UNIVERSIDADE FEDERAL DO OESTE DO PARÁ
CONSELHO SUPERIOR DE ADMINISTRAÇÃO

CENTRO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
COORDENAÇÃO DE REDES

NORMAS PARA UTILIZAÇÃO DOS RECURSOS DE REDES

CAPÍTULO I
DO OBJETIVO

Art. 1º Estabelecer as responsabilidades e regras para uso dos recursos de rede de computadores da instituição, sejam eles de infraestrutura física e/ou lógica.

CAPÍTULO II
DA ABRANGÊNCIA

Art. 2º Este documento se aplica a todos os usuários que utilizam os recursos da rede de dados da instituição e está alinhado com a Política de Segurança da Informação da universidade.

CAPÍTULO III
CONCEITOS E DEFINIÇÕES

Art. 3º Define termos referentes a segurança da informação:

I – Política de Segurança da Informação: Documento que estabelece diretrizes de Segurança da Informação a serem observadas no âmbito da Universidade Federal do Oeste do Pará;

II – ativos: Tudo aquilo que tem valor para a universidade, sejam equipamentos, softwares, informações ou pessoas. Tudo aquilo que necessita de proteção;

III – incidentes de segurança: É qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança da informação;

IV – endereço IP local: Número utilizado para identificar um dispositivo (computador, impressora, celular, etc.) na rede da universidade com visibilidade local, mas que permite acesso à Internet;

V – endereço IP válido: Número utilizado para identificar um dispositivo (computador, impressora, celular, etc.) na Internet. Possibilita que um dispositivo seja acessível a partir de qualquer lugar através da Internet, sendo necessário para a publicação de conteúdos visíveis a nível global;

VI – internet: Rede mundial de computadores;

VII – intranet: Rede de computadores privada que faz uso dos mesmos protocolos da Internet. Pode ser entendida como rede interna de alguma instituição em que geralmente o acesso ao seu conteúdo é restrito;

VIII- *peer-to-peer* (P2P) – (Ponto a ponto): Permite conectar o computador de um usuário a outro, para compartilhar ou transferir dados, como MP3, jogos, vídeos, imagens, entre outros.

CAPÍTULO IV
REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 4º Esta norma se baseia nas diretrizes estabelecidas pelo Art. 1º da Resolução nº 04 de 20 de outubro de 2015, que aprova a Política de Segurança da Informação e Comunicações no âmbito da Universidade Federal do Oeste do Pará.

CAPÍTULO V
POLÍTICA E REGRAS

Art. 5º O acesso à internet da instituição tem como finalidade o complemento às atividades administrativas dos setores, para aprimoramento, o enriquecimento intelectual dos servidores e comunidade acadêmica e/ou, como ferramenta de busca de informações. No âmbito institucional, tem como finalidade, também, ser meio para divulgação de informações de interesse da UFOPA e possibilitar o acesso aos sistemas de informação institucionais.
I – por não fazerem parte das atividades institucionais e por prejudicarem o tráfego na rede, sendo considerado má utilização da internet, fica proibido:
a) o uso de aceleradores de download;
b) a utilização de jogos online (salvo em casos de interesse da instituição);
c) o uso de programas de compartilhamento de arquivo ponto-a-ponto (*P2P - Peer-to-peer*);
d) acessar páginas de conteúdo considerado ofensivo, ilegal ou impróprio, tais como: Pornografia, pedofilia, preconceitos, vandalismo, entre outros;
e) uso recreativo da internet em horário de expediente;
f) acesso a rádio e TV online em horário de expediente, exceto os canais institucionais ou governamentais;
g) a divulgação de informações confidenciais da instituição por meio de correio eletrônico, grupos ou listas de discussão, sistemas de mensageiro ou bate-papo, blogs, microblogs, ou ferramentas semelhantes;
h) o envio a destino externo de qualquer software licenciado à UFOPA ou dados de sua propriedade ou de seus usuários, salvo expressa e fundada autorização do responsável pela sua guarda;
i) o contorno ou tentativa de contorno às políticas de bloqueios automaticamente aplicadas pelas ferramentas sistêmicas do CTIC.

Parágrafo único. O uso da rede para fins pessoais deve ser feito preferivelmente em horários fora do expediente e de maneira que não comprometa o tráfego de dados ou prejudique o funcionamento dos serviços oferecidos pela universidade.

Art. 6º A ocorrência de qualquer hipótese de má utilização da internet deverá ser comunicada, de imediato, ao CTIC.

Parágrafo único. Comprovada a utilização irregular, o usuário envolvido terá o seu acesso à Internet bloqueado pelo CTIC, caso seja servidor da instituição será comunicado o fato à chefia imediata, podendo incorrer em Processo Administrativo Disciplinar e nas sanções

legalmente previstas, assegurados o contraditório e a ampla defesa. Caso seja discente, responderá através dos procedimentos disciplinares correspondentes, assegurados o contraditório e a ampla defesa.

Art. 7º Ao fazer compartilhamentos de pastas e arquivos na rede da instituição, deve-se adotar o uso de senhas de compartilhamento. Este procedimento deve ser solicitado ao suporte através de abertura de chamado. O CTIC não se responsabilizará por acessos indevidos a arquivos em compartilhamentos de armazenamento em computadores institucionais e particulares, sendo a responsabilidade por esses compartilhamentos exclusivamente dos usuários.

Art. 8º Fica proibida a abertura de *racks* e manipulação de equipamentos de infraestrutura de redes sob responsabilidade do CTIC. Em caso de manipulação indevida de equipamentos, tais como *switches*, rádios, etc. serão tomadas as providências cabíveis para apurar os incidentes.

Parágrafo único. Apenas as equipes da Coordenação de Redes do CTIC, e pessoal autorizado por esta, podem manipular tais equipamentos.

Art. 9º Cabe ao CTIC solicitar abertura de Processo Administrativo Disciplinar para apurar os incidentes relacionados quando couber.

Art. 10 O CTIC terá direito de acesso aos locais onde estejam localizados os *racks* de equipamentos, inclusive, com direito a ter cópias das chaves para casos de emergências.

Art. 11 Fica proibida a instalação de equipamentos de rede (tais como: switches, *hubs*, roteadores, rádios, etc.) não autorizados pela Coordenação de Redes na rede de computadores da instituição, sendo tratados como Incidente de Segurança em caso de ocorrência:
I – caso seja necessária a instalação e/ou configuração de equipamentos de rede particulares ou de projetos, esta deve ser avaliada e autorizada pelo CTIC;
II – a Coordenação de Redes poderá bloquear os equipamentos instalados na rede da instituição, que não possuam a devida autorização do CTIC;
III – fica estabelecido que a gerência dos equipamentos de redes é responsabilidade do Centro de Tecnologia da Informação e Comunicação, sendo que os técnicos desse setor terão acesso direto a esses equipamentos quando necessário;
IV – esses equipamentos de rede ficarão sob custódia dos gestores do setor onde estão alocados, o que implica em cuidados sobre os equipamentos, tornando-os responsáveis por incidentes que venham a ocorrer.

Art. 12 As paralisações programadas dos serviços de Internet e Intranet, para manutenção preventiva, devem ser previamente comunicadas pelo CTIC a todos os usuários.

Parágrafo único. No caso de indisponibilidade repentina dos serviços de Internet ou Intranet por alguma falha, o CTIC deverá se pronunciar acerca do incidente.

CAPÍTULO VI
DO DATA CENTER

Art. 13 O objetivo do Data Center é oferecer a infraestrutura necessária para garantir a disponibilidade dos equipamentos que executam os sistemas que são fundamentais para a instituição, assegurando desta forma a continuidade do funcionamento desses sistemas.

Art. 14 O acesso ao Data Center se dará mediante autorização da Coordenação de Redes ou Direção do CTIC, sempre monitorado por servidores da unidade e por câmeras de segurança.

Art. 15 Todo acesso ao Data Center por pessoal que não faça parte da equipe da Coordenação de Redes deve ser registrado com data, horário e nome dos visitantes, seja por meio eletrônico ou registro manual em caderno ou ficha.

Art. 16 É proibida a entrada de alimentos, líquidos, produto inflamável ou qualquer outro produto nocivo ao ambiente do Data Center, exceto em casos necessários, autorizados pela equipe da Coordenação de Redes.

Art. 17 Qualquer entrada ou retirada de equipamentos do Data Center dependerá de autorização da equipe ou unidade responsável por este, devendo ser registrada, seja por meio eletrônico ou registro manual em caderno ou ficha.

Art. 18 Deve-se estabelecer Política de Proteção do Data Center.
I – o Data Center deve conter mecanismos para:
a) combate e prevenção de incêndios: prevenir e evitar que equipamentos sejam danificados por incêndios com a utilização de instrumentos como extintores e sensores de fumaça e alta temperaturas;
b) refrigeração: o Data Center deve oferecer o sistema de refrigeração redundante, para que em caso de falha de equipamento primário de refrigeração um sistema de refrigeração secundário entre em operação;
c) energia: sistemas de *nobreaks* e geradores deverão oferecer a proteção necessária contra oscilações de energia no Data Center, evitando corrompimento de dados e danos aos equipamentos.

Parágrafo único. O Data Center é a infraestrutura física projetada para abrigar servidores de rede e outros recursos computacionais, como sistemas de armazenamento de dados (*storages*), dentre outros recursos de rede (*switches*, roteadores), além do próprio cabeamento de rede de dados e equipamentos elétricos que sustentam o Data Center.

CAPÍTULO VII
DO ENDEREÇAMENTO DE IP (INTERNET PROTOCOL)

Art. 19 O endereçamento IP local na rede da UFOPA pode ser estático ou dinâmico, sendo tais endereços alocados e atribuídos pelo CTIC, manualmente ou através de DHCP (*Dynamic Host Configuration Protocol*) ou serviço similar.

Art. 20 É vetado o uso de endereços IPs locais estáticos por usuários, sem conhecimento do CTIC.

Art. 21 O usuário, flagrado utilizando endereços IPs estáticos, sem conhecimento do CTIC, receberá advertência e em caso de reincidência, responderá por Incidente de Segurança da Informação.

Art. 22 O uso de endereços IPs (Versão 4) válidos (endereços globais), pertencentes ao bloco de endereçamento alocado para a UFOPA, pela RNP (Rede Nacional de Ensino e Pesquisa), é restrito a equipamentos que exijam visibilidade na Internet, ou seja, que sejam acessíveis a partir da Internet.

Art. 23 A alocação dos IPs válidos para serviços mantidos pelo CTIC deve passar por avaliação da Coordenação de Redes, que realizará a alocação e registro do endereço, sendo a responsabilidade dos conteúdos divulgados na Internet atribuída ao setor solicitante.

Art. 24 A alocação dos IPs válidos para serviços (servidores) não mantidos pelo CTIC deve ser realizada mediante formalização de processo destinado ao CTIC, onde devem constar documentos detalhando o uso do endereço.

Art. 25 Podem solicitar endereços IPs válidos, servidores da UFOPA para uso em projetos de interesse da Universidade, mediante assinatura de termo de responsabilidade dos solicitantes, uma vez que o uso desse recurso gera responsabilidade legal.

Art. 26 O atendimento da solicitação de IP válido dependerá de viabilidade técnica, disponibilidade e avaliação técnica da equipe do CTIC, em especial a Coordenação de Redes, responsável pela gestão dos endereços. Cabe ao Comitê Gestor de Tecnologia da Informação, com participação do Comitê Gestor de Segurança da Informação, julgar os casos quando solicitado, respeitando a política de uso da Rede Ipê (Rede Nacional de Ensino e Pesquisa).

Art. 27 Para implementar acesso à Internet através de endereço IP válido, por uma questão técnica, o CTIC poderá fazer uso de NAT (*Network Address Translation*) com mapeamento do IP válido para um endereço local, estando este associado diretamente ao endereço válido.

Parágrafo único. O endereçamento IP, necessário para implementação do protocolo de Internet, fornece identificação para os equipamentos da rede. O endereçamento pode ser local (endereço IP local) ou global (endereço IP válido).

CAPÍTULO VIII
DA VIGÊNCIA

Art. 28 Estas normas passam a vigorar a partir da data de sua aprovação pelo Conselho Superior desta instituição.