Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Tocantins
Reitoria
GABINETE DO REITOR

UTILIZAÇÃO DE EQUIPAMENTOS E SOFTWARES

Institui normativa para utilização e acesso a equipamentos e *softwares* no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Tocantins (IFTO).

O REITOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO TOCANTINS, nomeado pelo Decreto Presidencial de 3 de abril de 2018, publicado no Diário Oficial da União de 4 de abril de 2018, seção 2, no uso de suas atribuições legais e regimentais, e com base no inciso IX do art. 61, art. 76-A e § 4º do art. 98 da Lei nº 8.112, de 11 de dezembro de 1990, no Decreto nº 6.114, de 15 de maio de 2007, e na Portaria MEC nº 1.084, de 2 de setembro de 2008, publicada no DOU de 3 de setembro de 2008, resolve expedir a seguinte normativa sobre a utilização e acesso aos equipamentos e *softwares*:

CAPÍTULO I

DO OBJETIVO

Art. 1º Esta normativa tem por objetivo definir as regras para a utilização de equipamentos e *softwares*, no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Tocantins (IFTO), estabelecendo as diretrizes básicas a serem seguidas pelos usuários de forma assegurar a correta utilização dos recursos computacionais, visando à conservação, controle, padronização, segurança da informação e respeito aos direitos autorais.

CAPITULO II

DAS DEFINIÇÕES

Art. 2º Para fins de compreensão desta normativa, serão adotadas as seguintes definições:

I - **administrador de rede:** pessoa designada formalmente pela instituição com atribuição principal de gerenciar a rede de comunicação de dados local, bem como os recursos computacionais a ela conectados, direta ou indiretamente;

II - **computador:** equipamento dedicado às atividades laborais, inclusive aqueles alocados em laboratórios, salas de treinamento, salas de reunião ou portáteis, utilizado pelo usuário para acesso à serviços de rede e compartilhamento de dados;

III - **conta de rede:** identificação pessoal do usuário (conta de acesso a rede) que permite

acesso à rede local, recursos, serviços e sistemas informatizados disponibilizados pela instituição;

IV - **controle de acesso:** processo que determina o acesso ou não de um indivíduo às áreas ou objetos específicos, identificando e registrando esses acessos;

V - **equipamentos de rede:** meios físicos necessários para a comunicação entre os componentes de uma rede de dados. São exemplos típicos de dispositivos de rede: *switch*, roteadores, concentradores, repetidores, adaptadores de rede, modem, *gateway, bridge*, *firewall*, ponto de acesso sem fio e outros *hardwares* relacionados;

VI - **equipamentos portáteis:** equipamentos de pequeno porte que possuem sistema operacional e executam aplicativos, conectáveis à rede de dados através de dispositivos de rede sem fio (*smartphone, notebook, tablets*);

VII - **equipe de TI:** analistas, técnicos de TI e técnicos de laboratório lotados no setor de TI;

VIII - **ilha de impressão:** composição de um ou mais setores que compartilham o mesmo recurso de impressão;

IV - **login:** processo pelo qual o acesso a um sistema informatizado é controlado através da identificação e autenticação do usuário, por meio de credenciais fornecidas pela instituição. Essas credenciais são normalmente constituídas por um nome de utilizador (conta de acesso a rede) e uma senha;

V - **recurso de impressão:** conjunto de equipamentos e/ou serviços que possibilitam a impressão de documentos;

VI - **recursos computacionais:** equipamentos, instalações e recursos de informação direta ou indiretamente administrados, mantidos ou operados pelos setores de TI (gestão, ensino, pesquisa e extensão), tais como: computadores de mesa (*desktops*), servidores de rede, equipamentos portáteis, impressoras, equipamentos de redes de dados, telecomunicações, dispositivos periféricos, equipamentos que compõem o Datacenter, ferramentas eletrônicas de comunicação de dados, softwares adquiridos ou desenvolvidos, dados armazenados em computadores, dispositivos periféricos e outros equipamentos, bem como em CDs, DVDs e outras mídias, dispostos ou não em banco de dados, tais como arquivos e certificados digitais, sistemas de segurança e sistemas operacionais;

VII - **rede corporativa:** infraestrutura física e lógica que possibilita a transmissão de informação através da troca de dados;

VIII - **servidor de arquivos:** computador conectado a rede de dados que provê serviço de compartilhamento de arquivos digitais (documentos, áudios, imagens, vídeos) para outros servidores, computadores e equipamentos de rede;

IX - **servidor de impressão:** servidor destinado a gerenciar impressões enviadas para uma impressora em rede por diferentes computadores e dispositivos portáteis;

IX - **servidor de rede:** computador dedicado que provê um ou mais serviços de rede para outros servidores, computadores e equipamentos de rede;

X - **técnico de TI:** servidor lotado no setor de TI responsável pelo suporte e manutenção dos recursos computacionais;

XI - **usuário:** qualquer pessoa, física ou jurídica, com vínculo formal direto ou indireto com a instituição, ou em condição autorizada, que faça uso de algum recurso computacional.

CAPÍTULO III
DAS DIRETRIZES GERAIS

Art. 3º Para a disponibilização de recursos computacionais foram definidas as seguintes diretrizes básicas:

I - os recursos computacionais deverão ser utilizados de maneira responsável, consistente com os objetivos das áreas de gestão, ensino, pesquisa e extensão;

II - cada usuário, no uso de recursos computacionais que necessite de credenciais de acesso, deverá obrigatoriamente ter uma identificação única na rede de comunicação de dados, visando resguardar a segurança da informação;

III - para cada usuário será criado uma conta individual de acesso (conta de acesso a rede) como um dos mecanismos de controle de acesso e monitoramento no uso dos recursos computacionais, não sendo permitido o compartilhamento com outros usuários, uma vez que são credenciais de acesso confidenciais e intransferíveis;

IV - a equipe de TI irá realizar a gestão (especificação, instalação, administração e manutenção) dos recursos computacionais, em conformidade com as exigências regulatórias e orientações governamentais;

V - o IFTO adotará regulamentações federais, estaduais e municipais quanto ao uso da Internet, para identificar e estabelecer mecanismos técnicos e procedimentos que garantam a funcionalidade, segurança e robustez de seu ambiente computacional;

VI - a utilização dos recursos de TI com finalidade pessoal é permitida, desde que não viole as normas institucionais de segurança da informação previstas pelo IFTO;

VII - os equipamentos pessoais conectados à rede de dados institucional estão sujeitos às mesmas políticas, diretrizes e regulamentações previstas nesta normativa;

VIII - os equipamentos institucionais deverão manter preservados, de modo seguro, os registros de eventos com identificação de login, data e horário de acesso de forma a resguardar a segurança da informação;

IX - o IFTO se reserva o direito de realizar investigação forense digital em quaisquer dos recursos computacionais que integram sua rede de comunicação de dados, sem prévio aviso, sempre que necessário para garantir a segurança da informação;

X - a equipe de TI poderá remover, a qualquer momento e sem aviso prévio, aplicativos instalados nos equipamentos institucionais conectados à sua rede de comunicação de dados que não se enquadre aos critérios estabelecidos neste documento;

XI - sempre que necessário, para preservação da integridade dos recursos computacionais, técnicos da equipe de TI poderão, mediante fundamentação formal, suspender temporariamente qualquer acesso à site, serviços e sistemas informatizados durante análises de incidentes de segurança;

XII - instituições e pessoas sem vínculo formal ao IFTO poderão utilizar os recursos computacionais, desde que respeitadas as orientações e diretrizes de uso estabelecidas neste documento;

XIII - equipamentos que integram o patrimônio do IFTO poderão ser utilizados, excepcionalmente, fora de suas instalações, desde que haja disponibilidade, seja apresentado justificativa plausível e sua saída seja documentada pelo setor de patrimônio da unidade;

XIV - o usuário não deve armazenar informações pessoais em equipamentos do IFTO. Arquivos não pertinentes às atividades da Instituição (fotos, músicas, vídeos, etc.) poderão ser excluídos sem comunicação prévia;

XV - atualizações de segurança nos equipamentos institucionais ocorrerão de forma automática através de procedimentos realizados pela equipe de TI. O usuário não deverá

intervir no processo de atualização. Caso o usuário identifique a necessidade de alguma atualização ainda não realizada, deverá comunicar ao responsável pelo setor de TI;

XVI - solicitações de instalação e/ou configuração de recursos computacionais deverão ser feitas através da central de serviços disponibilizada no SUAP.

CAPÍTULO IV
DOS EQUIPAMENTOS

Art. 4º As diretrizes básicas a serem consideradas para o uso seguro dos equipamentos são:

I - os computadores disponibilizados aos usuários terão configurações de hardware e software, definidas pelo equipe de TI, compatíveis com a natureza da utilização;

II - os computadores devem ser acessados através de identificador pessoal único e intransferível conta de acesso a rede IFTO);

III - as atividades de manutenção e suporte no uso dos computadores serão realizadas e/ou coordenadas pelo equipe de TI;

IV - manutenção nos computadores, solicitadas pelo usuário, serão agendadas e realizadas após abertura de chamado na central de serviços disponibilizada no SUAP;

V - somente técnicos autorizados pelo equipe de TI devem realizar manutenções preventivas e corretivas em computadores e periféricos pertencentes ao IFTO;

VI - alterações na configuração padrão do ambiente operacional dos computadores, realizadas pelo usuário, devem ser notificadas, justificadas e autorizadas pela equipe de TI;

VII - arquivos digitais salvos nas unidades de armazenamento de dados dos computadores não têm garantia de recuperação nos casos de falha, manutenção e formatação. A equipe de TI não é responsável pelo *backup* de arquivos pessoais do usuário ou arquivos armazenados em locais não indicados pelo setor;

VIII - o compartilhamento de pastas e arquivos digitais, armazenados em estações de trabalho, somente deve ser configurado quando justificado e for imprescindível para a execução das atividades do setor, e deve ser informado formalmente à equipe de TI;

IX - o usuário deve informar à equipe de TI qualquer identificação de dispositivo estranho conectado à sua estação de trabalho;

X - é dever do usuário zelar pela conservação e bom funcionamento de sua estação de trabalho, seguindo as boas práticas estabelecidas para o uso seguro de recursos computacionais.

CAPÍTULO V
DOS EQUIPAMENTOS PORTÁTEIS INSTITUCIONAIS

Art. 5º As diretrizes básicas a serem consideradas para o uso seguro de equipamentos portáteis fornecidos pelo IFTO são:

I - equipamentos portáteis devem ser guardados em local seguro, com controle de acesso e garantia quanto à sua integridade;

II - o usuário ao solicitar o empréstimo de equipamentos portáteis, deve assinar o Termo de Empréstimo de Equipamento no setor de patrimônio;

III - o usuário deverá realizar periodicamente, cópia de segurança (*backup*) dos dados

gravados no dispositivo móvel e guardá-los em ambiente diferente, ou seja, não carregá-los / armazená-los juntos num mesmo lugar;

IV - os equipamentos portáteis devem respeitar as mesmas regras estabelecidas para os computadores.

CAPÍTULO VI
DOS SERVIDORES DE REDE

Art. 6º As diretrizes básicas a serem consideradas para a disponibilização de servidores de rede nas unidades do IFTO, são:

I - todo equipamento com função de servidor deverá ser instalado em salas seguras e apropriadas, destinadas especificamente para uso da equipe de TI;

II - servidores de rede serão disponibilizados de acordo com a capacidade da infraestrutura tecnológica de cada unidade;

III - quando disponibilizados servidores de arquivos em rede, deverão ser armazenados somente documentos relacionados ao trabalho cotidiano e à produção acadêmica, científica e administrativa local, que demande compartilhamento ou resguardo institucional;

IV - arquivos que não refletem atividades relacionadas à demandas institucionais poderão ser apagados sem prévio aviso;

V - as permissões de acesso deverão ser solicitadas através de abertura de chamado na central de serviços disponibilizada no SUAP e serão concedidas a nível de grupos de usuários de acordo com a necessidade do setor.

CAPÍTULO VII
DOS ATIVOS DE REDE

Art. 7º As diretrizes básicas a serem consideradas para a disponibilização de ativos de rede são:

I - o ativo de rede deve possibilitar a configuração de controle de acesso com no mínimo as seguintes informações: login, data e horário;

II - o ativo de rede deve ser instalado em local reservado e com acesso controlado pelos técnicos da equipe de TI e quando possível devem ser instalados em *racks* devidamente fechados e seguros;

III - os ativos de rede devem ser instalados no ambiente de produção somente após sua adequação em relação aos padrões de segurança da informação estabelecidos pelo IFTO;

IV - as intervenções no ambiente que tenham instalados ativos de rede devem ser realizadas com supervisão dos técnicos autorizados pelo setor de TI, de forma a evitar indisponibilidade de recursos, serviços e sistemas informatizados.

CAPÍTULO VIII
DO USO DE SOFTWARES

Art. 8º As diretrizes básicas para uso adequado de softwares no âmbito do IFTO são:

I - a equipe de TI deverá manter atualizado o registro de *softwares* homologados e utilizados em equipamentos institucionais;

II - o usuário será responsabilizado por quaisquer programas e/ou aplicativos que tenham sido instalados, utilizando sua conta de acesso a rede IFTO;

III - a transferência e/ou a divulgação de qualquer *software*, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida autorização da equipe de TI, de acordo com o nível de classificação da informação, após identificação e justificativa do solicitante;

IV - as solicitações para aquisição de novas licenças de uso de software devem ser encaminhadas para a equipe de TI, devidamente justificadas. A instalação e a utilização de software estão sujeitas ao cumprimento dos seguintes requisitos:

a) Quantidades de licenças de uso adquiridas;

b) Conformidade com a área de atuação do setor interessado;

c) Compatibilidade com os sistemas operacionais e softwares utilizados pelo IFTO;

d) Desempenho do ambiente computacional;

e) Impacto entre a necessidade de instalação e a demanda de outros setores.

V - a instalação de *software freeware* (gratuito), de domínio público (não protegido por *copyright*) e/ou cópias de demonstração que não sofram ação de direitos autorais, deve ser previamente informada à equipe de TI.

CAPÍTULO IX
DO USO DE IMPRESSORAS

Art. 9º As diretrizes básicas a serem consideradas para o uso apropriado de impressoras nas Unidades do IFTO, são:

I - equipamentos de impressão instalados são para uso exclusivo relacionados a atividades de gestão, ensino, pesquisa e extensão. É vedado o uso dos recursos de impressão para fins particulares;

II - somente os usuários previamente autorizados poderão ter acesso aos recursos de impressão;

III - o usuário não deve deixar informações críticas, sigilosas ou sensíveis em equipamentos de impressão, de tal forma que pessoas não autorizadas possam obter acesso a elas;

IV - a impressão de documentos deve ser reduzida ao mínimo necessário, utilizando-se os meios disponíveis para a sua racionalização. Para isso, devem ser adotadas regras de cota de impressão de acordo com a realidade de cada setor;

V - as unidades deverão definir estratégias para a centralização de impressão de documentos através de ilhas e servidor de impressão;

VI - quando for constatado uso mínimo do equipamento de impressão em determinado setor, o mesmo poderá ser remanejado para outro de forma a uniformizar a distribuição, visando o uso racional de recursos públicos;

VII - todo o suporte e manutenção de impressora deve ser registrado através da central de serviços disponibilizada no SUAP;

VIII - para evitar desperdício de recursos públicos, as impressoras sempre que possível, deverão ser configuradas no modo de impressão frente e verso (duplex).

CAPÍTULO X
DO SUPORTE E MANUTENÇÃO DE RECURSOS COMPUTACIONAIS

Art. 10º As diretrizes básicas a serem consideradas para o suporte e a manutenção dos recursos computacionais nas unidades, são:

I - toda solicitação de atendimento para instalação, manutenção, suporte e configuração dos recursos computacionais deve ser efetuada mediante abertura de chamado na central de serviços disponível no SUAP;

II - a execução dos serviços de assistência técnica deve ser realizada apenas em equipamentos de propriedade do IFTO;

III - a manutenção técnica deve preferencialmente ser realizada no local de instalação do equipamento. Quando a manutenção for feita, é importante que o usuário esteja presente, pelo menos no início do suporte, para orientar o técnico sobre o problema ou defeito apresentado no recurso computacional;

IV - o usuário deve ser avisado da saída do equipamento de seu local de trabalho, caso seja necessária a retirada do mesmo para manutenção, seja preventiva ou corretiva.

CAPÍTULO XI
DA DISPONIBILIZAÇÃO DE RECURSOS COMPUTACIONAIS PARA PROJETOS DE ENSINO, PESQUISA E EXTENSÃO

Art. 11º Serão disponibilizados para ensino, pesquisa e extensão recursos computacionais de TI, desde que o IFTO tenha condições técnicas (processamento, armazenamento e memória). Para isso, o requisitante deverá registrar sua solicitação formalmente através de abertura de chamado na central de serviços (SUAP). Para a disponibilização de recursos computacionais serão observadas as seguintes regras:

I - ficará a cargo do responsável pelo projeto o *backup* dos dados hospedados nos servidores disponibilizados pelo setor de TI;

II - caso o responsável pelo projeto precise disponibilizar acesso externo de seu projeto, o mesmo será responsável por manter a segurança da informação referente a seu projeto;

III - a equipe de TI poderá monitorar as vulnerabilidades e sugerir correções/atualizações de segurança em equipamentos utilizados em projetos de ensino, pesquisa e extensão;

IV - a equipe de TI poderá bloquear a comunicação entre o recurso computacional e a Internet, caso sejam detectados incidentes que comprometam a segurança da informação e a imagem do IFTO.

CAPÍTULO XII
DA REDE DE COMUNICAÇÃO DE DADOS

Art. 12º A equipe de TI é responsável pela gestão da rede de comunicação de dados e pela segurança da informação local.

§ 1º o acesso à rede de comunicação de dados por parte dos usuários será realizado por meio de credenciais de acesso (conta de acesso a rede).

SEÇÃO I - Da distribuição de blocos de endereços IP disponibilizados pela RNP

Art. 13º A Diretoria de TI é responsável por cuidar do controle e distribuição dos blocos de endereços IP alocados ao IFTO pela Rede Nacional de Pesquisa (RNP).

Art. 14º As unidades do IFTO deverão seguir o padrão adotado e não devem alterar a máscara de suas sub-redes, assumindo para si a responsabilidade de tratar o roteamento de forma adequada conforme definição do grupo de trabalho de infraestrutura de TI.

SEÇÃO II - Da distribuição dos blocos de endereços IP especialmente reservados (RFC 1918) para a construção de redes internas

Art. 15º A Diretoria TI é responsável por cuidar do controle e da distribuição dos blocos de endereços especialmente reservados para a construção de redes internas nas unidades do IFTO. A distribuição de blocos de endereços IP levará em consideração as seguintes regras:

I - a distribuição de endereçamento IP está normatizada de forma a garantir unicidade de blocos de endereço por unidade;

II - o grupo de trabalho de Infraestrutura de TI definiu blocos de endereços reservados para as sub-redes das unidades;

III - cada unidade cuidará da configuração de seus *firewalls, gateways* e outros equipamentos de acordo com o padrão normatizado pelo grupo de trabalho de Infraestrutura de TI.

SEÇÃO III - Dos servidores de domínio

Art. 16º A Diretoria de TI é responsável por gerenciar as atribuições de *nameservers*. A unidade que precisar de apontamentos nos servidores DNS, deverá solicitar formalmente através da central de serviços (SUAP). Em relação aos servidores de domínio serão observados as seguintes regras:

I - a unidade deverá informar à coordenação de redes e segurança da informação (Reitoria) qualquer alteração de nomes em serviços e sistemas informatizados que esteja divergente da configuração atual dos servidores de DNS do IFTO;

II - no caso de criação de um domínio, sua delegação será feita para o servidor DNS principal;

III - os servidores de DNS não permitirão a transferência de seus mapas (“*zone files*”) para outros servidores que não sejam seus servidores secundários;

IV - nomes de domínios podem ser utilizados para mapear um ou mais endereços de rede IP, identificar domínios, sítios, serviços, além de outras aplicações;

V - nomes subordinados ao domínio "ifto.edu.br" deverão ser hospedados em servidores disponibilizados na rede do IFTO;

VI - a atribuição de nomes no domínio "ifto.edu.br" atenderá a seguinte regra:

f) O *namespace* deverá ser relacionado a um projeto, programa, evento ou convênio com o IFTO;

g) O *namespace* deverá estar relacionado a um serviço disponibilizado pela TI da unidade.

SEÇÃO IV - Dos firewalls existentes na rede IFTO

Art. 17º Os *firewalls* deverão ser configurados atendendo as seguintes regras:

I - ser dedicado unicamente ao serviço de roteamento e filtragem de pacotes e não devendo possuir outros serviços configurados além dos necessários para controle de tráfego de rede;

II - não possuir contas destinadas a usuários comuns, devendo conter apenas contas para administradores de rede da unidade;

III - permitir o acesso remoto apenas aos hosts definidos como seguros pelos administradores da rede da unidade;

IV - implementar o filtro de pacotes de acordo com as diretrizes estabelecidas pelo grupo de trabalho de Infraestrutura de TI, levando em conta a política de segurança da informação e suas normas complementares;

V - utilizar sistemas operacionais atualizados, conforme a padronização definida pelo grupo de trabalho de Infraestrutura de TI.

SEÇÃO V - Do filtro de pacotes

Art. 18º Os filtros de pacotes poderão ser aplicados nos *firewalls* das unidades atendendo às seguintes regras:

I - bloqueio de pacotes com o objetivo de que os recursos computacionais das unidades não sejam utilizados como base de ataque por *hackers/crackers*;

II - bloqueio de pacotes que estejam prejudicando o tráfego da rede ou colocando em risco a segurança da rede;

III - bloqueio de serviços que podem causar rompimento de segurança ("*deny of service*") em alguma das máquinas internas da unidade.

SEÇÃO VI - Do tráfego na rede IFTO

Art. 19º A critério da equipe de TI poderão ser aplicadas políticas de priorização de tráfego e limitação da taxa de transferência ou volume de dados, com o intuito de priorizar ou beneficiar as atividades essenciais do IFTO. O tráfego na rede deverá ser gerenciado a partir da seguinte regra:

I - banda consumida por aplicações específicas fica sujeita à limitação, sendo de responsabilidade dos administradores de rede da unidade a definição do percentual de uso da banda disponível.

SEÇÃO VII - Das conexões externas à rede do IFTO

Art. 20º Para garantir a segurança da informação na rede IFTO, as conexões externas para a rede interna somente serão liberadas após justificativa formal por meio de abertura de chamado na central de serviços (SUAP) e deverão estar relacionadas à gestão administrativa, projetos de ensino, pesquisa e extensão.

SEÇÃO VIII - Do acesso a Internet

Art. 21º O acesso à internet, deverá ser realizado exclusivamente através de sistema de segurança da informação configurado pela equipe de TI. Para acesso a Internet são definidas as seguintes regras:

I - a internet deverá ser utilizada nas dependências do IFTO de forma a atender as atividades desenvolvidas pela área de gestão, ensino, pesquisa e extensão, observando o disposto nesta norma;

II - terão acesso à internet os servidores técnicos administrativos, professores, estudantes, prestadores de serviços, temporários, voluntários, estagiários e pessoas que participam de projetos de pesquisa e extensão;

III - caberá à equipe de TI aplicar as restrições de acesso à internet necessárias por meio de ferramenta de filtro de conteúdo;

IV - a equipe de TI poderá bloquear o acesso a páginas e arquivos que se enquadrem nas atividades inadequadas ao desenvolvimento das atividades institucionais do IFTO;

V - caso ocorra bloqueio de acesso a sites ou páginas em razão da classificação indevida da ferramenta de filtro de conteúdo, caberá à equipe de TI, mediante solicitação formal do interessado através da central de serviços no SUAP, providenciar a adequação e desbloqueio do site.

SEÇÃO IX - Do desempenho do acesso à internet

Art. 22º A equipe de TI não garantirá desempenho de acesso a sites de internet externos, uma vez que este acesso não depende das atividades realizadas localmente pelo setor.

§ 1º A critério da equipe de TI, medidas poderão ser adotadas, visando a manutenção da disponibilidade e desempenho do acesso aos recursos, serviços e sistemas de informação, tais como:

a) bloqueios totais ou parciais de acessos a determinados sites e serviços inadequados, impróprios, prejudiciais ou não necessários ao desenvolvimento das atividades de ensino, pesquisa, extensão e gestão administrativa;

b) priorização de acessos a determinados sites e serviços;

c) limitação de tráfego na rede.

§ 2º Caso o usuário necessite de acesso a algum site que esteja bloqueado, deverá solicitar a liberação através da central de serviços (SUAP). Esta solicitação deverá passar pela análise técnica da equipe de TI e em seguida, será encaminhada para autorização da direção da unidade.

SEÇÃO X - Do monitoramento e auditoria

Art. 23º O IFTO por meio da equipe de TI poderá monitorar e auditar a rede visando garantir a disponibilidade e a segurança das informações, bem como a apuração de um ato administrativo.

§ 1º Os registros de acessos à rede deverão ser arquivados e utilizados, exclusivamente, para

fins de auditoria.

SEÇÃO XI - Do registro de incidentes de segurança da informação

Art. 24º Os incidentes de segurança da informação dentro da rede de comunicação de dados deverão ser relatados à equipe de TI através da central de serviços (SUAP), contendo no mínimo as seguintes informações:

I - identificação do recurso computacional;

II - identificação do usuário(s) envolvido(s);

III - data e horário da identificação do incidente.

SEÇÃO XII - Da rede sem fio

Art. 25º As diretivas básicas de segurança da informação para a rede sem fio são:

I - a utilização da rede sem fio para acesso à rede somente será efetuada por meio de autenticação utilizando mecanismos e protocolos seguros;

II - não é permitido o uso da rede sem fio administrativa por *notebooks* de terceiros e/ou particulares, sem a prévia autorização da equipe de TI e /ou da chefia do setor;

III - todos os *access points*, antenas e componentes de transmissão de uma infraestrutura de rede sem fio nas unidades devem estar registrados junto ao setor de TI;

IV - um equipamento que venha emitir ondas de rádio em nível que provoque interrupções, interferências ou sobrecarga em outros serviços ou sistemas, deverá permanecer desligado até que se consiga eliminar as causas da interferência;

V - em caso de interferência entre redes sem fio, terá prioridade aquela que seja aberta ao maior número de dispositivos de usuários, devendo as demais serem desligadas ou remanejadas;

V - qualquer equipamento que utilize a rede sem fio deve respeitar as regras estabelecidas para computadores e dispositivos portáteis.

CAPÍTULO XIII
DAS RESPONSABILIDADES

Art. 26º As responsabilidades do usuário em relação ao uso seguro dos recursos computacionais são:

I- respeitar todas as políticas, normas, orientações e procedimentos de segurança da informação, incluindo, mas não limitado, às normas e procedimentos de uso dos recursos computacionais;

II - contribuir para a melhoria dos níveis de segurança da informação dos recursos computacionais disponibilizados pelo IFTO;

III - respeitar os direitos de outros usuários, incluindo os direitos garantidos em outras normas do IFTO;

III - não permitir ou colaborar com o acesso indevido aos recursos computacionais do IFTO

por parte de pessoas não autorizadas, sob pena de ser co-responsabilizado pelos eventuais problemas que esses acessos vierem a causar;

IV - utilizar apenas *software* homologado pela equipe de TI;

V - zelar pela conservação dos equipamentos de informática sob sua responsabilidade, não podendo fumar ou alimentar-se próximo a eles;

VI - notificar imediatamente a equipe de TI a ocorrência de eventos que venham a alterar o funcionamento ou que possam causar algum dano aos equipamentos ou sistemas do IFTO;

VII - manter cópias de segurança *(backup*) dos dados armazenados no equipamento que estiver sob sua guarda;

VIII - trocar periodicamente a senha de acesso aos recursos computacionais;

IX - respeitar os direitos de propriedade intelectual, de acordo com a regulamentação pertinente, em particular as leis de proteção da propriedade intelectual do Programa de Computador (Lei N 9.609, de 19 de fevereiro de 1998, Lei de direitos autorais Lei N 9.610, de 19 de fevereiro de 1998;

X - comunicar à equipe de TI qualquer evidência de violação das normas de segurança contidas neste documento, não podendo acobertar, esconder ou ajudar a esconder violações de terceiros, de qualquer natureza;

XI - manter conduta compatível com a legalidade e a moralidade administrativa durante o uso dos recursos computacionais, ficando diretamente responsável pelas consequências decorrentes de práticas que danifiquem ou coloquem em risco a segurança da informação ou de terceiros;

XII - desligar o computador de forma adequada e segura no final de sua jornada de trabalho;

XIII - o usuário que tiver equipamento em sua responsabilidade, no caso de furto ou roubo, deverá notificar imediatamente seu gestor direto, setor de TI e Patrimônio, e deve informar as autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO);

XIV - imprimir apenas documentos relacionados às atividades finalísticas do IFTO.

Art. 27º As responsabilidades dos técnicos de TI em relação ao uso dos recursos computacionais são:

I - verificar periodicamente a conformidade dos equipamentos com os requisitos básicos de segurança da informação;

II - instalar, configurar e atualizar *hardware e softwares*;

III - realizar manutenção preventiva e corretiva de *hardware e software*;

IV - monitorar o tráfego na rede e, se for o caso, vetar o acesso a qualquer usuário que violar as normas de segurança da informação ou ameaçar os direitos de outros usuários;

V - promover a segurança preventiva em todo o escopo físico e lógico da unidade, respeitando as regulamentações em vigor e adequando às implementações de ações relacionadas às melhores práticas de gerenciamento de incidentes e segurança da informação;

VI - manter atualizado o registro de *softwares* instalados nos laboratórios e rede administrativa do IFTO;

VII - gerenciar as licenças de *softwares* utilizadas pelo IFTO, de modo a garantir o cumprimento do disposto na política de segurança da informação e normas complementares;

VIII - realizar vistoria periódica, no local ou por meio informatizado remoto, dos *softwares*

instalados nos equipamentos de informática;

IX - identificar, registrar, notificar e adequar eventuais inconformidades relacionadas à segurança da informação;

X - avaliar a viabilidade técnica das solicitações oriundas dos setores, quanto a incorporação de novas soluções (softwares) ao ambiente computacional existente;

XI - abrir chamado técnico para a prestadora de serviços quando da detecção de problemas físicos e necessidade de manutenções preventivas e corretivas em impressoras.

CAPÍTULO XIV
DAS PROIBIÇÕES/VIOLAÇÕES

Art. 28º Qualquer violação ou suspeita de quebra das regras contidas neste documento deve ser comunicada imediatamente ao responsável direto pelo recurso computacional no local onde o fato tenha ocorrido.

§ 1º As violações desta norma estarão sujeitas a ações específicas e podem resultar em ações disciplinares definidas na legislação brasileira.

§ 2º O IFTO caracteriza como não ético é inaceitável, passível de ação disciplinar as seguintes ações por parte do usuário:

I - abrir equipamentos e modificar qualquer configuração, seja de hardware ou software, sem autorização prévia da equipe de TI;

II - utilizar a exploração de falhas de configuração, falhas de segurança ou tentar obter conhecimento de senhas especiais para alterar a configuração de um recurso computacional;

III - fornecer informações a terceiros sobre características, funcionalidades e configurações dos recursos computacionais disponíveis, ressalvada os casos em que o desempenho de atividades profissionais assim exigir;

IV - instalar softwares não licenciados que possam disponibilizar acessos indevidos a sites bloqueados ou qualquer vantagem de navegação web não permitida pela equipe de TI;

V - instalar software não autorizado pelo equipe de TI mesmo que sejam gratuitos, de domínio público e/ou cópias de demonstração;

VI - efetuar cópias dos softwares licenciados pelo IFTO sem autorização prévia;

VII - utilizar softwares que, por algum motivo, descaracterizem os propósitos da instituição ou danifiquem de alguma forma o ambiente instalado;

VIII - monitorar ou interceptar o tráfego de dados nos sistemas de TI, sem a autorização da equipe de TI;

IX - desabilitar ou alterar configurações de softwares de rede ou relacionados à segurança da informação, tais como, antivírus, firewall, e outros similares;

X - transportar equipamentos para qualquer outra unidade organizacional sem o conhecimento do setor de patrimônio;

XI - ceder, mesmo que temporariamente, o uso dos recursos computacionais a terceiros não pertencentes ao quadro funcional do IFTO;

XII - utilizar as credenciais de acesso de outro usuário para acessar ou utilizar um recurso computacional ou sistema informatizado dentro da rede de comunicação de dados do IFTO;

XIII - efetuar conexão de dispositivos não autorizados pela equipe de TI na rede local, especialmente equipamentos de conexão à rede sem fio ou qualquer outra solução que

estabeleça conexão simultânea com a rede de dados do IFTO e outras redes externas;

XIV - compartilhar o acesso à rede do IFTO com usuários não autorizados, por qualquer meio, inclusive através de compartilhamento por meio físico, ou através da divulgação de nome de usuário e senha;

XV - realizar ações que violem questões de direitos autorais ou proteção de patentes e autorizações do IFTO ou de terceiros, como também licenças de uso e outros contratos;

XVI - invadir a privacidade de indivíduos ou entidades que são autores, criadores, usuários ou responsáveis através do uso de recursos computacionais;

XVII - remover dos recursos computacionais do IFTO algum documento de propriedade do IFTO ou por ela administrado, sem uma autorização específica;

XVIII - passar por outra pessoa ou esconder sua identidade na utilização dos recursos disponibilizados na rede de comunicação de dados do IFTO;

XIX - violar os sistemas de segurança dos recursos computacionais do IFTO, como quebrar ou tentar adivinhar identificação ou senhas de terceiros, interferir em fechaduras automáticas ou sistemas de alarme;

XX - divulgar e/ou compartilhar indevidamente informações da área administrativa do IFTO em listas de discussão, sites ou comunidades de relacionamento, salas de bate papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet;

XXI - interferir nos serviços de qualquer outro usuário, ou seja realizar ataques, tentativas de congestionar a rede interna de comunicação de dados, sobrecarregar ou invadir um servidor de rede ou, ainda, o computador de outro usuário;

XXII - armazenar, transmitir, divulgar ou disponibilizar qualquer conteúdo, dentre outros similares, que contenham vírus ou qualquer outro código, arquivo ou programa de computador com o propósito de interromper, destruir ou limitar a funcionalidade de qualquer software, hardware ou equipamento de telecomunicações;

XXIII - compartilhar qualquer conteúdo ilegal, ofensivo à honra, que invada à privacidade de terceiros, que seja vulgar, obsceno, pornográfico, preconceituoso, racista, neonazista, antissemita ou qualquer outro que venha a atentar contra a integridade moral de terceiros ou grupos da sociedade;

XXIV - remover softwares “padrão” instalados pelo setor de TI nos computadores sem prévio conhecimento do setor de TI;

XXV - remover, interromper ou qualquer outro meio de parar os programas que fazem inventário, produtividade e controle de acesso aos computadores, sendo tratado como tentativa de burlar as ferramentas de segurança da Instituição.

CAPÍTULO XV
DAS PENALIDADES

Art. 29º O usuário será responsabilizado pelos atos que venham a acarretar algum dano em virtude de imprudência, imperícia ou negligência no uso dos recursos computacionais do IFTO.

§ 1º A violação das normas estabelecidas neste documento e outras decorrentes de uso indevido de recursos computacionais são passíveis de punição administrativa, judicial e censura ética, sem prejuízo das sanções penais que o caso concreto exigir.

§ 2º A infração ou tentativa de infração às regras constantes neste documento ou às regras previstas em lei serão apuradas por meio de sindicância administrativa.

§ 3º O descumprimento desta regulamentação poderá acarretar, isolada ou cumulativamente, nos termos da legislação vigente, sanções administrativas, civis e penais, assegurando-se aos envolvidos a ampla defesa.

CAPÍTULO XVI
DAS DISPOSIÇÕES FINAIS

Art. 30º A violação das determinações contidas nesta normativa são passíveis de punição administrativa, judicial e censura ética, sem prejuízo das sanções penais que o caso concreto exigir.

Art. 31º As atualizações necessárias nesta normativa serão analisadas pelo comitê de segurança da informação, validadas pelo comitê gestor de tecnologia da informação.

Art. 32º Casos omissos não tratados nesta normativa serão submetidos ao comitê gestor de tecnologia da informação.

Art. 33º Os casos excepcionais não abordados nesta normativa serão tratados pela equipe de TI juntamente com a direção geral da unidade.

Art. 34º Esta normativa será revisada regularmente pelo comitê de segurança da informação e quando ocorrerem eventos ou fatores relevantes que exijam correções será atualizada e disponibilizada publicamente.

Art. 35º Esta normativa entra em vigor a partir da data de sua publicação.