UNIVERSIDADE FEDERAL DO PIAUÍ
Superintendência de Tecnologia da Informação

DISPÕE SOBRE A NORMA DE USO DA INTERNET DA UNIVERSIDADE FEDERAL DO PIAUÍ

ORIGEM

Superintendência de Tecnologia de Informação

REFERÊNCIA LEGAL E NORMATIVA

Decreto nº 9.637, de 26 de Dezembro de 2018.
Decreto nº 7.845, de 14 de Novembro de 2012.
NBR ISO/IEC 27001:2013.
PoSIN/UFPI - Política de Segurança da Informação da UFPI de xx de xxx de xx.

CAMPO DE APLICAÇÃO

Esta Norma se aplica no âmbito da Universidade Federal do Piauí.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não há

HISTÓRICO DE MUDANÇAS

Data	Revisão	Responsável	Detalhes
01/02/2020	00	Ênio Rodrigues	Produção da versão inicial para aprovação
05/01/2021	01	Ênio Rodrigues	Revisão e Atualização
02/02/2021	02	Colegiado Gestor da STI, Divisão de Segurança da Informação e Comissão de Regulamentação da STI	Revisão

Quadro 1. Histórico de mudanças desta Norma

1. CONSIDERAÇÕES INICIAIS

Esta norma faz parte dos instrumentos normativos de Segurança da Informação da Universidade Federal do Piauí (UFPI) complementar à Política de Segurança da Informação da Universidade Federal do Piauí - PoSIN/UFPI.

Neste documento constam orientações e regras de conduta que devem ser observadas por todos os agentes públicos, discentes e público externo, de forma a garantir o uso responsável da Internet através dos recursos disponibilizados pela Administração Pública do Poder Executivo.

2. OBJETIVO

Esta norma tem como objetivo estabelecer critérios para administração e utilização dos serviços de Internet e Intranet na Universidade Federal do Piauí.

3. FUNDAMENTO LEGAL

Conforme disposto no inciso II do Art. 15 do Decreto nº 9.637, de 26 de Novembro de 2018, da Secretaria-Geral da Presidência da República, compete aos órgãos e às entidades da Administração Pública Federal, em seu âmbito de atuação, elaborar sua política de segurança da informação e as normas internas de segurança da informação, observadas as normas de segurança da informação editadas pelo Gabinete de Segurança Institucional da Presidência da República. Ainda conforme o disposto no Art. 1º do Decreto nº 7.845, de 14 de Novembro de 2012, da Casa Civil da Presidência da República, é regulamentado procedimentos para o credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo no âmbito do Poder Executivo Federal.

4. CONCEITOS E DEFINIÇÕES

Para efeito desta Norma aplicam-se os seguintes conceitos e definições:

4.1 Agente Público: é todo aquele que presta qualquer tipo de serviço ao Estado, funções públicas, no sentido mais amplo possível dessa expressão, significando qualquer atividade pública. A Lei de Improbidade Administrativa (Lei nº 8429/92) conceitua agente público como “todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nas entidades mencionadas no artigo anterior”. Trata-se, pois, de um gênero do qual são espécies o servidor público, o empregado público, o terceirizado e o contratado por tempo determinado;

4.2 *Browser*: um navegador, também conhecido pelos termos ingleses web browser ou simplesmente browser, é um programa de computador que habilita seus usuários a interagirem com documentos virtuais da Internet, também conhecidos como páginas HTML, que estão hospedadas num servidor Web. Exemplos de browser: Internet Explorer, Mozilla Firefox, Opera, Safari e

Chrome;

4.3 Código Malicioso: Também conhecido por malware, é um programa desenvolvido especificamente para executar ações danosas em um computador;

4.4 Discente: toda e qualquer pessoa que tenha vínculo discente com a UFPI, ativo ou inativo e que utilize seus dados de acesso para uso da rede da universidade;

4.5 *Download*: (significa descarregar ou baixar, em português) é a transferência de dados de um computador remoto para um computador local;

4.6 Entidade Governamental: Incluem-se entre as entidades governamentais do poder executivo, para fins deste documento, as agências, auditorias, autarquias, empresas, federações, fundações, governadoria, procuradorias, secretarias e unidades desconcentradas;

4.7 *Internet*: é um conglomerado de redes em escala mundial de milhões de computadores interligados pelo Protocolo de Internet que permite o acesso a informações e todo tipo de transferência de dados;

4.8 Página: também conhecida pelo equivalente inglês webpage, é uma "página" na world wide web, geralmente em formato HTML e com ligações de hipertexto que permitem a navegação de uma página, ou secção, para outra;

4.9 *Peer-to-peer*: Conhecida como P2P (do inglês, peer-to-peer = ponto-a-ponto), é uma rede descentralizada de computadores que podem trocar entre si informações como músicas, vídeos, textos e programas. Os usuários das redes P2P fornecem e recebem dados ao mesmo tempo, ou seja, são servidores e clientes simultaneamente.

4.10 Recurso: além da própria informação, todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento;

4.11 *Software*: é uma sequência de instruções escritas para serem interpretadas por um computador com o objetivo de executar tarefas específicas. Também pode ser definido como os programas que comandam o funcionamento de um computador.

4.12 *Upload*: é a transferência de dados de um computador local para um servidor. Caso ambos estejam em rede, pode-se usar um servidor de FTP, HTTP ou qualquer outro protocolo que permita a transferência. É parecido com Download, só que em vez de carregar arquivos para a sua máquina, você os envia para o servidor;

4.13 Usuário: quem utiliza de forma autorizada recursos de informação da Administração Pública no âmbito do Poder Executivo da UFPI;

4.14 Vírus: É um programa ou parte de um programa, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos do computador.

4.15 *Proxy***:** é um servidor que recebe as requisições de um usuário e as passa para frente, dessa forma alterando o remetente da mensagem com o objetivo de filtrar o conteúdo ou enviar dados anonimamente.

5. DIRETRIZES GERAIS

5.1 Disponibilização de Acessos

5.1.1 O acesso à Internet será provido aos usuários que necessitem desse recurso para o desempenho de suas funções;

5.1.2 Para ter acesso à Internet o usuário deve receber orientações quanto ao uso correto desse recurso para assegurar que todos estão cientes das implicações referentes à segurança;

5.1.3 O acesso à rede interna (Intranet), ou rede externa via Internet, deve ser autenticado e criptografado;

5.1.3.1 A autenticação é a regra, casos excepcionais estão previstos, desde que fundamentados, justificados e autorizados pela unidade de Segurança de Rede da STI desta universidade. A autenticação dar-se-á por meio de credenciais pessoais e intransferíveis previamente cadastradas nos sistemas da UFPI;

5.1.3.2 Em casos de acessos internos a criptografia deve acontecer apenas nos casos que o ambiente/aplicação ou ambiente afim, assim exigir. A criptografia para acessos externos acontecerá se o fornecedor do serviço/ambiente/aplicação externa o disponibilizar, não estando a STI com a responsabilidade do fornecimento, segurança, criptografia e afins da aplicação de terceiros que seja de interesse do usuário.

5.2 Restrições de Acesso

5.2.1 É expressamente proibido utilizar a Internet de forma que possa prejudicar a imagem da Administração Pública ou de quaisquer de suas entidades, ou que prejudique o andamento dos trabalhos destas, ou que coloque em risco os ativos da rede de computadores da UFPI, dentre outras, nas seguintes situações:

a) Pornografia, pedofilia, preconceitos, vandalismo, entre outros;

b) Acessar ou obter na Internet arquivos que apresentem vulnerabilidade de segurança ou possam comprometer, de alguma forma, a segurança e a integridade da rede da UFPI;

c) Uso recreativo da Internet em horário de expediente;

d) Uso de *proxy* anônimo;

e) Acesso a jogos;

f) Acesso a outros conteúdos notadamente fora do contexto do trabalho desenvolvido;

g) Divulgação de informações confidenciais da instituição por meio de correio eletrônico, grupos, listas de discussão, sistemas de bate-papo, blogs, microblogs e ferramentas semelhantes;

h) Envio a destino externo de qualquer software licenciado à UFPI ou dados de sua propriedade ou de seus usuários, salvo expressa e fundada autorização do responsável pela sua guarda;

i) Tentativa de burlar as políticas de bloqueio aplicadas pelas ferramentas sistêmicas da UFPI;

j) Utilização de softwares de compartilhamento de conteúdos na modalidade *peer-to-peer*;

l) Tráfego de quaisquer outros dados em desacordo com a lei ou capazes de prejudicar o desempenho dos serviços de Tecnologia da Informação da UFPI, na forma definida pela STI;

m) Download de programas, jogos, protetores de telas, música, vídeos, imagens, *streaming* de vídeo e de áudio, *torrent* ou qualquer aplicação que não condiz com os propósitos da UFPI.

5.2.2 As situações descritas nos itens de a até m são consideradas permitidas se e somente se o usuário estiver no cumprimento de suas atribuições acadêmicas ou profissionais legítimas e de interesse da Administração Pública Federal;

5.2.3 O usuário poderá solicitar liberação de determinada página ou outro acesso, com a devida justificativa, mediante solicitação via chamado através da plataforma SINAPSE pelo link *https://sinapse.ufpi.br*;

5.2.4 Somente serão liberadas as páginas ou outro acesso analisadas e autorizadas pela Superintendência de Tecnologia da Informação - STI;

5.2.5 A ocorrência de qualquer hipótese de má utilização da Internet deverá ser comunicada, de imediato à STI;

5.2.6 Comprovada a utilização irregular, o usuário envolvido terá o seu acesso à Internet bloqueado pela STI, sendo comunicado o fato à chefia imediata, podendo incorrer em processo administrativo disciplinar e nas sanções legalmente previstas, assegurados o contraditório e a ampla defesa;

5.2.7 Cabe às coordenações e chefias disciplinar o uso da Internet em outras situações não previstas neste documento, desde que não fira o que estabelece o item 5.2.1;

5.2.8 No caso de download de interesse comum a várias áreas, convém que este seja realizado pela área responsável pela Tecnologia da Informação e disponibilizado aos interessados. Cita-se como exemplo, download de programas para cursos que exigem a instalação de determinado software nas máquinas determinada para aquela atividade em período de tempo definido pelos responsáveis da organização do evento;

5.2.9 Somente os usuários devidamente autorizados e em conformidade com suas atribuições funcionais podem fazer downloads, seguindo os procedimentos de segurança adotados pela entidade governamental da Administração Pública disponíveis no site da STI;

5.2.10 Os usuários que estiverem acessando a Internet devem encerrar sua conexão após término da navegação e bloquear a estação de trabalho sempre que se afastarem dela temporariamente.

5.3 Informações

5.3.1 Os navegadores de Internet e Intranet utilizados no âmbito da UFPI deverão ser homologados pela STI;

5.3.2 As paralisações dos serviços de Internet e Intranet, para manutenção preventiva, devem ser previamente comunicadas pela STI a todos os usuários;

5.3.3 No caso de indisponibilidade repentina dos serviços de Internet ou Intranet por alguma falha, a

paralisação deve ser comunicada pela STI via abertura de chamado através do sistema SINAPSE ou, quando da indisponibilidade deste sistema, via telefone;

5.3.4 Os problemas técnicos verificados pelos usuários, ocorridos durante o acesso aos serviços de Internet e Intranet, devem ser, o mais brevemente possível, comunicados à STI para que sejam solucionados;

5.3.5 Toda informação originada na Internet deve ser considerada suspeita até que seja confirmada por outros meios;

5.3.6 Antes de usar qualquer programa que tenha sido obtido da Internet, este deve ser testado e homologado pela área responsável em um equipamento preparado e isolado da rede da entidade governamental;

5.3.7 Antes de realizar download de qualquer natureza, desde que em atendimento aos interesses da administração pública, tais como textos, imagens, vídeos e sons, deve-se observar os direitos de uso do respectivo material;

5.3.8.Não é permitido upload (publicação, disponibilização) de programas ou de qualquer informação sem autorização da entidade proprietária ou custodiante de tal material.

5.4 Monitoramento/Auditoria

5.4.1 A entidade governamental, através de setor competente, se reserva o direito, a qualquer tempo e sem aviso prévio, de examinar os registros de acessos à Internet para verificação de atendimento à Política de Segurança. Tais registros podem referir-se a sites visitados, arquivos copiados da Internet, tempo gasto nos acessos e outras informações necessárias para a otimização dos recursos de acesso e realização de auditorias.

5.5 Recursos Tecnológicos

5.5.1 Toda conexão à Internet deve passar por equipamentos de segurança garantindo o controle de acesso e a aplicação dos demais mecanismos de segurança e, em caso contrário, o equipamento deve estar isolado da rede da entidade governamental;

5.5.2 Cada dispositivo com acesso a Internet (estação de trabalho, notebook, servidor de rede e outros) deve possuir um sistema de proteção instalado, ativado e atualizado contra vírus ou qualquer outro software malicioso;

5.5.3 Todo arquivo de texto, software ou dado copiado da Internet deve ser verificado automaticamente quanto à presença de vírus ou qualquer outro software com código malicioso antes da sua utilização.

5.5.4 A área responsável pela Tecnologia Informação deve prover as configurações de segurança a serem implementadas no browser das estações de trabalho, caso necessário.

5.6 Rede Sem Fio

5.6.1 A política de uso da rede sem fio deverá constar em documento auxiliar específico estendendo as diretrizes aqui já determinadas.

6. CONSIDERAÇÕES FINAIS

6.1 Esta Norma deverá ser amplamente publicada e divulgada, garantindo que todos tenham consciência da mesma, para usufruírem dos benefícios e assumirem as responsabilidades inerentes aos sistemas de informação da UFPI.

6.2 Os casos omissos a esta Norma serão resolvidos pelo Comitê de Segurança da Informação da UFPI, ouvido o CONSUN.

6.3 Esta Norma entra em vigor na data de sua aprovação pelo CONSUN, revogando-se as disposições em contrário.

Teresina, xx de xxxx de xxx

Xxxxx
Reitor