etc.); e

VI. Recomenda-se que uma lista de discussão só seja composta por usuários que tenham optado por sua inscrição.

Art.83 As seguintes recomendações devem ser seguidas pelo Administrador da Rede:

I. Recomenda-se que o servidor de correio eletrônico seja configurado para enviar email só após a autenticação do Usuário, utilizando configurações do tipo "smtp auth", "smtp after pop", etc;

II. Recomenda-se que o Administrador implemente medidas para filtragem de vírus no sistema de correio eletrônico;

III. Recomenda-se que o Administrador implemente medidas para filtragem de spam e emails indesejados (correntes, mensagens pornográficas, propagandas, etc.) no sistema de correio eletrônico;

IV. Recomenda-se que o Administrador implemente medidas para limitar o tamanho das caixas postais de seus usuários, por exemplo, utilizando um mecanismo de quota;

V. Recomenda-se que o servidor de correio eletrônico seja configurado de forma que o Usuário não tenha acesso de "login" ao servidor; e

VI. Recomenda-se que o Administrador monitore o funcionamento do servidor de correio eletrônico, em termos de número de conexões, número de mensagens enviadas e recebidas, número de mensagens bloqueadas, banda consumida na rede, etc.

Art.84 Referentes às listas de distribuição devem ser observados os seguintes itens:

I. Não usar para fins políticos, comerciais, religiosos, homofônicos, racistas, preconceituosos de qualquer natureza que venham denegrir a imagem da Instituição;

II. Recomenda-se que o envio de seja feito utilizando o recurso de Copia Oculta (CCO); e

III. Serão geradas listas padrões para os servidores ativos (Professores e Técnico-Administrativos) e inativos.

Art.85 São consideradas infrações no uso dos recursos computacionais oferecidos:

I. Fornecer a senha de acesso a externos;

II. Utilizar os recursos oferecidos com fins comerciais;

III. Utilizar software ou procedimentos para conseguir acesso não autorizado a recursos ou informações, ou para degradar o desempenho, ou para colocar fora de operação sistemas computacionais locais ou remotos;

IV. Armazenar arquivos de conteúdo ilegal ou considerados abusivos;

V. Comportamento ofensivo ou impróprio no tratamento com outros usuários ou grupos, locais ou externos. A definição de impropriedade fica a cargo dos grupos ou usuários;

VI. Utilizar os recursos para "spam" que é o envio de "malas diretas" e propagandas;

VII. Envolver-se em qualquer atividade que infrinja ou boicote a política de segurança; e

VIII. Violar outras regras e diretrizes de usuários ou administrador previstas nos documentos da "Política de Informática do IFAM".

Parágrafo único. A cada infração deverá corresponder uma ação administrativa, de acordo com o seguinte:

a. Primeira infração: comunicado por escrito;
b. Segunda infração: comunicado por escrito para chefe imediato; e
c. Terceira infração: a ação será aplicada de acordo com a infração cometida, que poderá incluir, entre outras ações administrativas, a restrição de serviços (bloqueios de envio ou recebimento, acesso a listas de distribuição, bloqueio de anexos, diminuição da quota, diminuir quantidade de copias por emai).

TÍTULO VIII

COMPUTADORES DE USO PESSOAL E SERVIÇOS DA REDE

CAPÍTULO I

DA UTILIZAÇÃO DE COMPUTADORES DE USO PESSOAL

Art.86 O usuário é responsável por todas as atividades no seu computador pessoal. Portanto, ele deve agir de acordo com as regras observando as seguintes diretrizes:

I. Somente utilizar o computador pessoal na rede IFAM para as atividades de uso acadêmico, desenvolvimento de ensino e pesquisa e atividades administrativas relacionadas à Instituição;

II. Responsabilizar-se pela manutenção de seu recurso Computacional (Hardware e Software);

III. Responsabilizar-se, ainda, pelo software (sistema operacional, utilitários, aplicativos e arquivos criados/instalados no microcomputador);

IV. Recomenda-se instalar software licenciado;

V. Instalar software livre ou arquivos, desde que não prejudiquem a performance da rede;

VI. Sempre notificar imediatamente ao administrador as ocorrências com o computador, quer seja invasão, dano ou roubo;

VII. A utilização de modem usando conexão discada em seu computador deve ser autorizada pelo DGTI ou CTI local;

VIII. Não manipular líquidos ou substâncias que possam danificar o equipamento quando os estiver operando, assim como não fumar;

IX. Informar ao CTI ou DGTI local sobre equipamentos pessoais para o Campus quando a intenção é integrar recursos compunacionais do Instituto ;

X. Recomenda-se back-up (cópia de segurança) dos arquivos pessoais instalados em seu computador pessoal, e outros dispositivos tais como pendrive, HD externo;

XI. Recomenda-se a instalação e atualização de antivírus e patches de correção no Sistema Operacional e aplicativos instalados em seu computador pessoal; e

XII. Recomenda-se que não tragam seus equipamentos de uso pessoais tais como; Desktops, Impressoras, Scanners, Nobreak, Estabilizadores, se caso houver necessidade Institucional deve ser formalizado junto a Administração do Campus.

Art.87 Cabe ao administrador dos recursos seguir as seguintes diretrizes:

I. Sempre que possível, disponibilizar ao usuário patches atualizados e antivírus para que o usuário faça a instalação e atualização em seus computadores pessoais;

II. Problema não informar ao usuário onde adquirir a manutenção adequada;

III. Cadastrar o computador pessoal do usuário em domínios, sub-domínios ou Grupos de Trabalho pré-definidos para tais fins. Esse cadastro depende do perfil do computador pessoal na Rede IFAM; e

IV. O Computador pessoal deve estar configurado em uma rede separada dos computadores administrativos e acadêmicos.

CAPÍTULO II

USO DE SERVIÇOS *FTP*

Art.88 O usuário, utilizando o serviço de FTP, deve atentar para as seguintes regras básicas:

I. A senha é de uso exclusivo do usuário; e

II. Não executar comandos que comprometam a segurança do sistema, tais como comandos que geram ou podem gerar em loop (laço).

Art.89 O serviço de FTP deve estar desabilitado nos servidores que não o utilizem, do contrário, as seguintes regras devem ser seguidas pelo administrador da rede:

I. Monitorar os *logs* para detectar atividades suspeitas e impedir que o serviço seja usado indevidamente;

II. Eliminar o acesso anônimo;

III. Jamais disponibilizar no servidor de FTP material pornográfico, software comercial ou pirata ou qualquer material considerado abusivo;

IV. Controlar o acesso por classe de usuários;

V. Utilizar mensagens de advertência aos usuários, informando que as transações são registradas e podem ser monitoradas;

VI. Dar preferência a isolar o servidor de FTP dos outros servidores públicos (e-mail, DNS, WWW, entre outros);

VII. Recomenda-se o uso de *proxies*;

VIII. Manter o servidor de FTP sempre com a versão mais atual e com os *patches* de correção aplicados; e

IX. Participar de listas de discussão para acompanhar alertas de segurança.

CAPÍTULO III

UTILIZAÇÃO DA REDE

Art.90 Ao utilizar a rede IFAM, que está sob a responsabilidade da DGTI e CTI's e é composta pela rede de Pesquisa, rede Acadêmica, Recad (Rede Computacional Administrativa), Rede de Serviços (VOIP, Vídeo Segurança e outros) e Rede Pública (Telecentro, Terminais Públicos, Access Points, sala de aulas, bibliotecas e outros), o usuário deve seguir as seguintes diretrizes:

I. Não distribuir arquivos do tipo correntes ou manifestos, pois esses podem causar excessos tráfego na rede;

II. Não será permitido o uso do compartilhamento de pastas, a não ser que seja com autenticação e certificando-se que esta livre de vírus;

III. Não utilizar ou disponibilizar para fins particulares ou de recreação, serviços que comprometam os recursos e desempenhos das redes de computadores, tais como: jogos, músicas, vídeo, filmes e software comercial;

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

V. Não interceptar a transmissão de dados através da rede, exceto com solicitação para fins acadêmico ou institucional, com prévio conhecimento da CTI local;

VI. Não desenvolver, manter, usar ou divulgar meios que possibilitem a violação da rede de computadores da Instituição, exceto com solicitação para fins acadêmico ou institucional; e

VII. Não colocar um hub, switch, roteador sem fio ou qualquer equipamento em um ponto de rede para ampliar o número de pontos de rede da sala ou laboratório, exceto com solicitação para fins acadêmico ou institucional.

Art.91 Cabe ao administrador zelar pelo bom funcionamento da rede observando o seguinte:

I. Sempre fazer uso de ferramentas para monitorar a rede da Unidade;

II. Proteger os serviços de rede utilizando ferramentas apropriadas, como firewall, *Proxy*, Sistemas de Detecção de Intrusão entre outros;

III. Sugere-se que o administrador divida as redes muito grandes em sub-redes, cada uma protegida por um perímetro de segurança;

IV. Cada campus terá a sua sub-rede falsa;

V. Cada CTI ou GTI terá comunicar o uso de outras ferramentas como NAT (*Network Adress Translation*) para o DGTI, cuidando do gerenciamento dos logs e responsabilizando-se pela identificação do usuário na eminência de alguma atividade tida como ilícita;

VI. Comunicar ao DGTI, DTI ou CTI local a instalação ou adoção de redes Wireless;

VII. Consultar o DGTI sobre o uso da VPN;

VIII. Bloquear o acesso a conteúdo que violem as leis federais, estaduais e municipais ou qualquer item desta política;

IX. Fazer a atualização de *patches* e erratas nos equipamentos de rede (*switches*, *hubs* e roteadores);

X. 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);

XI. Limitar ao máximo a divulgação de informações de roteamento, faixa de IP, servidores, equipamentos de rede, entre outros, a terceiros;

XII. Não é permitido desenvolver, manter, usar ou divulgar meios que possibilitem a violação de rede de computadores da Instituição, exceto com solicitação para fins acadêmico ou institucional; e

XIII. Consultar o DGTI, DTI ou CTI local quando tiver dúvidas.

Art.92 Cabe ao administrador bloquear sites conforme:

I. Quando o site disponibilizar conteúdo com finalidades particulares que possam ir contra aos interesses Institucionais, tanto Acadêmicos quanto Administrativo, tais como: pedofilia, pornografia, software não licenciado (programas, imagens, músicas, textos, áudio, vídeo e filmes) ou outro meio que comprometa a imagem da Instituição;

II. Site de downloads que possam ser utilizados para violar direitos autorais; e

III. Haverá controles de acesso a serviços da rede e de banda diferenciados nas redes.

Art.93 Nas redes de Pesquisa, Acadêmica e Administrativa ~~podem~~ por motivo de limitação de banda, ou seja, sobrecarga da saída principal, o coordenador deverá bloquear sites ou programas na seguinte ordem levando em consideração o tráfego e o tipo de serviço em cada rede:

I. Sites de Vídeos e Áudio;

II. Web *Proxy*'s;

III. Sites de Downloads de Softwares;

IV. Trafego P2P; e

V. Redes Sociais.

Art.94 Os coordenadores de CTI's podem bloquear em cada *Campus* sites e serviços específicos que estejam afetando somente aquele *Campus* ou se o *Campus* não tiver uma saída de rede que suporte o tráfego;

Art.95 O coordenador de Rede ou do CTI poderá liberar serviços, sites e programas em horários específicos (Intervalo de Almoço, Intervalo de Turno e outros), sempre levando em consideração o não prejuízo das atividades administrativas e acadêmicas.

Art.96 Os Chefes de Departamentos podem solicitar bloqueios específicos para o seu Setor, mediante solicitação por escrito enviada para a Coordenação de TI.

CAPÍTULO IV

PLANO DE CONTINGÊNCIA E CONTINUIDADE DO NEGÓCIO

Art.97 Com relação aos elementos que impactam diretamente sobre a rede IFAM, a contingência pode ser classificada em média, alta e altíssima.

Art.98 Na contingência média é aceitável a disponibilidade em horário comercial, podendo ser interrompida eventualmente.

§ 1º. Com relação à contingência para Servidores são recomendadas as seguintes ações:

I. Procedimentos de Back/up regulares;

II. Contrato de manutenção de Hardware (5x8);

III. Na falta de contrato de manutenção, possuir peças de reposição e pessoal técnico para atuar;

IV. Manutenção de patches atualizados; e

V. Disco de boot espelhado (mirror).

§ 2º. Com relação à contingência para outros Ativos de Rede são recomendadas as seguintes ações:

I. Contrato de manutenção de Hardware (5x8) e elemento de back-up; e

II. Na falta de contrato de manutenção, possuir hardware de back-up e pessoal técnico para atuar.

Art.99 Na contingência alta é requerida disponibilidade 24 horas por dia e 7 dias por semana (24X7), podendo ser interrompida eventualmente.

§ 1º. Com relação à contingência para Servidores são recomendadas as seguintes ações:

I. Procedimentos de Back-up regulares;

II. Cópia de segurança armazenada em 2 tipos diferentes de mídia;

III. Contrato de manutenção de hardware (24x7);

IV. Na falta do contrato de manutenção, possuir outro hardware idêntico e pessoal técnico em regime de plantão;

V. Manutenção de patches atualizados;

VI. Todos os discos espelhados;

VII. Placas de rede redundantes; e

VIII. Utilização de No-Breaks.

§ 2º. Com relação à contingência para outros Ativos de Rede são recomendadas as seguintes ações:

I. Contrato de manutenção de hardware (24x7);

II. Na falta do contrato de manutenção, possuir outro hardware idêntico e pessoal técnico em regime de plantão; e

III. Alimentação através de no-break.

Art.100 Na contingência altíssima é requerida disponibilidade 24 horas por dia e 7 dias por semana (24X7) sem interrupções.

§ 1º. Com relação à contingência para Servidores são recomendadas as seguintes ações:

I. Procedimentos de Back-up regulares;

II. Cópia de segurança armazenada em 2 tipos diferentes de mídia;

III. Armazenamento das mídias de back-up em local físico alternativo;

IV. Contrato de manutenção de hardware (24x7);

V. Manutenção de patches atualizados;

VI. Todos os discos espelhados;

VII. Placas de rede redundantes;

VIII. Fontes de alimentação do hardware redundantes;

IX. Utilização de Grupo gerador e no-break;

X. Hardware idêntico em espera (Standby) com Failureover automatizado por serviço;

XI. Ambiente alternativo em local físico diferente do principal cujo tempo de disponibilização por serviço não ultrapasse 8 horas; e

XII. Pessoal técnico distribuídos em plantão.

§ 2º. Com relação à contingência para outros Ativos de Rede são recomendadas as seguintes ações:

I. Contrato de manutenção de hardware (24x7);

II. Pessoal técnico em plantão;

III. Hardware com fonte redundante;

IV. Hardware idêntico em espera (Standby) utilizando protocolo VRRS no caso de roteadores; e

V. Alimentação através de grupo gerador e no-break.

Art.101 Como critério para aplicação recomenda-se que os níveis de contingência sejam definidos através da pontuação dos ativos quanto a criticidade.

O critério sugerido pela tabela GUTA é:

a. Pontuação = 625 ---------- Contingência altíssima;

b. Pontuação >= 256 e < 625 --------- Contingência alta; e

c. Pontuação > 81 e < 256 ---------- Contingência média.

Art.102 Recomenda-se que todos os atores de cada sistema possuam procedimentos alternativos (manuais) independentes do fluxo normal do sistema para aqueles processos que forem qualificados como críticos por demandarem ônus jurídico ou financeiro para a Instituição.

Art.103 Deverão ser testados a intervalos regulares todos os níveis de contingência implantados e homologados pelas equipes técnicas envolvidas.

Art.104 Os itens técnicos definidos em cada nível de contingência deverão ser revistos ou modificados sempre que houver uma melhoria tecnológica à disposição.

CAPÍTULO V

SERVIÇOS E UTILIZAÇÃO DE DNS

Art.105 A responsabilidade da Administração do DNS (*Domain Name System*) ifam.edu.br é da DGTI, sendo ele o responsável legal pelo bloco de IP 200.129.168.0/24 que deve atender somente pelo dns *.ifam.edu.br.

Art.106 Cabe à DGTI administrar o domínio "*.ifam.edu.br" e seus sub-domínios. Um *Campus* pode requerer o registro de um sub-domínio.

Art.107 Não serão declarados equipamentos de outras redes nos servidores DNS da Instituição. Também não deverá haver registro de domínio "ifam.edu.br" em máquinas não pertencentes à Rede IFAM ou que não estejam sobre o bloco de IP do IFAM.

Art.108 O título V, referente aos sub-domínios da Rede IFAM deve ser consultada. Para domínios não contidos nesta Resolução, a DGTI deverá ser consultada.

Art.109 São deveres do Administrador de DNS:

I. Fornecer informações aos Usuários que permitam a configuração correta do DNS em seus computadores (quais servidores utilizar na resolução de nomes e que nome de domínio colocar);

II. Manter o servidor de DNS configurado de forma correta e eficiente;

III. Seguir recomendações da DGTI ou DTI ou CTI quanto a versão do servidor de DNS;

IV. Manter um "reverso" para todos os computadores pertencentes ao sub-domínio do IFAM;

V. Comunicar ao Diretor da DGTI as alterações que forem feitas na configuração das zonas (mudanças de IPs e nomes dos servidores DNS) dos sub-domínios cuja responsabilidade lhe foi delegada;

VI. Manter o registro SOA corretamente configurado para o sub-domínio, em relação aos parâmetros temporais e também ao endereço de e-mail para contato;

VII. Manter atualizados os Contatos Administrativo, Técnico e de Segurança pertinentes ao seu sub-domínio, no sistema disponibilizado pelo DGTI e pelo Registro BR para essa finalidade (servidor WhoIs);

VIII. Evitar a utilização de registros do tipo TXT ou HINFO, pois estes permitem que alguém obtenha de forma remota informações adicionais sobre os computadores da rede (fabricante do computador, sistema operacional instalado, etc.);

IX. Configurar seu servidor para limitar o número de computadores que tem permissão para fazer a leitura das zonas (transferência de zonas ou AXFR);

X. Configurar seu servidor para que não seja possível fazer a leitura da versão instalada;

XI. Auxiliar a Unidade que deseje criar um sub-domínio como proceder; e

XII. Computadores que se utilizam de acesso remoto para se conectar a Instituição devem ter nomes que identifiquem claramente esse tipo de acesso, de preferência devem pertencer a um subdomínio reservado a essa finalidade. Isso facilita a criação de regras de bloqueio baseadas em nomes. Exemplos de nomes que podem ser utilizados: tty21.dialup.ifam.edu.br, 54-45-107.143.dsl.ifam.edu.br, etc.

Art.110 O Usuário deve configurar seu computador para que ele procure nomes em pelo menos dois servidores de DNS (primário e secundário). Isso só quando o IP estiver alocado de maneira fixa no computador do usuário.

CAPÍTULO VI

SERVIÇOS E SERVIDORES WEB

Art.111 O coordenador de Rede é a pessoa **e equipe** que é responsável pela instalação e configuração do software que estará disponibilizando conteúdo WWW.

Art.112 As regras e diretrizes referentes ao Administrador de Serviços WWW são as seguintes:

I. Seguir as diretrizes definidas pela CCS (Coordenação de Comunicação Social) que se referem a serviços WWW, como por exemplo, a "Resolução sobre Propagandas na WWW do IFAM";

II. Não disponibilizar dados de uma pessoa na WWW sem o prévio consentimento desta. Particular atenção deve ser dada a endereços de e-mail, que uma vez publicados, podem servir de alvo para o envio de spam;

III. Observar todos os direitos autorais e de propriedade intelectual ao publicar algo na WWW;

IV. Serviços WWW que coletam dados através de formulários e cookies devem apresentar aos mesmos informações sobre como a informação será tratada e armazenada pelo sistema; e

V. Serviços WWW que coletam endereços de e-mail para envio de mensagens aos usuários (por exemplo, uma newsletter) devem fornecer um método para que o usuário possa remover seu endereço do cadastro caso não deseje mais receber as mensagens. A instrução de como fazer esse descadastramento deve aparecer na página WWW e na mensagem enviada por e-mail. A mensagem deve ser enviada com um endereço válido de retorno, e o Administrador deve verificar periodicamente esse endereço para excluir endereços de usuários inválidos ou que não existam mais.

Art.113 Os deveres referentes ao Administrador de Servidores WWW são os seguintes:

I. Proteger de forma adequada o conteúdo fornecido, seja configurando adequadamente as permissões do sistema de arquivos (file-system) onde os dados se encontram, seja provendo mecanismos de acesso do tipo user/password, ou mesmo fornecendo acesso criptografado aos dados.

II. Ter cuidado ao configurar *proxies* WWW, pois um *proxy* mal configurado pode ser utilizado para envio de *spam* (open *proxy*).

Parágrafo Único. Recomenda-se que os servidores WWW só ofereçam esse serviço.

Art.114 As recomendações para o Usuário são as seguintes:

I. Evitar o uso do browser WWW para finalidades que não sejam de interesse da Instituição; e

II. Evitar o fornecimento de dados institucionais (e-mail, telefone e outros) em sites que não sejam de fins institucionais, pois essas informações podem ser utilizadas para finalidades indevidas, como o envio de propaganda ou spam.

TÍTULO IX

REDES MÓVEIS E ATIVOS DA REDE IFAM

CAPÍTULO I

IMPLANTAÇÃO E UTILIZAÇÃO DE REDES MÓVEIS

Art.115 Quando nos referimos a comunicação móvel, não estamos considerando as possibilidades que derivam de comunicações de dados através de *backbones* fora da Rede IFAM, como o que pode advir através do uso de dispositivos móveis (PDAs) com interfaces para redes de dados de 2,5G ou 3G, enquanto estas redes não tiverem provimento através da Rede IFAM. Se e quando isto vier a ocorrer, as recomendações precisarão ser atualizadas para incorporar este fato.

Art.116 A equipe da DGTI ou DTI ou CTI local de seu campus é responsável pela tarefa de configuração adequada dos acessos e de implementação de políticas de *backbone* relacionadas.

Art.117 As medidas apresentadas a seguir descrevem procedimentos buscando garantir a autenticação, autorização e confidencialidade dos dados numa comunicação no contexto de redes móveis. Essas medidas podem ser resumidas através das seguintes recomendações de caráter geral:

I. Implementar mecanismos de autenticação baseados em usuário, ao invés de baseados nos dispositivos;

II. Implementar gerenciamento centralizado de senhas, grupos e políticas de acesso;

III. Implementação de chaves de cifragem dinâmicas, baseadas na sessão;

IV. Autenticação mútua da base e do dispositivo móvel, isto Significa que a base autentica o usuário e este autentica a base; e

V. Prospecção regular pelos administradores da rede (scanning) em busca de dispositivos não autorizados.

Art.118 As regras e diretrizes referentes ao usuário são as seguintes:

I. O usuário não deve emprestar dispositivos institucionais móveis ou divulgar dados de configuração para acesso em redes móveis por terceiros;

II. Se um dispositivo for de uso coletivo (ex: *laptop*), a lista com os usuários (cadastro) desse dispositivo deverá ser fornecida ao administrador da rede local e o responsável pelo dispositivo deverá manter um controle de quem está utilizando o dispositivo, podendo vir a ser requisitado a respeito; e

III. Indiretamente, recomenda-se que o usuário evite o fornecimento de dados pessoais em sites WWW ou outros meios de divulgação, pois essas informações podem ser utilizadas para violações: uma vez que os dispositivos móveis são também objetos pessoais, ali podem estar contidas informações que levam a vulnerabilidades, se os usuários vierem a utilizá-las nas suas senhas de acessos.

Art.119 Os deveres referentes ao Administrador são os seguintes:

I. O Coordenador da Rede deve proteger de forma adequada o conteúdo fornecido, seja configurando adequadamente as permissões do "file-system" onde os dados se encontram, seja provendo mecanismos de acesso do tipo user/password, ou mesmo fornecendo acesso criptografado aos dados; e

II. De modo geral, o Coordenador da rede de acesso deve estar informado das vulnerabilidades que decorrem o uso de um sistema sem fio ou móvel em sua rede local, devendo buscar nas recomendações (RFCs e normas) a melhor implementação, no sentido maximizar praticidades de uso e segurança, fatores normalmente conflitantes. Por se tratar de uma tecnologia recente, a inclusão de mobilidade no sistema importará maior atenção aos logs nos roteadores de acesso, que deverão ser inspecionados com maior regularidade.

Art.120 Relaciona-se a seguir as recomendações, em ordem decrescente de relevância e facilidade, que podem vir a ser implementadas como proteção da rede local e de seus usuários:

I. Habilitar WPA2. Configurar o AP para que se conecte ao servidor radius da Rede IFAM;

II. Ao se posicionar AP deve-se evitar a colocação das mesmas próximas à áreas de que possibilitem grande exposição dos sinais, para usuários que não são os usuários potenciais do sistema. Assim é que, deve-se evitar a colocação de AP próximos a pontos de janela, nas laterais de uma edificação e nos AP’s que atendem somente a setores específicos do

Campus deve-se observar a intensidade do sinal e a potencia do sinal irradiado;

III. Mudar o SSID default (pré-configurado) na AP. Repetem-se as razões do item anterior;

IV. Desabilitar broadcast de SSID na AP (se o ponto de acesso implementar essa característica);

V. Mudar periodicamente a senha do roteador, ao qual a base wireless está conectada;

VI. Utilizar um nível adicional de autenticação para as associações com os pontos de acesso através de servidores de autenticação (RADIUS). Quando disponível, utilizar equipamentos que de acesso de rede que implementam o padrão 802.1X. Esses dispositivos travam a porta no endereço MAC autenticado, o que impede que uma base clandestina seja instalada na rede local, utilizando um ponto de rede "disponível";

VII. Não utilizar DHCP no roteador, onde a rede wireless está conectada. Preferir utilizar o DHCP da rede IFAM ou do Campus;

VIII. Utilizar pontos de acesso que implementem WPA2 com chaves de 128 *bits*;

IX. Preferir pontos de acesso com firmware em memória flash, que permitirão a sua atualização com a evolução dos padrões de segurança;

X. Pesquisar periodicamente a existência de bases clandestinas nas áreas de cobertura de interesse;

XI. Ao alocar as bases na rede corporativa, investigar o quanto um sinal de dentro do prédio pode ser captado pelo lado de fora, pelo uso de uma antena de alto ganho e software de captura apropriado; e

XII. Somente será permitido o uso de redes Ad-Hoc integradas a Rede IFAM com fins Institucionais, acadêmicos e administrativos.

CAPÍTULO II

PONTUAÇÃO DOS ATIVOS DA REDE IFAM E CRITICIDADE DE SERVIÇOS

Art.121 A Técnica de Execução para estabelecer pontuação dos ativos Rede IFAM quanto a criticidade relativa aos serviços que cada um oferece e estabelecer a criticidade relativa entre os serviços oferecidos por cada ativo Rede IFAM é a seguinte:

I. Reunir o corpo técnico envolvido com o assunto (ativos e seus serviços) e apresente os itens a serem abordados;

II. Cada participante deverá dar notas de 01 a 05 para cada item (pontuar), quanto a sua influência com relação ao assunto abordado em termos de sua gravidade (G), urgência (U) e tendência (T) de agravamento;

III. Também deverá ser dada um nota de 01 a 05 com relação a abrangência (A) do ativo sobre a Rede IFAM, sendo nota 05 quando a abrangência for maior;

IV. Tire a média das notas dadas pelos participantes para cada item para gravidade, urgência, tendência e abrangência; e

V. Multiplique para cada item as médias obtidas para gravidade, urgência, tendência e abrangência e estabeleça a prioridades dos itens. Quanto maior o valor obtido, maior a prioridade do item.

Art.122 A avaliação dos resultados deve ser considerada da seguinte forma:

I. Pontuação acima de 256 até 625: ativos em que devem se concentrar as atenções e esforços quanto à segurança e providências quando ocorre alguma falha;

II. Pontuação entre 81 e 256: ativos que merecem atenção especial mas depois de atendidas as necessidades dos pontuados acima desta faixa;

III. Pontuação abaixo de 81: ativos que não oferecem grandes prejuízos quando em situação de falha; e

IV. Para orientações sobre a pontuação com relação à criticidade, ver o Anexo II (tabela para o critério de pontuação).

Art.123 Para o preenchimento do formulário (anexo III) para estabelecer a criticidade dos ativos relativa aos serviços que cada um oferece, deve-se observar o seguinte:

I. O preenchimento do Formulário deve seguir as orientações do documento, podendo ser em equipe ou individual;

II. O campo "Identificação" deve ser usado para número de série, patrimônio, localização ou outro dado que facilite a identificação; e

III. Se o Ativo pertence ao backbone Rede IFAM, é obrigatório o seu cadastro na árvore LDAP ou no CACIC.

TÍTULO X
DAS DISPOSIÇÕES GERAIS

Art.124 Os casos omissos devem ser submetidos ao CETI/IFAM .

ANEXO I
TERMINOLOGIA

- Coordenador de Rede, detentor, ou dono do Serviço: pessoa, grupo de pessoas ou órgão/seção responsável pelo serviço.
- Administrador de Rede, detentor, ou dono do Serviço: pessoa, grupo de pessoas ou órgão/seção responsável pelo serviço.
- Computador Pessoal: Equipamento que contém um Sistema Operacional e programas específicos que auxiliam na interação homem-máquina para realização de atividades relacionadas à pesquisa, ao desenvolvimento tecnológico e as Atividades administrativos.
- Contato: Pessoa de contato das Unidades ou Centros de Informática com os órgãos centrais de administração de informática da Instituição. O contato pode ser o próprio administrador.
- Contingência: é o conjunto de configurações e procedimentos estabelecidos para manter a disponibilidade dos sistemas, bem como a continuidade do negócio.
- Equipamento: compreende servidor de rede, microcomputador, PABX, ativo de rede, entre outros, pertencentes às Instalações de Processamento.
- HTTP: (*Hyper Text Transfer Protocol*) Protocolo cliente/servidor usado para acessar informações na *World Wide (Web*).
- Instalação de processamento: é o local onde se localiza os equipamentos do núcleo da rede IFAM, local de equipamentos da camada de distribuição, sala onde estejam instalados servidores de rede ou outra área cujos danos causem a interrupção de atividades essenciais.
- Informação: refere-se a cópia de segurança (*back/up*), dados corporativos, banco de dados com material de pesquisa ou afim, etc., armazenada em algum tipo de mídia magnética, óptica ou eletrônica.
- Norma de Uso do Serviço: Norma aplicada a um serviço específico, por exemplo, Norma de Uso de laboratórios, Norma de Uso do Correio Eletrônico Central entre outros.
- Público Alvo: Conjunto de usuários para o qual o serviço se destina, por exemplo, alunos de graduação, docentes ou público em geral.
- Recursos computacionais da Instituição: bens pertencentes à Instituição disponíveis aos usuários para execução de funções profissionais, culturais e intelectuais. Inclui-se nesses bens tanto o patrimônio físico, equipamentos,

cabeamento, meios de armazenamento de informação, quanto o patrimônio lógico, programas de computadores e serviços de redes.

- Rede: é um grupo de computadores, equipamentos e dispositivos complementares conectados por meio de recursos de comunicação. A rede pode ter conexões permanentes, como cabos, ou temporárias, como linhas telefônicas ou outros links de comunicação. A rede pode ser uma pequena rede local, formada por alguns poucos computadores, impressoras e outros dispositivos, ou por diversos computadores grandes ou pequeno porte distribuídos por uma grande área geográfica.
- Servidores: equipamentos que disponibilizam serviços na rede, tais como *Web, E-mail*, FTP, *Proxy* e DNS, ou ainda Banco de Dados.
- Serviços: Recursos, normalmente de software, disponibilizado aos usuários da Instituição.
- Usuário: Qualquer pessoa que utiliza os recursos computacionais da Instituição, em qualquer local, meio ou ainda hora do dia. São considerados usuários os alunos de graduação e pós-graduação, docentes, pesquisadores e servidores do IFAM. Em condições especiais, quando solicitado, outras pessoas podem receber credencial provisória, acesso temporário ou por tempo determinado

Glossário

- Administradores dos Sistemas: (Gerencia os recursos de um sistema).
- Administrador de um serviço móvel: a pessoa e equipe que é responsável, em sua unidade IFAM, pela instalação e configuração do roteador de acesso, ao qual está conectada uma base da acesso wireless, pela configuração do equipamento de acesso, pelo estabelecimento e divulgação de políticas de controle de acesso entre os usuários de serviços móveis e pela distribuição física das AP no local de uso.
- AP: Access Point, base de acesso para serviços móveis em redes Ethernet estruturadas.Uma AP estabelece o controle sobre o acesso ao meio físico de rede, podendo ser configurada de acordo com algumas regras, cuja flexibilidade implicará maior ou menor segurança ao demais usuários de rede local.
- Ativos de rede: Os ativos de rede são os equipamentos básicos que fazem sua rede funcionar. São os *switches*, roteadores, *access points*, dentre outros.
- Autenticação eletrônica: Ato de comprovar a identidade de um usuário por método eletrônico.

- Backbone: é a espinha dorsal da rede IFAM, ou seja, a rede de fibra óptica, em geral subterrânea, interligando equipamentos ativos adequados que permitem a disponibilização dos serviços de transmissão de dados, voz e imagem.
- Bounce attacks: tipo de ataque proveniente de *hackers*, de servidores distintos.
- Bug: erro na codificação ou na lógica que faz com que um programa não funcione corretamente ou que produza resultados incorretos.
- CACIC: O CACIC é um software de inventário de Hardware e Software. Ele faz coleta destes dados nos computadores. **CACIC** – **C**onfigurador **A**utomático e **C**oletor de **I**nformações **C**omputacionais. Então, com o CACIC, é possível ter uma gerência de todo o hardware e software da sua empresa.
- Centelhadores: um elemento de proteção de alta capacidade de corrente e baixa velocidade de condução, apresentando duas tensões de disparo, a nominal (100V/s) àquela especificada no componente e a de regime de impulso (1kV/µs), que pode variar entre 350V e 1,2kV dependendo do fabricante e da tensão nominal.
- Computadores de Uso Pessoal: São computadores pertencentes aos usuários, ou seja, que não pertencem ao patrimônio da Instituição e que podem utilizar os serviços da Rede IFAM.
- Contas funcionais: É aquela fornecida pela Instituição destinada para uso nos serviços internos da Rede IFAM.
- Contas pessoais: É aquela criada pelo usuário para serviços fornecidos fora da Rede IFAM.
- Cookies: É um grupo de dados trocados entre o navegador e o servidor de páginas, colocado num arquivo (ficheiro) de texto criado no computador do utilizador. A sua função principal é a de manter a persistência de sessões HTTP.
- Correio eletrônico: É um método que permite compor, enviar e receber mensagens através de sistemas de comunicação utilizando a Internet.
- Crack: Programa cuja a finalidade é descobrir senhas vulneráveis.
- Cracker: Uma pessoa que burla as medidas de segurança de um sistema de computador e obtém acesso não autorizado. O objetivo de alguns *crackers* é obter informações ilegalmente de um sistema de computador ou utilizar recursos do computador. No entanto, o objetivo da maioria deles é simplesmente invadir o sistema.
- Data Center: é o local onde são concentrados os equipamentos de processamento e armazenamento de dados de uma empresa ou organização.

- DNS: (*Domain Name System*) Na Internet, o sistema através do qual hosts têm endereços de nome de domínio (como IFAM) e endereços IP (como 192.17.3.4). O endereço de nome de domínio é utilizado pelos usuários e é automaticamente traduzido no endereço IP, que é utilizado pelo software de roteamento de pacotes.
- Domínios: É um nome que serve para localizar e identificar conjuntos de computadores na Internet. O nome de domínio foi concebido com o objetivo de facilitar a memorização dos endereços de computadores na Internet. Sem ele, teríamos que memorizar uma sequência grande de números.
- *E-mail*: A troca de mensagens eletrônicas entre computadores através de uma rede de comunicação, como uma rede local ou a Internet.
- Fail over: É a capacidade de alternar automaticamente para um computador servidor redundante, sistema ou rede devido a uma falha ou término anormal do serviço anteriormente ativo.
- Fakemail: e-mail falsificado.
- Fakenews: lista com falsas notícias.
- Firewall: Um sistema de segurança cujo objetivo é proteger a rede de uma organização contra ameaça externas, como hackers, vindas de outras redes, como a Internet. Um *firewall* impede que os computadores da rede da organização se
- Flame wars: É o ato de publicar mensagens deliberadamente ofensivas e/ou com a intenção de provocar reações hostis dentro do contexto de uma discussão na Internet.
- Freeware: Um programa de computador cedido gratuitamente e amplamente distribuído pela Internet. Um programador autônomo pode oferecer programas.
- FTP - (*File Transfer Protocol*) é o protocolo usado para a cópia de arquivos entre sistemas de computador remotos em uma rede que utiliza TCP/IP, como a Internet.
- Grupos : Um conjunto de usuários que compartilham o uso de um determinado conjunto de serviços. Grupo de pessoas ou entidades que utilizam o serviço de um sistema de processamento de dados.
- Hacker: Pessoa que usa seus profundos conhecimentos de informática para fins ilícitos, como, por exemplo, acessar sistemas sem permissão e violar programas e dados.
- Host: Computador principal de um sistema de computadores ou terminais conectado por enlaces de comunicação.

- Hub: Em uma rede, um dispositivo que une linhas de comunicação em um local central, fornecendo uma conexão comum a todos os dispositivos da rede. O termo é uma analogia ao eixo (hub) de uma roda.
- ID: Nome do usuário no sistema remoto.
- Incidente de segurança: Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores.
- IP móvel: refere-se a um host que, ao mudar de rede, mantém a mesma capacidade de comunicação que na rede original, sem que para isso seja necessário especificar outro IP para a rede em trânsito, ou seja, ao migrar, o host mantém o mesmo número IP da rede original e não é necessária nenhuma configuração adicional no mesmo.
- Kerberos: Protocolo de autenticação de rede desenvolvido pelo MIT (Massachusetts Institute of Technology) . O *Kerberos* autentica a identidade dos usuários que tentam efetuar login em uma rede e criptografa suas comunicações através da criptografia de chave secreta.
- LDAP: É um protocolo para atualizar e pesquisar diretórios rodando sobre TCP/IP. Um diretório LDAP geralmente segue o modelo X.500, que é uma árvore de nós, cada um consistindo de um conjunto de atributos com seus respectivos valores.
- Listas de discussão: também denominada grupo de discussão é uma ferramenta gerenciável pela Internet que permite a um grupo de pessoas a troca de mensagens via e-mail entre todos os membros do grupo.
- Login: Processo de identificação do usuário para o computador, depois que entra em contato com ele através de uma linha de comunicação.
- Logon: Entrada em comunicação, início de comunicação. Procedimento pelo qual um usuário inicia uma sessão de comunicação de terminal.
- Malwares: Malicious Software malicioso. Corresponde a programas criados com a intenção de invadir sistemas, ou causar algum tipo de dano. Exemplos são *trojans*, vírus, backdoors, etc.
- MH: Mobile Host, refere-se ao dispositivo móvel que tem acesso aos recursos de rede (um lap/top ou um PDA, entre outros p.ex.), ou através de uma interface sem fio padrão IEEE 802.11 (rede Ethernet sem fio), ou através de interface de rede convencional cabeada, quando em rede estrageira. Em nosso escopo de entendimento, uma rede estrangeira é aquela cujo domínio de administração é diferente daquele de quem administra o dispositivo móvel;

- NAT: Acrônimo de *network address translation*. Processo usado para realizar a conversão entre endereços IP usados em uma intranet ou outra rede privativa (chamada de *stub domain*, ou domínio *stub*) e endereços IP da Internet. Esse método possibilita o uso de um grande número de endereços no domínio *stub* sem esgotar o número limitado de endereços IP numéricos da Internet disponíveis.
- Npasswd: Programa Unix para proporcionar senhas mais seguras.
- Pastas públicas: Pastas criadas dentro do Domínio IFAM para setores ou servidores.
- Patch: Arquivo ou programa para atualização de um sistema.
- Processos de informática: Uma sequência semântica de operações realizadas com a finalidade de produzir um resultado específico.
- Proxy: Componente de firewall que gerencia o tráfego da Internet de/para uma rede local e pode oferecer outros recursos, como o cache de documentos e o controle de acesso. Um servidor *proxy* pode melhorar o desempenho ao fornecer os dados solicitados com freqüência, como uma página conhecida da Web, e pode filtrar e descartar solicitações que o proprietário não considere apropriadas, como solicitações de acesso não autorizado a arquivos patenteados.
- Public Key Cryptography: Esquema assimétrico que utiliza um par de chaves para a criptografia: a chave pública criptografa os dados, e uma chave secreta correspondente os decriptografa. Para assinaturas digitais, o processo é invertido: o emissor utiliza a chave secreta para criar um número eletrônico exclusivo, que pode ser lido por qualquer pessoa que possua a chave pública correspondente, que verifica se a mensagem foi enviada realmente pelo emissor.
- Rede Acadêmica: É aquela destinada a disponibilizar serviços para a Área Acadêmica. Fazem parte dessa rede as Salas dos Professores, salas de aula, bibliotecas e laboratórios computacionais.
- Rede Computacional Administrativa: É aquela destinada a disponibilizar serviços de apoio às atividades da Instituição. Fazem parte dessa rede todos os setores Administrativos do Instituto.
- Rede de Pesquisa: É aquela destinada a disponibilizar serviços para fins de pesquisa Cientifica. Fazem parte dessa rede, os laboratórios e salas de estudo da Pós-Graduação.
- Rede de Serviços: É aquela destinada a disponibilizar serviços de comunicação, acesso e vigilância.

- Rede Pública: É aquela destinada a disponibilizar serviços para fins de acesso Público. Fazem parte dessa os Telecentros, Terminais Públicos e Access Points.
- Redes Móveis: São redes sem fio que proporcionam a existência hospedeiros que podem ou não serem móveis e enlaces sem fio, estação-base e a infra-estrutura da rede.
- Roteador: Dispositivo intermediário que acelera a remessa das mensagens em uma rede de comunicação. Em uma rede que interligue vários computadores através de uma malha complexa de conexões, o roteador recebe as mensagens transmitidas e as encaminha para os destinatários corretos selecionando a rota mais eficiente disponível no momento. Em uma série de redes locais interconectadas, usando os mesmos protocolos de comunicação, o roteador tem uma função diferente, servindo como link entre as redes e permitindo o envio de mensagens entre elas.
- Senhas: Uma única série de caracteres que um programa, um operador ou usuário de computador deverá fornecer para atender aos requisitos em matéria de segurança e como medida prévia para acessar dados. Conjunto de caracteres criptografados que dão acesso ou não a uma determinada área do sistema.
- Sistemas de Informação Corporativos: É a expressão utilizada para descrever sistemas que abrange pessoas, máquinas, e métodos organizados para coletar, processar, transmitir e disseminar dados que representam informação para o usuário.
- Sistemas WWW: sistemas, programas e servidores que se utilizam do protocolo HTTP e variantes (por exemplo, HTTPS) para funcionar.
- Shareware: Programa protegido por direitos autorais, distribuído em caráter experimental gratuitamente.
- Shell: Um componente de software - geralmente um programa em separado - que faz a comunicação direta entre o usuário e o sistema operacional através de uma interface de comandos.
- Sistemas de criptografia: A transformação de dado ou informação, para encobrir ou dissimular o seu significado.
- SOA: O registro SOA (*Start of Authority*) contém informações importantes que regulam a forma como o servidor DNS interage com seus clientes e com servidores secundários.
- Spam: Envio de e-mails em grande quantidade sem a prévia autorização do destinatário.

- SSH: *Secure Shell* - realiza um serviço similar ao TELNET, porém de maneira criptografada, permitindo que o usuário ou administrador estabeleça acesso a computadores remotos para realizar tarefas de maneira seguras.
- Switch: Na comunicação, um computador ou dispositivo eletromecânico que controla o roteamento e a operação de um sinal de percurso.
- TCP: (Transmission Control Protocol) O protocolo dentro do TCP/IP (*Transmission* Control Protocol/Internet Protocol) que controla a subdivisão das mensagens de dados em pacotes a serem enviados através do protocolo IP, e a remontagem e verificação das mensagens completas dos pacotes recebidos pelo IP.
- TCP_WRAPPERS: Programa Unix utilizado para controlar os acessos ao protocolo TCP.
- Telnet: é um protocolo que permite a um usuário abrir uma sessão em um computador que disponibiliza o serviço. Para efetuar login o usuário (cliente) utilizará de um programa TELNET (cliente) informando o endereço IP do servidor do serviço , o login e a senha do usuário, o servidor irá conferir os dados e disponibilizará uma sessão para que o usuário execute determinada tarefa.
- Terminais de Pesquisa: São aqueles disponibilizados ao público da Biblioteca.
- Terminais públicos: São aqueles disponibilizados para o público em geral.
- Trojans: Cavalo de Tróia. Um programa malicioso, enviado como se fosse um jogo, ou outro arquivo qualquer que possa levar o usuário a executá-lo. Uma vez instalado, o trojan abre uma ou várias portas do micro para que quem o enviou possa ter acesso. A maioria permite ao "visitante" ter pleno controle sobre o PC, deletar ou criar arquivos, modificar configurações, instalar programas, ou até mesmo fazer coisas como mover o mouse ou abrir a bandeja do CD-ROM remotamente.
- Usuários: Aquele que utiliza um serviço de computação ou de telecomunicações. Qualquer pessoa ou entidade que utiliza os serviços de um sistema de processamento de dados.
- Varistores: Os varistores são componentes usados em filtros de linhas e em outros aparelhos que oferecem proteção contra descargas elétricas de curta duração.
- Vínculo com a Instituição: É qualquer pessoa ou entidade que presta serviços para a Instituição.
- Vírus: Programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo copias de si mesmo e se tornando parte de outros o programas e arquivos de um computador. O vírus depende da

execução do programa ¸ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

- WEP: Wireless Equivalent Privacy, refere-se à mecanismo de confidencialidade disponível pelo mecanismos definidos no padrão IEEE 802.11, que se estiver configurado, deveria fornecer privacidade equivalente ao de uma rede cabeada.
- Worms: Programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o worm não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitatamente executado para se propagar. Sua propagação se da através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores.
- WWW: ou Web ou W3 sátios Um conjunto totalmente interligado de documentos em hipertexto que residem em servidores. Os documentos da World Wide Web, denominados páginas da Web, são escritos em HTML (Hypertext Markup Language), são identificados por URLs (*Uniform Resource Locators*) que especificam uma determinada máquina e o nome de caminho pelo qual um arquivo é acessado, e são transmitidos de nó em nó até o usuário final através do protocolo HTTP (Hypertext Transfer Protocol).

ANEXO II

TABELA PARA O CRITÉRIO DE PONTUAÇÃO

A tabela abaixo orienta a pontuação com relação à criticidade (Ver Título IX, Capítulo II Pontuação dos ativos da rede IFAM e criticidade de serviços)

ATIVO					
Valor	**Gravidade**	**Urgência**	**Tendência**	**Abrangência**	**Total**
5	Os prejuízos ou dificuldades são extremamente graves	. Urgentíssima	Se nada for feito a situação irá piorar rapidamente	O ativo tem impacto sobre toda a Rede IFAM	625
4	Muito graves	Urgente	Vai piorar em pouco tempo	O impacto incide sobre todo o Campus	256
3	Graves	Tão cedo quanto possível	Vai piorar a médio prazo	Atinge parte do Campus	81
2	Pouco graves	Pode esperar um pouco	Vai piorar a longo prazo	Restringe-se a uma Unidade/Depto	16
1	Sem gravidade	Não tem pressa	Não vai piorar e pode até esperar	Rede Local	1

ANEXO III

FORMULÁRIO PARA ESTABELECER CRITICIDADE DOS ATIVOS

Este documento contém o Formulário padrão para estabelecer a criticidade dos ativos relativa aos serviços que cada um oferece e fornecer um padrão de formulário para que os ativos possam ser pontuados com relação a sua criticidade sobre a Rede IFAM ou rede local (Ver Título IX, Capítulo II - Pontuação dos ativos da rede IFAM e criticidade de serviços).

.

FORMULÁRIO PARA PONTUAÇÃO DOS ATIVOS QUANTO A CRITICIDADE									
Avaliador / Equipe :									
Ativo						**TOTAL**	**Responsável**		
IDENTIFICAÇÃO	**DESCRIÇÃO DO ATIVO**	**G**	**U**	**T**	**A**	**PONTOS**	**Nome**	**Nro. Funcional**	**E-mail**

João Luiz Cavalcante Ferreira
Presidente da Comissão
Portaria nº 136 GR-IFAM de 25/03/2010

_____

André Felipe Aloise
Membro
Portaria nº 136 GR-IFAM de 25/03/2010

_____

Carlos Tiago Garantizado
Membro
Portaria nº 136 GR-IFAM de 25/03/2010

_____

Ronaldo Alves Borges
Membro
Portaria nº 136 GR-IFAM de 25/03/2010

_____

Márcio Antônio dos Santos Souza
Membro
Portaria nº 136 GR-IFAM de 25/03/2010

_____

Francisco Souza da Costa
Membro
Portaria nº 136 GR-IFAM de 25/03/2010

_____

Ricardo Brandão Sampaio
Membro
Portaria nº 136 GR-IFAM de 25/03/2010