



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

USO DE RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

Estabelece a norma sobre uso de recursos de Tecnologia da Informação no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Tocantins (IFTO).

CAPÍTULO I DO ESCOPO

Art. 1º Esta norma tem por objetivo definir as diretrizes, competências e responsabilidades para uso de recursos de Tecnologia da Informação e Comunicação no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Tocantins (IFTO) visando a regulamentar, em seus diversos aspectos, respeitando os princípios éticos e profissionais, a utilização dos referidos serviços e recursos de tecnologia da informação de forma a preservar o patrimônio e a informação da instituição.

§1º Os recursos e serviços de TI devem ser utilizados de maneira responsável, de acordo com os objetivos de ensino, pesquisa, extensão e de gestão do IFTO.

§2º Os recursos e serviços de TI não podem ser utilizados para invadir, alterar ou destruir sistemas de informação ou a infraestrutura de TI do IFTO, de outras instituições ou de indivíduos.

Art. 2º Esta norma abrange recursos de tecnologia da informação relacionados a uma variedade de áreas para garantir que o IFTO utilize, proteja e gerencie seus recursos de TI de maneira eficiente, segura e conforme regulamentações vigentes no âmbito da administração pública federal. No IFTO são considerados como recursos de TI:

- I - equipamentos de informática de qualquer espécie e seus componentes periféricos;
- II - servidores de rede;
- III - ativos de redes e de telecomunicações de qualquer espécie;
- IV - softwares;
- V - impressoras;
- VI - laboratórios de informática de qualquer espécie, incluindo, mas não se limitando a salas multimídia e videoconferência;
- VII - redes de comunicação de dados;
- VIII - sistemas de informação;
- IX - soluções de computação em nuvem;
- X - mídias sociais; e

XI - comunicação eletrônica.

CAPITULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 3º Para fins de compreensão dos termos utilizados neste documento serão utilizados os seguintes conceitos e definições:

I - ameaça: conjunto de fatores externos com o potencial de causar em dano para um sistema ou organização;

II - atividade: ação ou conjunto de ações executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;

III - ativo: tudo que tenha valor para a organização, material ou não;

IV - ativos de informação: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

V - *backup/cópia de segurança*: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

VI - banco de dados: coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam, a fim de criar algum sentido (informação) e de dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento;

VII - Comitê de Segurança da Informação: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal;

VIII - computação em nuvem: modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem (PSN);

IX - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação;

X - controles de segurança: certificado que autoriza uma pessoa natural para o tratamento de informação classificada;

XI - criptografia: arte de proteção da informação, por meio de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem;

XII - CTIR GOV: Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, subordinado ao Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República;

XIII - descarte: eliminação correta de informações, documentos, mídias e acervos digitais;

XIV - documento: unidade de registro de informações, qualquer que seja o suporte ou o formato;

XV - e-mail: sigla de correio eletrônico (*electronic mail*);

XVI - eliminação: exclusão de dado ou conjunto de dados, armazenados em banco de dados, independentemente do procedimento empregado;

XVII - equipe de tratamento e resposta a incidentes cibernéticos (ETIR): grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da administração pública federal, em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação. Anteriormente era chamada de Equipe de Tratamento de Incidentes Cibernéticos;

XVIII - evento: qualquer mudança de estado que tem importância para a gestão de um item de configuração ou serviço de tecnologia da informação. Em outras palavras, qualquer ocorrência dentro do escopo de tecnologia da informação que tenha relevância para a gestão dos serviços entregues ao cliente;

XIX - evento de segurança: qualquer ocorrência identificada em um sistema, serviço ou rede, que indique uma possível falha da política de segurança, falha das salvaguardas ou mesmo uma situação até então desconhecida, que possa se tornar relevante em termos de segurança;

XX - *firewall*: ferramenta para evitar acesso não autorizado, tanto na origem quanto no destino, a uma ou mais redes. Podem ser implementados por meio de hardware ou software, ou por meio de ambos. Cada mensagem que entra ou sai da rede passa pelo *firewall*, que a examina a fim de determinar se atende ou não os critérios de segurança especificados;

XXI - incidente: interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

XXII - incidente cibernético: ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema;

XXIII - incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XXIV - informação: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXV - internet: rede global, composta pela interligação de inúmeras redes. Conecta mais de 500 milhões de usuários, provendo comunicação e informações das mais variadas áreas de conhecimento;

XXVI - medidas de segurança: medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo;

XXVII - política de segurança da informação: documento aprovado pela autoridade responsável pelo órgão ou entidade da administração pública federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação. Este termo substituiu o termo Política de Segurança da Informação e Comunicação;

XXVIII - prestador de serviço: pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso;

XXIX - rede de computadores: conjunto de computadores, interligados por ativos de rede, capazes de trocar informações e de compartilhar recursos, por meio de um sistema de comunicação;

XXX - risco: no sentido amplo, trata-se da possibilidade de ocorrência de um evento que pode impactar o cumprimento dos objetivos. Pode ser mensurado em termos de impacto e de probabilidade;

XXXI - risco de segurança da informação: risco potencial associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

XXXII - serviços: meio de fornecimento de valor a clientes, com vistas a entregar os resultados que eles desejam, sem que tenham que arcar com a propriedade de determinados custos e riscos;

XXXIII - SI: sigla de segurança da informação;

XXXIV - sistema de informação: conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens, que possibilitam a agregação dos recursos de tecnologia, informação e comunicações de forma integrada;

XXXV - tecnologia da informação: ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas, utilizados para obter, processar, armazenar, disseminar e fazer uso de informações; e

XXXVI - usuário: pessoa física ou jurídica com vínculo formal direto ou indireto com o IFTO, ou em condição autorizada, que faça uso de algum recurso de TI da instituição, de qualquer forma, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da administração pública federal, formalizada por meio da assinatura de Termo de Responsabilidade.

CAPÍTULO III DOS PRINCÍPIOS

Art. 4º Esta política considera os seguintes princípios:

I - respeito aos princípios e diretrizes constitucionais, legais e regulamentares que regem a administração pública federal;

II - garantia de integridade, autenticidade e disponibilidade da informação sob a custódia do IFTO, com respeito ao princípio da transparência e atribuição de confidencialidade apenas nos casos expressamente previstos na legislação;

III - alinhamento estratégico da Política de Segurança da Informação com os demais planos institucionais;

IV - responsabilidade pelo cumprimento das normas pertinentes à segurança da informação vigentes; e

V - conscientização, educação e comunicação como alicerces fundamentais para o fomento da cultura em segurança da informação.

CAPÍTULO IV DAS DIRETRIZES GERAIS

Art. 5º A equipe de TI deverá realizar a gestão (especificação, instalação, administração e manutenção) dos recursos de Tecnologia da Informação, em conformidade com as exigências regulatórias e orientações governamentais.

§1º Os recursos de TI devem ser utilizados de maneira responsável, consistente com os objetivos educacionais das áreas de gestão, ensino, pesquisa e extensão.

§2º Os procedimentos de operação dos recursos de TI devem ser definidos, documentados e atualizados continuamente.

§3º Competências e responsabilidades devem ser definidas para gestão e uso de recursos de TI para garantir que haja um controle satisfatório de todas as mudanças em equipamentos, softwares, recursos, sistemas, serviços ou procedimentos.

§4º Funções e áreas de responsabilidade devem ser segregadas para reduzir as oportunidades de modificação ou uso indevido não autorizado ou não intencional dos recursos de TI.

§5º Na medida do possível registros (logs) de auditoria devem ser coletados dos dispositivos, recursos, sistemas e serviços de TI considerados críticos para o IFTO.

§6º Acordos de níveis de serviços devem ser estabelecidos com prestadores de serviço de forma a garantir níveis adequados de proteção de dados e segurança da informação.

§7º Prestação de serviços relacionados a recursos de TI devem ser avaliadas, documentadas e monitoradas continuamente.

§8º Procedimentos operacionais apropriados para a proteção de documentos, mídias magnéticas de computadores, dados de entrada e saída e documentação de sistema devem ser estabelecidos para evitar divulgação não autorizada, modificação, remoção e destruição.

§9º Mídias devem ser descartadas de forma segura e protegida quando não forem mais necessárias, por meio de procedimentos formais.

§10º Informações envolvidas em transações on-line devem ser protegidas para prevenir transmissões incompletas, erros de roteamento, alterações não autorizadas de mensagens, divulgação não autorizada, duplicação ou rerepresentação de mensagem não autorizada.

§11º Aplicações, dados e informações adicionais que requeiram um alto nível de integridade e que sejam disponibilizados em sistemas publicamente acessíveis devem ser protegidos por mecanismos apropriados.

§12º O uso de programas utilitários capazes de sobrepor os controles dos sistemas e aplicações deve ser restrito e controlado.

§13º Recursos de segurança da informação devem ser utilizados para restringir o acesso aos sistemas de informação.

§14º Regras, planos operacionais e procedimentos para o uso de recursos de trabalho remoto devem ser estabelecidos, implementados e atualizados de forma a evitar furto ou roubo do equipamento e de informações.

§15º Regras para o uso de controles criptográficos para a proteção da informação devem ser desenvolvidas e implementadas.

§16º Procedimentos para controle de instalação de *softwares* em sistemas operacionais devem ser implementados, documentados e atualizados continuamente.

§17º A utilização dos recursos de Tecnologia da Informação com finalidade pessoal é permitida, desde que não viole as normas institucionais de segurança da informação previstas pelo IFTO.

§18º O IFTO se reserva o direito de realizar investigação forense digital em quaisquer dos recursos de Tecnologia da Informação que integram sua rede de comunicação de dados, sem prévio aviso, sempre que necessário para garantir a segurança da informação.

§19º Sempre que necessário, para preservação da integridade dos recursos de Tecnologia da Informação, técnicos da equipe de TI poderão, mediante fundamentação formal, suspender temporariamente qualquer conta, acesso à site, serviços e sistemas informatizados durante análises de incidentes de segurança até que todos os fatos sejam completamente apurados.

§20º Instituições e pessoas sem vínculo formal ao instituto poderão utilizar os recursos de Tecnologia da Informação, desde que respeitadas as orientações e diretrizes de uso estabelecidas neste documento.

§21º Solicitações de instalação e/ou configuração de recursos de Tecnologia da Informação deverão ser feitas através da central de serviços disponibilizada no SUAP.

§22º Os recursos de TI não devem ser utilizados para invadir, alterar ou destruir recursos computacionais de outras instituições.

§23º Os direitos de acesso a cada recurso, sistema ou serviço de TI serão concedidos de maneira seletiva, de acordo com a necessidades do usuário e com a atribuição referente ao

cargo do usuário, mediante deferimento de perfis e níveis de acesso, e poderão ser retirados ou restringidos por solicitação do chefe do setor onde o usuário está lotado, setor de TI ou setor de gestão de pessoas.

§24º Mudanças de lotação de servidores deverão ser comunicadas imediatamente pelo setor de origem ao setor de TI, para que se conceda ou exclua o acesso aos recursos, sistemas e serviços de TI.

CAPÍTULO V DOS EQUIPAMENTOS

Art. 6º Os equipamentos disponibilizados aos usuários terão configurações de *hardware* e *software*, definidas pela equipe de TI, compatíveis com a natureza da utilização.

§1º Os equipamentos devem ser acessados através de identificador pessoal único e intransferível (*login* de usuário).

§2º As atividades de manutenção e suporte de equipamentos serão realizadas e/ou coordenadas pela equipe de TI.

§3º Manutenção nos equipamentos, solicitadas pelo usuário, serão agendadas e realizadas após abertura de chamado na central de serviços disponibilizada no SUAP.

§4º Somente técnicos autorizados pelo equipe de TI devem realizar manutenções preventivas e corretivas em equipamentos pertencentes ao IFTO.

§5º Alterações na configuração padrão do ambiente operacional dos equipamentos, realizadas pelo usuário, devem ser notificadas, justificadas e autorizadas pela equipe de TI.

§6º Arquivos digitais salvos nas unidades de armazenamento de dados dos equipamentos 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.

§7º O compartilhamento de pastas e arquivos digitais, armazenados em equipamentos, 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.

§8º O usuário deve informar à equipe de TI qualquer identificação de dispositivo estranho conectado ao equipamento que utilizar.

§9º 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.

§10º Equipamentos que integram o patrimônio da instituição 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.

§11º Os equipamentos pessoais conectados à rede de dados institucional estão sujeitos às mesmas políticas, diretrizes e regulamentações previstas nesta norma.

§12º Os equipamentos institucionais deverão manter preservados, de modo seguro, os registros de eventos com identificação de *login* de usuário, data e horário de acesso de forma a resguardar a segurança da informação.

§13º O usuário não deve armazenar informações pessoais em equipamentos do IFTO. Arquivos não pertinentes às atividades da Instituição (documentos, fotos, músicas, vídeos, etc.) poderão ser excluídos sem comunicação prévia.

§14º Atualizações de segurança nos equipamentos institucionais poderão ocorrer 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.

§15º Equipamentos portáteis devem ser guardados em local seguro, com controle de acesso e garantia quanto à sua integridade.

§16º Na medida do possível os equipamentos devem manter o sistema operacional, aplicativos e programas atualizados com as últimas versões de patches de segurança para evitar vulnerabilidades conhecidas.

§17º Firewalls e programas antivírus/anti-*malware* confiáveis devem ser atualizados continuamente para proteger contra ameaças internas e externas.

CAPÍTULO VI DOS SERVIDORES DE REDE

Art. 7º A segurança de servidores de rede é essencial para proteger os dados sensíveis e manter a integridade das operações do IFTO.

§1º Servidores de rede devem ser mantidos em salas seguras, com acesso restrito apenas a pessoas autorizadas de forma a prevenir o acesso não autorizado aos equipamentos.

§2º Sempre que possível servidores de rede devem ter sistemas operacionais e softwares atualizados com patches de segurança mais recentes para mitigar vulnerabilidades conhecidas.

§3º Serviços considerados desnecessários devem ser desativados ou desinstalados para reduzir a superfície de ataque.

§4º Firewalls e filtros de pacotes devem ser implementados para controlar e monitorar o tráfego de rede, permitindo apenas o tráfego necessário.

§5º Deve-se estabelecer uma política de controle de acesso rigorosa para garantir que apenas pessoal autorizado possa acessar o servidor.

§6º Eventos de segurança devem ser registrados e monitorados para detectar atividades suspeitas ou tentativas de acesso não autorizado.

§7º Criptografia de dados deve ser utilizada para proteger dados sensíveis, tanto em trânsito quanto em repouso, especialmente se houver transferência de dados pela rede.

§8º Backups regulares dos dados do servidor devem ser realizados e testes de recuperação devem ser executados para garantir a integridade e utilidade em caso de falhas ou incidentes.

§9º Auditoria de segurança devem ser realizadas periodicamente para identificar e corrigir quaisquer vulnerabilidades ou falhas de configuração no servidor.

§10º Regras de segurança da informação devem ser estabelecidas e implementadas para a administração e manutenção de servidores.

§11º Administradores de sistemas devem ser conscientizados e treinados sobre as melhores práticas de segurança para garantir que eles estejam cientes dos riscos e saibam como agir adequadamente.

CAPÍTULO VII DOS ATIVOS DE REDE

Art. 8º A segurança dos ativos de rede é crucial para proteger a infraestrutura e os dados.

§1º Um inventário atualizado de todos os ativos de rede deve ser mantido atualizado incluindo dispositivos, equipamentos de rede, software e serviços em execução para ajudar a identificar e gerenciar adequadamente os recursos de TI.

§2º A rede deve ser dividida em segmentos lógicos, utilizando VLANs ou outros métodos de segmentação, para restringir o tráfego entre diferentes partes da rede e limitar a propagação de eventuais ataques.

§3º Mecanismos de autenticação forte para acessar ativos de rede devem ser implementados como por exemplo: senhas robustas, autenticação de dois fatores e políticas de controle de

acesso baseadas em funções.

§4º Os ativos de rede devem ser mantidos atualizados com patches de segurança mais recentes, incluindo roteadores, *switches*, firewalls e outros dispositivos de rede.

§5º Firewalls devem ser implementados em pontos estratégicos da rede para controlar e monitorar o tráfego.

§6º Avaliações periódicas de vulnerabilidades devem ser realizadas na rede para identificar possíveis pontos fracos e corrigi-los antes que possam ser explorados por ameaças.

§7º Protocolos de criptografia devem ser utilizados para proteger o tráfego de dados sensíveis e comunicação segura.

§8º Política de segurança de rede deve ser estabelecida e mantida atualizada incluindo diretrizes para configurações padrão, políticas de senha, uso aceitável da rede e acesso remoto.

§9º Backups regulares de configurações e dos dados críticos da rede devem ser realizados para permitir uma rápida recuperação em caso de incidente ou falha.

§10º Administradores de rede devem ser conscientizados e treinados sobre as melhores práticas de segurança da rede para que possam lidar com riscos potenciais e estabelecer procedimentos a serem seguidos em caso de incidentes.

CAPÍTULO VIII DO USO DE SOFTWARES

Art. 9º Softwares devem ser utilizados com segurança minimizando os riscos de exposição a ameaças e garantindo a proteção dos dados e sistemas.

§1º Softwares devem ser utilizados a partir de fontes confiáveis e verificadas.

§2º Os usuários devem evitar instalar programas de origens desconhecidas ou suspeitas, pois podem conter malware.

§3º Softwares devem ser mantidos atualizados com versões mais recentes e patches de segurança.

§4º A equipe de TI deverá manter atualizado o inventário de *softwares* homologados e utilizados em equipamentos institucionais.

§5º O usuário será responsabilizado por quaisquer programas e/ou aplicativos que tenham sido instalados, utilizando sua conta de acesso a rede IFTO.

§6º 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.

§7º 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:

I - quantidades de licenças de uso adquiridas;

II - conformidade com a área de atuação do setor interessado;

III - compatibilidade com os sistemas operacionais e softwares utilizados pelo IFTO;

IV - desempenho do ambiente computacional; e

V - impacto entre a necessidade de instalação e a demanda de outros setores.

§8º 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.

Art. 10º *Software* produzido no âmbito do IFTO por qualquer dos integrantes de sua comunidade será regido por norma específica.

CAPÍTULO IX DO USO DE IMPRESSORAS

Art. 11º equipamentos de impressão instalados no parque computacional do IFTO são para uso exclusivo relacionados a atividades de gestão, ensino, pesquisa e extensão.

§1º Sistema de monitoramento e controle para registrar e controlar o acesso à impressora deve ser utilizado.

§2º O firmware da impressora deve ser mantido atualizado.

§3º Somente os usuários previamente autorizados deverão ter acesso aos recursos de impressão.

§4º Senhas devem ser definidas para acesso a funções específicas das impressoras.

§5º Usuários devem ser conscientizados sobre práticas seguras ao utilizar a impressora, como não deixar documentos sensíveis na bandeja de saída e a importância de seguir as diretrizes de segurança ao imprimir documentos confidenciais.

§6º 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.

§7º As unidades do IFTO deverão definir estratégias para a centralização de impressão de documentos através de ilhas e servidor de impressão.

§8º 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.

§9º Todo o suporte e manutenção de impressora deve ser registrado através da central de serviços disponibilizada no SUAP.

§10º 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 DE TECNOLOGIA DA INFORMAÇÃO

Art. 12º As atividades de suporte e manutenção em recursos de TI são vitais para garantir a funcionalidade e a segurança dos recursos, sistemas e serviços de TI:

§1º Solicitação de atendimento para instalação, manutenção, suporte e configuração dos recursos de Tecnologia da Informação deve ser efetuada mediante abertura de chamado na central de serviços disponível no SUAP.

§2º A execução dos serviços de assistência técnica e manutenção realizada pelos servidores da área de TI deve ser realizada apenas em equipamentos de propriedade do IFTO.

§3º 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.

§4º 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.

§5º As atividades de suporte e manutenção em recursos de TI devem ser documentadas para ajudar a garantir consistência e conformidade com as políticas de segurança da informação.

CAPÍTULO XI

DA DISPONIBILIZAÇÃO DE RECURSOS DE TECNOLOGIA DA INFORMAÇÃO PARA PROJETOS DE ENSINO, PESQUISA E EXTENSÃO

Art. 13º Serão disponibilizados para ensino, pesquisa e extensão recursos de Tecnologia da Informação, 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 destes recursos serão observadas as seguintes diretrizes:

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 e responderá pelos incidentes de segurança da informação originados pelo recurso de TI disponibilizado para o 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; e

IV - a equipe de TI poderá bloquear a comunicação entre o recurso de TI 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. 14º A segurança da rede de comunicação de dados é essencial para proteger informações confidenciais e garantir a integridade, confidencialidade e disponibilidade dos dados transmitidos.

§1º As redes devem ser adequadamente gerenciadas e controladas pela equipe de TI local nas unidades do IFTO, de forma a protegê-las contra ameaças e manter a segurança de sistemas e aplicações que utilizam estas redes.

§2º A banda consumida por aplicações específicas fica sujeita à limitação, sendo de responsabilidade dos administradores de redes e sistemas lotados no setor de TI da unidade a definição do percentual de uso da banda total disponível.

§3º É vedado adicionar qualquer equipamento estranho de interconexão de rede nas instalações do IFTO sem autorização prévia, específica ou genérica, dada pelos administradores de redes e sistemas.

Seção I

Da distribuição de blocos de endereços IP disponibilizados pela RNP

Art. 15º 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).

Parágrafo único. 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. 16º 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 diretrizes:

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; e

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

Seção III

Dos servidores de domínio

Art. 17º 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 deverão ser 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; e

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

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

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

Seção IV

Dos firewalls

Art. 18º Os *firewalls* deverão ser configurados atendendo as seguintes diretrizes:

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; e

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

Art. 19º 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 de Tecnologia da Informação 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; e

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

Art. 20º 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.

Parágrafo único. A 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.

Art. 21º 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 V

Do acesso a Internet

Art. 22º A utilização da internet englobando desde a navegação de sites, downloads e uploads de arquivos deverá seguir as seguintes diretrizes.

§1º A internet deve 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.

§2º Informações sobre URLs, endereços IP, sítios e aplicações web acessados a partir da rede do IFTO poderão ser armazenados em dispositivos de auditoria protegidos e sob responsabilidade do setor de TI. Estas informações poderão ser utilizadas somente para fins específicos de tratamento de incidentes de segurança, para melhoria da infraestrutura de TI ou para o cumprimento de ordem judicial.

§3º Terão acesso à internet os servidores técnicos administrativos, professores, estudantes, prestadores de serviços, temporários, voluntários, fornecedores, estagiários e pessoas que participam de projetos de ensino, pesquisa e extensão.

§4º Caberá à equipe de TI aplicar as restrições de acesso à internet necessárias por meio de ferramenta de filtro de conteúdo.

§5º 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.

§6º 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.

Art. 23º 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. 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:

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

II - priorização de acessos a determinados sites e serviços; e

III - limitação de tráfego na rede.

Parágrafo único. 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 sobre a viabilidade do desbloqueio.

Art. 24º Constituem uso indevido do serviço de acesso à internet as seguintes ações:

I - acessar páginas de conteúdo considerado ofensivo, ilegal ou impróprio, tais como: pornografia, pedofilia, racismo, comunidades de relacionamento pessoal, jogos, dentre outros;

II - utilizar programas de troca de mensagens em tempo real (bate-papo), exceto os definidos como ferramenta de trabalho e homologados pelo setor de TI da unidade;

III - acessar páginas de áudio e vídeo em tempo real, ou sob demanda, exceto nos casos de comprovada necessidade, mediante solicitação ao setor de TI da unidade;

IV - obter na internet arquivos (*download*) que não estejam relacionados com suas atividades funcionais, a saber: imagens, áudio, vídeo, jogos e programas de qualquer tipo; e

V - acessar sítios que apresentem vulnerabilidade de segurança ou possam comprometer de alguma forma a segurança e integridade da rede de computadores do IFTO.

Seção VI

Do monitoramento e auditoria

Art. 25º O IFTO por meio da equipe de TI poderá monitorar e auditar a rede de comunicação de dados visando garantir a disponibilidade e a segurança das informações, bem como a apuração de violações às diretrizes de segurança da informação.

Parágrafo único. Os registros de acessos à rede poderão ser arquivados e utilizados, exclusivamente, para fins de auditoria.

Seção VII

Da rede sem fio

Art. 26º As diretivas básicas de segurança da informação para a rede sem fio são:

I - o acesso à rede sem fio 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; e

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

Seção VIII

Da segurança lógica

Art. 27º O IFTO deverá manter soluções de proteção contra problemas de segurança lógica (vírus, acesso não autorizado, invasões, desempenho, espaço em disco, etc.), cabendo à área de TI da unidade a definição de tais soluções de proteção, considerando a criticidade dos

ativos de informação envolvidos e que estejam sob sua responsabilidade.

Art. 28º Cabe aos servidores lotados na área de TI a definição dos procedimentos de segurança para a implantação, manutenção, atualização, desinstalações e recuperação de softwares, sistemas operacionais, bancos de dados, de forma a garantir que estes ambientes lógicos não tragam vulnerabilidades que comprometam a segurança da informação, bem como, propor as normas que regulamentarão tais procedimentos.

Art. 29º Cabe aos responsáveis pela área de TI na unidade providenciar que os ambientes lógicos, sob sua responsabilidade, tenham o seu acesso restrito por senhas seguras, ou outros mecanismos de segurança apropriados, salvo em situações nas quais existam restrições técnicas impeditivas.

CAPÍTULO XIII DOS SISTEMAS DE INFORMAÇÃO

Art. 30º Diretrizes de segurança da informação para sistemas de informação são fundamentais para proteger os dados, garantir a confiabilidade e a integridade das operações.

Parágrafo único. Regras para o desenvolvimento, manutenção e operação de sistemas de informação devem ser estabelecidos, documentadas e atualizadas continuamente observando os seguintes aspectos:

I - identificação e classificação de dados;

II - controle de acesso;

III - política de senha e autenticação;

IV - auditoria e monitoramento;

V - atualizações e patches de segurança;

VI - criptografia de dados;

VII - backup e recuperação de dados;

VIII - gestão de vulnerabilidades;

IX - gestão de incidentes; e

X - conformidade com regulamentações.

CAPÍTULO XIV DA UTILIZAÇÃO DE SOLUÇÕES DE COMPUTAÇÃO EM NUVEM

Art. 31º O IFTO deverá estabelecer estratégia e norma sobre o uso seguro de software e prestação de serviços em nuvem computacional, considerando os seguintes aspectos:

I - modelo de contratação de *software* e de serviços de computação em nuvem, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal; e

II - requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem no âmbito da administração pública federal.

CAPÍTULO XV DO USO DE MÍDIAS SOCIAIS

Art. 32º O IFTO deve editar ato normativo sobre o uso seguro de mídias sociais conforme legislação pertinente.

§ 1º Os usuários não devem utilizar os recursos de TI para acesso a mídias sociais com a finalidade de produzir, compartilhar ou distribuir conteúdos ofensivo, obsceno, pornográfico, sexualmente sugestivo, abusivo, discriminatório, difamatório, ameaçador, de ódio, infrinja a

Lei nº 7.716, de 5 de janeiro de 1989, infrinja as leis de propriedade intelectual e as leis de privacidade.

§ 2º Ao usar mídias sociais os usuários devem considerar as práticas de segurança da informação para proteger sua privacidade e dados pessoais, tais como:

I - configurações de privacidade devem ser revisadas e reajustadas continuamente limitando o acesso às suas informações apenas para pessoas confiáveis e deve configurar as opções de compartilhamento de acordo com suas preferências;

II - os usuários devem usar senhas fortes e exclusivas para cada uma de suas contas de mídia social;

III - os usuários devem ativar a autenticação de dois fatores sempre que possível para adicionar uma camada extra de segurança;

IV - os usuários devem evitar compartilhar informações pessoais sensíveis, como números de telefone, endereço residencial, detalhes financeiros, ou informações de identificação pessoal;

V - antes de postar, os usuários devem certifique-se de verificar quem pode ver as publicações;

VI - os usuários devem evitar compartilhar informações que possam comprometer sua segurança ou privacidade;

VII - os usuários devem manter os aplicativos de mídia social atualizado com as versões mais recentes para garantir a correção de vulnerabilidades conhecidas;

VIII - os usuários devem ter cuidado ao clicar em links ou baixar arquivos de fontes desconhecidas ou não confiáveis nas mídias sociais, pois podem conter malware ou *phishing*;

IX - os usuários devem estar atentos a tentativas de engenharia social;

X - os usuários devem revisar regularmente os aplicativos e serviços conectados às suas contas de mídia social;

XI - os usuários devem revogar o acesso de aplicativos desnecessários ou suspeitos; e

XII - antes de compartilhar qualquer conteúdo os usuários devem avaliar as consequências.

CAPÍTULO XVI DO SERVIÇO DE COMUNICAÇÃO ELETRÔNICA

Art. 33º O serviço de e-mail corporativo é exclusivo do IFTO, constituindo-se ferramenta de comunicação corporativa oficial a ser utilizada de forma ética e legal, podendo ser acessado por meio de navegador ou aplicativos homologados pelo Google.

§1º Os usuários da rede IFTO devem evitar utilizar o seu endereço com o domínio "ifto.edu.br" para comunicações de caráter pessoal.

§2º Usuários que utilizem os serviços de comunicação eletrônica institucional para fins pessoais, deverá fazê-lo ciente da obrigatoriedade de cumprimento das normas da IFTO e da possibilidade de acesso ao conteúdo das comunicações eletrônicas, nos termos do disposto na norma que trata sobre e-mail institucional.

CAPÍTULO XVII DAS RESPONSABILIDADES

Seção I Da alta administração

Art. 34º Cabe à alta administração:

I - prover a orientação e o apoio necessário às ações de segurança da informação, de acordo com os objetivos estratégicos, planos institucionais, estrutura organizacional, leis e

regulamentos pertinentes; e

II - disponibilizar recursos (humanos, tecnológicos e financeiros) para a execução de ações relacionadas a execução desta norma.

Seção II

Do Comitê de Segurança da Informação

Art. 35º Cabe ao Comitê de Segurança da Informação:

- I - deliberar sobre normas internas complementares sobre gestão e uso de recursos de TI;
- II - assessorar a implementação das ações de gestão e uso de recursos de TI;
- III - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre gestão e uso de recursos de TI;
- IV - participar da elaboração da norma de gestão e uso de recursos de TI;
- V - propor alterações à norma de gestão e uso de recursos de TI; e
- VI - deliberar sobre normas internas complementares de gestão e uso de recursos de TI .

Seção III

Do Gestor de Segurança da Informação

Art. 36º Cabe ao Gestor de Segurança da Informação:

- I - coordenar o Comitê de Segurança da Informação;
- II - coordenar a elaboração da Política de Segurança da Informação e das normas internas complementares de segurança da informação do IFTO, observadas as recomendações exaradas pelo Gabinete de Segurança Institucional da Presidência da República;
- III - assessorar a alta administração na implementação da Política de Segurança da Informação;
- IV - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;
- V - promover, com apoio da alta administração, a ampla divulgação da PSI, das normas internas complementares de segurança da informação e de suas atualizações, de forma ampla e acessível, a todos os usuários, a fim de que esses tomem conhecimento de tais instrumentos;
- VI - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;
- VII - propor recursos necessários às ações de segurança da informação;
- VIII - acompanhar os trabalhos da Equipe de Tratamento e Resposta a Incidentes Cibernéticos;
- IX - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;
- X - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação;
- XI - coordenar a gestão de riscos de segurança da informação em âmbito institucional;
- XII - coordenar a gestão de continuidade de negócios em segurança da informação;
- XIII - avaliar a conformidade nos aspectos de segurança da informação;
- XIV - coordenar ações de segurança da informação em âmbito institucional;
- XV - fomentar e coordenar ações periódicas de conscientização e de treinamento em segurança da informação para todas as partes interessadas, incluindo autoridades, servidores e

colaboradores; e

XVI - manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

Seção IV

Equipe de Tratamento e Resposta a Incidentes Cibernéticos

Art. 37º Cabe à Equipe de Tratamento e Resposta a Incidentes Cibernéticos:

I - deliberar sobre procedimentos internos para gestão e uso de recursos de TI;

II - receber, analisar e responder às notificações e atividades relacionadas à gestão e uso de recursos de TI; e

III - desenvolver as atividades de prevenção, tratamento e resposta a incidentes relacionados à gestão e uso de recursos de TI.

Seção V

Da Diretoria de Tecnologia da Informação e demais setores de TI das unidades do IFTO

Art. 38º Cabe à Diretoria de Tecnologia da Informação e demais setores de TI das unidades do IFTO:

I - definir o administrador de redes, pessoa designada formalmente com atribuição de gerenciar redes, bem como recursos de TI a elas conectados, direta ou indiretamente;

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

III - instalar, configurar, atualizar ou remover *hardwares e softwares*;

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

V - 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;

VI - 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;

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

VIII - 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;

IX - realizar vistoria periódica, no local ou por meio informatizado remoto, dos *softwares* instalados nos equipamentos de informática;

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

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

XII - controlar e se for o caso vetar o acesso a qualquer usuário que violar as diretrizes de segurança da informação estabelecidas na Política de Segurança da Informação e normas internas complementares ou ameaçar os direitos de outros usuários;

XIII - propor, obter aprovação da Direção Geral da unidade e implantar procedimentos locais de TI em consonância com esta norma e demais regulamentações publicadas pelo IFTO e governo federal; e

XIV - promover a segurança preventiva em todo o escopo físico e lógico das unidades do IFTO, respeitando às regulamentações em vigor e adequando às suas implementações às ações relacionadas às melhores práticas de gerenciamento de incidentes e segurança da informação.

Seção VI **Dos usuários**

Art. 39º Cabe aos usuários:

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 de Tecnologia da Informação;

II - 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 de Tecnologia da Informação;

III - contribuir para a melhoria dos níveis de segurança da informação dos recursos de Tecnologia da Informação disponibilizados pelo IFTO;

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

V - não permitir ou colaborar com o acesso indevido aos recursos de Tecnologia da Informação por parte de pessoas não autorizadas, sob pena de ser co-responsabilizado pelos eventuais problemas que esses acessos vierem a causar;

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

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

VIII - 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;

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

X - trocar periodicamente a senha de acesso aos recursos de Tecnologia da Informação;

XI - 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) e demais leis vigentes;

XII - 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;

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

XIV - desligar o computador de forma adequada e segura no final de sua jornada de trabalho, assim como o bloqueio de sua sessão sempre se se ausentar da estação de trabalho;

XV - 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);

XVI - responder pelos eventuais prejuízos comprovadamente atribuídos à sua conta/perfil ou seu uso autorizado, decorrentes de qualquer atividade desenvolvida com o auxílio dos recursos computacionais do IFTO;

XVII - não conectar, fisicamente ou logicamente a um recurso computacional do IFTO componentes estranhos à sua configuração atual, sem que haja uma autorização ou específica dos administradores de redes e sistemas do IFTO;

XVIII - utilizar apenas softwares com as licenças de uso válidas; e

XIX - permitir ou causar qualquer alteração ou destruição de ambientes operacionais, dados ou equipamentos de processamento ou comunicações instalados no IFTO, de sua propriedade ou de qualquer outra pessoa ou instituição.

CAPÍTULO XVIII DAS PROIBIÇÕES/VIOLAÇÕES

Art. 40º Qualquer violação ou suspeita de quebra das regras contidas neste documento deve ser comunicada imediatamente ao responsável direto pelo recurso de TI no local onde o fato tenha ocorrido. 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 de TI;

III - fornecer informações a terceiros sobre características, funcionalidades e configurações dos recursos de TI 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 de *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 de Tecnologia da Informação a terceiros não pertencentes ao quadro funcional do IFTO;

XII - utilizar as credenciais de acesso de outro usuário para acessar ou utilizar um recurso de TI 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 de Tecnologia da Informação, 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, inserir vírus, 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;

XXVI - sem autorização, invada a privacidade de indivíduos ou entidades que são autores, criadores, usuários ou responsáveis pelos recursos computacionais;

XXVII - sem autorização, destrua, altere, desmonte, desconfigure, impeça o acesso de direito ou interfira na integridade dos recursos computacionais;

XXVIII - faça-se passar por outra pessoa ou esconda sua identidade na utilização dos recursos de TI do IFTO com exceção dos casos em que o acesso anônimo é explicitamente permitido;

XXIX - viole ou tente 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; e

XXX - intercepte ou tente interceptar transmissão de dados não destinados ao seu próprio acesso.

CAPÍTULO XIX DAS PENALIDADES

Art. 41º O usuário será responsabilizado pelos atos que venham a acarretar algum dano em virtude de imprudência, imperícia ou negligência no uso dos recursos de Tecnologia da Informação do IFTO.

§ 1º A infração ou tentativa de infração às regras constantes neste documento ou às regras previstas em lei serão apuradas por meio de sindicância administrativa, processo administrativo disciplinar ou processo sumário, nos termos da legislação vigente.

§ 2º 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.

§ 3º Qualquer violação ou suspeita de violação dessa norma deve ser comunicada imediatamente ao responsável direto pelo recurso computacional no local onde o fato tenha ocorrido e, no mais breve momento possível, ao setor de TI para análise do caso e prosseguimento das ações cabíveis.

§ 4º Casos omissos não tratados nesta norma serão avaliados e tratados pelo Comitê de Segurança da Informação.

CAPÍTULO XX DA REVISÃO E ATUALIZAÇÃO

Art. 42º Esta norma deve passar por revisões, aprovações e atualizações sempre que houver alterações na legislação pertinente, nas diretrizes políticas do governo federal, alterações nas normativas internas do IFTO, ou quando considerada necessária pelo Comitê de Segurança da Informação.

CAPÍTULO XXI DAS DISPOSIÇÕES FINAIS

Art. 43º Esta norma deve ser divulgada amplamente a todos os usuários, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

Art. 44º A alta administração deverá disponibilizar os recursos (humanos, tecnológicos e financeiros) necessários para a execução das diretrizes contidas nesta norma.

Art. 45º Esta norma entra em vigor na data de sua publicação.



Documento assinado eletronicamente por **Fabiana Ferreira Cardoso, Gestora de Segurança da Informação**, em 15/12/2023, às 16:16, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Kleyton Matos Moreira, Diretor**, em 15/12/2023, às 16:22, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site http://sei.iftto.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2218199** e o código CRC **7B3BE70C**.

Avenida Joaquim Teotônio Segurado, Quadra 202 Sul, ACSU-SE 20, Conjunto 1, Lote 8 - Plano Diretor Sul — CEP 77020-450 Palmas/TO — (63) 3229-2200
portal.iftto.edu.br — reitoria@iftto.edu.br