RESOLUÇÃO CONDIR 015/2009

Teresina, 12 de agosto de 2009.

Dispõe sobre a proteção dos Recursos de Tecnologia de Informação da Universidade Estadual do Piauí – UESPI, e dá outras providências.

A Reitora e Presidente do Conselho Diretor da Fundação Universidade Estadual do Piauí – UESPI, no uso de suas atribuições legais,

Considerando o processo nº 00007/09,

Considerando deliberação do Conselho Diretor em reunião plenária de 12/08/2009,

RESOLVE

Art. 1º - As normas dispostas neste Regulamento têm o escopo de proteger os recursos de Tecnologia de Informação, desta IES, das ameaças de:

I. Divulgação não autorizada de informações;
II. Modificações e/ou adulterações das informações;
III. Indisponibilidade dos recursos;
IV. Armazenamento de conteúdo ilegal;
V. Recebimento de conteúdo malicioso (vírus, cavalos-de-tróia, spywares);
VI. Invasões externas;
VII. Invasões à rede interna e de recursos compartilhados.

Art. 2º - Este Regulamento rege os procedimentos de todos os usuários (efetivos, terceirizados, estagiários, bolsistas, etc.) de recursos de Tecnologia de Informação da UESPI, que o seguirão como normas de uso geral.

§ 1º - São normas de uso geral:

I. Os usuários devem conhecer o Regulamento Geral de Segurança da Informação da UESPI.

II. Somente pessoal autorizado deve utilizar os recursos de informática e o seu uso deve ser limitado exclusivamente aos interesses desta IES e inerentes às funções de cada colaborador/terceirizado/estagiário/bolsista.

III. O usuário é responsável pelas informações armazenadas nos equipamentos dos quais faz uso e nos casos de equipamentos de utilização coletiva, o superior imediato é o responsável ou a pessoa por ele delegado.

IV. O usuário deve manter sigilo sobre as informações consideradas estratégicas e/ou confidenciais.

V. O usuário deve cientificar seu superior imediato, quando informações ou aplicações consideradas estratégicas e/ou confidenciais forem encontradas sem tratamento de segurança correto, o qual deve comunicar a ocorrência ao Núcleo de Processamento de Dados – NPD nesta IES.

VI. A transferência de grandes volumes de informações consideradas estratégicas e/ou confidenciais deve ser feita através da rede em diretórios (pastas) específicos para este fim, com orientação e supervisão de técnico designado pelo NPD.

VII. Documentos impressos de conteúdo estratégico e/ou confidencial devem ser resguardados contra acessos não autorizados.

VIII. Ao término de suas atividades, o usuário deve encerrar sua sessão (*logoff*) na estação de trabalho, que deve ser desligada ao final do expediente.

IX. Em casos de ausência do usuário por menores períodos (ex: intervalo do almoço), deve ser ativada a proteção de tela com senha (*screen saver*) em sua estação de trabalho. O período de tempo configurado para que a proteção de tela seja automaticamente acionada não deve exceder a 10 (dez) minutos.

X. Os diretórios (pastas) de trabalho das estações não podem ser compartilhados.

XI. Cabe ao NPD autorizar a conexão de equipamentos de prestadores de serviço na rede interna da UESPI.

XII. A entrada e saída de pessoas não pertencentes aos ambientes críticos de TI (salas de servidores, centrais de monitoramento, etc.) não são permitidas e as necessidades específicas devem ser autorizadas pelos gestores das áreas e registradas.

XIII. O usuário deve zelar pelo bom uso do equipamento e os problemas de manutenção em função de líquidos, restos de comida, etc. serão de sua responsabilidade.

XIV. O usuário é responsável pela guarda do equipamento e, em caso de roubo dentro do ambiente de trabalho, deverá informar à UESPI. Em caso de roubo fora do ambiente de trabalho, o usuário deverá tomar as providências cabíveis com a polícia ou órgãos competentes e notificar a Instituição.

XV. O usuário deve respeitar a integridade dos Recursos de Tecnologia de Informação da UESPI e a menos que tenham uma autorização específica para esse fim, não podem tentar, permitir ou causar qualquer alteração ou destruição de ambientes operacionais, dados ou equipamentos de processamento ou comunicações instalados na UESPI, de sua propriedade ou de qualquer outra pessoa ou instituição.

XVI. O usuário não pode ligar ou desligar fisicamente ou eletricamente um recurso de tecnologia de informação da UESPI, nenhum componente externo, como cabos, impressoras, discos ou sistemas de vídeo, sem conhecimento necessário e/ou uma autorização específica.

XVII. O usuário deve comunicar ao NPD qualquer evidência de violação das normas em vigor, não podendo acobertar, esconder ou ajudar a esconder violações de terceiros, de qualquer natureza.

Art. 3º - As informações importantes e relacionadas às atividades de trabalho na UESPI devem ser armazenadas nos servidores de rede específicos para este fim.

Art. 4º - A cópia de segurança (backup) das informações existentes nas estações de trabalho é responsabilidade de cada usuário.

Art. 5º - O controle de acesso aos recursos de Tecnologia de Informação será de responsabilidade de cada usuário, obedecendo ao seguinte:

I. Os atos e acessos do usuário aos dados e sistemas devem ser realizados através de sua identificação única no ambiente informatizado.

II. É vedada a inclusão de usuários na rede fora do processo normal de inclusão estabelecido pela equipe do NPD.

III. O tamanho de caracteres para formação de senhas não pode ser menor que 6 (seis) caracteres.

IV. Não devem ser utilizadas senhas óbvias, como datas, nomes próprios e siglas.

V. Considerando 4 (quatro) tipos de caracteres (letras minúsculas, letras maiúsculas, números e símbolos), a senha deve ser composta de pelo menos 3 (três) tipos.

VI. É obrigatória a troca de senha no primeiro acesso do usuário.

VII. A troca de senha deve ser de responsabilidade do usuário.

VIII. É proibido o compartilhamento de senhas/usuários e, em caso de suspeita de perda de sigilo, o usuário deve trocar a sua senha.

IX. O usuário será responsabilizado por tentar "quebrar" a segurança do sistema, inclusive com tentativas de descobrir a senha de outros usuários.

X. O perfil de acesso dos usuários aos aplicativos e sistemas será o mínimo necessário para o desempenho de suas atividades.

XI. É proibido o uso de recursos computacionais por usuários desligados da UESPI, os quais terão seus privilégios (conta na rede e em qualquer sistema desta IES, uso de e-mail, acesso à Internet, etc.) imediatamente revogados na data de desligamento.

XII. O usuário deverá respeitar a integridade e limites de sua autorização de acesso ou conta.

XIII. A segurança das contas e das senhas que são atribuídas a um único usuário, não podem ser compartilhadas com mais pessoas sem autorização.

XIV. O usuário deverá informar imediatamente ao NPD qualquer suspeita de tentativa de violação de segurança de recursos computacionais, em qualquer nível.

XV. O usuário não deve permitir ou colaborar com o acesso aos Recursos de Tecnologia de Informação da UESPI por parte de pessoas não autorizadas, sob pena de ser co-responsabilizado pelos eventuais problemas que esses acessos vierem a causar.

Art. 6º - O procedimento de descarte de informações seguirá as seguintes premissas:

I. Devem ser removidos da rede e das estações de trabalho os arquivos que não sejam mais necessários ou não se refiram a assuntos de trabalho.

II. Arquivos com informações estratégicas e/ou confidenciais não devem ser mantidos na Lixeira do Sistema Operacional (Windows, Linux, etc.).

III. Documentos impressos de conteúdo estratégico e/ou confidencial devem ser fragmentados antes de jogados no lixo.

Art. 7º - Quanto ao combate a vírus eletrônico:

I. Todas as estações de trabalho devem possuir *software* antivírus padrão utilizado e autorizado pelo NPD, instalado, configurado, ativado e atualizado, incluindo microcomputadores e *notebooks*.

II. O usuário deve informar imediatamente ao NPD em caso de contaminação do computador por vírus.

Art. 8º - Os sistemas de correio eletrônico (institucional – webmail@uespi.br) e as informações neles contidas são pertencentes à UESPI e disponibilizados aos usuários como uma ferramenta de apoio às atividades do serviço público, seguindo às seguintes orientações:

§ 1º - Ao utilizar os recursos, o usuário deve manter o cuidado de:

I. Utilizar o sistema exclusivamente em prol dos interesses da UESPI;

II. Tratar sua senha como pessoal e intransferível;

III. Identificar suas mensagens com seu nome e endereço eletrônico;

IV. No caso de informações sigilosas enviadas por correio eletrônico para usuários internos, explicitar no cabeçalho ou no corpo da mensagem que se trata de informações confidenciais;

V. Manter o mínimo necessário de mensagens armazenadas na caixa postal.

§ 2º - São inadmissíveis quanto ao uso do correio eletrônico:

I. Criar, transmitir ou armazenar material que caracterize atividade ilegal, ofensiva, discriminatória ou contrária aos interesses da UESPI;

II. Criar, transmitir ou armazenar material que seja atentatória a dignidade da pessoa humana;

III. Transmitir mensagens para pessoas ou sistemas não autorizados;

IV. Criar ou transmitir mensagens prejudiciais à imagem da UESPI;

V. Criar ou transmitir mensagens de caráter pessoal que ofendam a integridade moral dos servidores da UESPI;

VI. Criar, transmitir ou armazenar qualquer tipo de conteúdo malicioso, como vírus e cavalos-de-tróia;

VII. Criar ou transmitir piadas, correntes, material pornográfico, pedófilo, etc;

VIII. Divulgar sua senha;

IX. Utilizar a senha de outra pessoa;

X. Utilizar o sistema para negócios pessoais;

XI. Sobrecarregar o sistema e, neste sentido, o envio de arquivos anexos mensagens, sempre que possível, deve ser evitado;

XII. Violar os padrões de segurança estabelecidos;

XIII. Influenciar comportamento considerado inaceitável.

§ 3º - Responsabilização pelo uso do correio eletrônico:

Parágrafo único - Cada usuário é responsável pelo conteúdo armazenado ou enviado através do correio eletrônico;

Art. 9º - Sobre a privacidade das informações contidas no correio eletrônico:

I. Informações confidenciais não devem ser enviadas pelo correio eletrônico sem alguma forma de proteção contra vazamento e alteração não autorizados;

II. A UESPI reserva para si o direito de monitorar e interferir no tráfego de mensagens, com o propósito de verificar o cumprimento dos padrões de segurança, sempre que julgar necessário e sem aviso prévio.

Art. 10 - O acesso à Internet é disponibilizado a colaboradores, parceiros e estagiários como uma ferramenta de apoio às atividades profissionais e acadêmicas, e o seu uso deve ser restrito e controlado.

§ 1º - O acesso à Internet deve seguir as seguintes orientações:

I. É restrito às atividades relacionadas com as funções administrativas e acadêmicas da UESPI, como por exemplo: comunicação com os campi e fornecedores, pesquisas acadêmicas e obtenção de informações úteis, no sentido de manter os níveis mais altos de produtividade, qualidade e atualização tecnológica;

II. Conduzir adequadamente o uso da Internet, respeitando direitos autorais, regras de licenciamento de *softwares*, direitos de propriedade, privacidade e proteção de propriedade intelectual;

III. A proteção de arquivos contendo dados sensíveis ou sigilosos da UESPI, assim definido pela Política de Segurança, quando transferidos de qualquer forma pela Internet;

IV. O uso da Internet em prol dos interesses da UESPI.

§ 2º - São inadmissíveis quanto ao acesso à Internet:

I. Utilizar a Internet para negócios pessoais;

II. Acessar ou armazenar material indevido e/ou que caracterize atividade ilegal, como pornografia e pirataria;

III. Acessar qualquer tipo de conteúdo malicioso, como vírus e cavalos-de-tróia;

IV. Acessar salas de bate-papo (*chat rooms*), exceto se o acesso for necessário para realização das atividades de trabalho;

V. Usar softwares de comunicação instantânea, como *ICQ, IRC, NetMeeting, Instant Messenger*, etc, exceto se o acesso for necessário para realização das atividades de trabalho;

VI. Sobrecarregar o sistema;

VII. Realizar o *download* de arquivos de interesse pessoal;

VIII. Violar os padrões de segurança estabelecidos;

IX. Influenciar comportamento considerado inaceitável.

X. A UESPI reserva para si o direito de monitorar e interferir no tráfego de acesso a Internet, com o propósito de verificar o cumprimento dos padrões de segurança, sempre que julgar necessário e sem aviso prévio, e para atender os padrões vigentes na Lei de Cibercrime no Brasil PLC 89/2003.

Art. 11 - As penalidades a serem aplicadas às condutas elencadas neste Regulamento, sem prejuízo de outras penas previstas em lei ou em normas da UESPI, são: notificação escrita, redução ou eliminação, temporárias ou permanentes, de *privilégios de acesso, tanto aos Recursos Computacionais, quanto às redes, outros* serviços ou facilidades.

Art. 12 - Esta Norma se aplica a qualquer funcionário (efetivo, provisório, comissionado, terceirizado, estagiário, bolsista.) e se refere a todos os recursos computacionais, controlados individualmente ou compartilhados, isolados ou em rede.

Art. 13 - A Administração Superior desta IES pode definir condições de uso específicas para os recursos sob seu controle, consistentes com a política geral, mas com detalhes, diretrizes e/ou restrições adicionais.

Art. 14 - Cabe à UESPI tratar das violações de restrições adicionais de acordo com as normas internas vigentes e se não houver estes mecanismos específicos, o exposto neste regulamento deve prevalecer.

Art. 15 - No caso do uso de redes externas, as políticas envolvendo este tipo de uso também são aplicáveis e precisam ser adotadas.

Art. 16 - A infração ou tentativa de infração às regras constantes neste Regulamento e demais normas sobre segurança da informação caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil.

Art. 17 - Esta Resolução entrará em vigor na data de sua publicação.

COMUNIQUE-SE, PUBLIQUE – SE E CUMPRA – SE.

Valéria Madeira Martins Ribeiro
Presidente do CONDIR