DECRETO Nº 8.052/2018

DISPÕE SOBRE A HOMOLOGAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI, DO MUNICÍPIO DE ÁGUIA BRANCA-ES E DÁ OUTRAS PROVIDÊNCIAS.

O PREFEITO MUNICIPAL DE AGUIA BRANCA, Estado do Espírito Santo, no uso das atribuições que lhe são conferidas pela Lei Orgânica do Município de Águia Branca, Estado do Espírito Santo,

CONSIDERANDO que a integração dos dados, como a forma de aperfeiçoar e aumentar a qualidade da atividade assistencial aos usuários, bem como democratizar o patrimônio intelectual aqui produzido,

CONSIDERANDO que foi implantado na Prefeitura Municipal de Águia Branca/ES, a estrutura de rede de informações, rede esta idealizada para servir como base a implantação de um robusto sistema de gerenciamento, que irá integrar todas as informações pertinentes ás atividades assistenciais e pesquisa realizadas, todos unificados por meio desse sistema,

CONSIDERANDO O Plano Diretor da Tecnologia da Informação - PDTI,

DECRETA:

Art. 1º - Fica HOMOLOGADA a POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI, na qual tem por objetivo á integração dos dados como forma de aperfeiçoar e aumentar a qualidade das atividades assistenciais aos usuários e a segurança tecnológica desta municipalidade.

Art. 2º - Este Decreto entra em vigor na data de sua publicação.

PUBLIQUE-SE E CUMPRA-SE.

Gabinete do Prefeito Municipal de Águia Branca-ES, 06 de agosto de 2018.

ANGELO ANTÔNIO CORTELETTI
Prefeito Municipal

PREFEITURA MUNICIPAL DE
ÁGUIA BRANCA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI

PREFEITURA MUNICIPAL DE ÁGUIA BRANCA

SECRETARIA DE ADMINISTRAÇÃO – SEMAD

GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO – GTI

ÁGUIA BRANCA – ES

2018

PREFEITURA MUNICIPAL DE ÁGUIA BRANCA
SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO
GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

POLÍTICA INTERNA DE SEGURANÇA DA INFORMAÇÃO

1. INTRODUÇÃO

A Prefeitura Municipal de Águia Branca, visando à integração dos dados como forma de aperfeiçoar e aumentar a qualidade da atividade assistencial aos usuários, bem como democratizar o patrimônio intelectual aqui produzido, implantou a estrutura de rede de informações.

Esta rede foi idealizada para servir como base à implantação de um robusto sistema de gerenciamento, que irá integrar todas as informações pertinentes às atividades assistenciais e de pesquisa aqui realizadas, todos unificados por meio deste sistema, configurando-se, assim, o objetivo principal que embasou a implantação desta estrutura de rede.

Além desta poderosa ferramenta, a rede proporcionaria de imediato, outros recursos, como o acesso a internet e caixas de correio eletrônico (e-mail), cujo intuito maior foi disponibilizar aos servidores e pesquisadores desta unidade central, ferramentas que contribuíssem para o enriquecimento pessoal e intelectual destes usuários, já que é sabido que a Internet é uma fonte riquíssima em informações sobre os mais variados assuntos, e que o correio eletrônico facilitaria a comunicação dos servidores e pesquisadores com outras pessoas das mais longínquas localidades.

Apesar de serem a internet e as caixas de e-mail os recursos diretamente relacionados à estrutura de rede interna mais difundida, é importante salientar que estes não são os únicos recursos oferecidos pela rede, nem os mais importantes.

1.1 A INTERNET E O CORREIO ELETRÔNICO

Com o advento do uso da internet, surgiram problemas diretamente ligados a esta ferramenta.

A análise das diversas formas de sua utilização levou à conclusão de que muitos usuários da Prefeitura Municipal manuseavam de forma indiscriminada, com objetivos extremamente alheios aos preceitos de crescimento individual e intelectual dos indivíduos, acessando sites de conteúdo discordante dos preconizados por esta municipalidade ou tratando a referida ferramenta como mecanismo exclusivo para entretenimento pessoal.

Estas condutas refletiram diretamente na segurança interna dos computadores da PMAB, uma vez que os acessos a tais sites ou o uso de programas específicos tornaram-se a estrutura vulnerável, passível de invasão por "hackers" (piratas da internet), vírus de computador e uma infinidade de outros perigos virtualmente existentes.

Assim, uma verdadeira avalanche de vírus passou a circular nesta rede, os quais, a muito custo, foram eliminados.

Uma vez que não havia qualquer restrição e/ou controle quanto ao acesso a Internet, decidiu-se adotar senhas de acesso.

Com isso, cada setor indicou os servidores que deveriam, por conta da necessidade do serviço do setor, acessar a Internet.

Paralelamente foi implantado um mecanismo que monitora todo o tráfego da rede, informando os sites acessados por cada usuário, dia/mês/ano e horário do acesso, o que permitiu ter uma melhor visão do que era acessado, quando e por quem.

Este recurso permitiu a identificação de computadores infectados por vírus e os usuários que persistiam em acessar sites de conteúdo proibido ou que utilizavam softwares que comprometiam a segurança da rede interna. Deste modo, todo tráfego de internet é permanentemente monitorado.

Fls. nº 004
Processo.
Mat.. Dec. 4436
Ass..

1.2 OS SOFTWARES DE CONVERSAÇÃO INSTANTÂNEA (Lan Messenger Corporativo)

Grande maioria dos equipamentos desta unidade possuía (ou ainda possui) algum software de conversação instantânea instalado.

Softwares de conversação instantânea, ou Google Talk, Messenger são programas que permitem a usuários se comunicarem remotamente (à distância), através de conexão com a Internet. Por meio destes programas, é possível enviar mensagens de texto entre equipamentos fisicamente distantes. Também é possível enviar arquivos ou iniciar sessões de conversação com áudio e/ou com vídeo, em tempo real.

Essa foi uma das formas com que muitos vírus adentraram em nossa rede e permaneceram por muito tempo se replicando freneticamente.

Exemplos de Instant Messengers
mIRC, Scoop Script, Avalanche, Full Throttle, MSN Messenger, Yahoo Messenger, Skype.

1.3 OS COMPARTILHADORES DE ARQUIVOS

Este tipo de software promove um compartilhamento universal de arquivos de todos os formatos, permitindo ainda ao usuário executar o referido arquivo on-line ou baixá-lo em seu computador.

Geralmente era utilizado para baixar músicas no formato MP3, localizar, baixar ou visualizar on-line filmes em DVD, ou encontrar outros softwares e realizar downloads gratuitamente.

O uso deste tipo de software também é altamente nocivo, principalmente pelo fato de que, ao instalá-lo no computador, o usuário dá amplas permissões de leitura e gravação. Ou seja, ao se conectar através do software, o usuário não está somente lendo arquivos de outros computadores, mas também permitindo que outros usuários efetuem uma verdadeira varredura em seu disco rígido. Esta vulnerabilidade também é explorada pelos vírus e/ou por "hackers" que vasculham por redes passíveis de invasão.

Exemplos de Compartilhadores de Arquivos
Full Throttle, Kazaa, Morpheus, Napster, Mp3X

1.4 OS SITES DE CONTEÚDO INAPROPRIADO

O acesso a este tipo de site trouxe uma série de situações de extremo constrangimento, pois a maioria deles tem a capacidade de tornar-se a página inicial do navegador, mesmo sem o consentimento do usuário, e fazer-se exibir automaticamente sempre que o navegador era iniciado.

Mesmo após o trabalho de conscientização realizado junto aos setores no sentido de coibir este tipo de prática foram procedidos ajustes no servidor de modo que não permitisse o acesso a uma série de sites cujo conteúdo vai de encontro aos interesses desta unidade.

1.5 A SEGURANÇA DA INFORMAÇÃO

A segurança é um dos assuntos mais importantes dentre as preocupações de qualquer secretaria municipal.

Confidencialidade, confiabilidade, integridade e disponibilidade da informação estão diretamente ligadas à segurança.

1.5 A SEGURANÇA DA INFORMAÇÃO

A segurança é um dos assuntos mais importantes dentre as preocupações de qualquer secretaria municipal.

Confidencialidade, confiabilidade, integridade e disponibilidade da informação estão diretamente ligadas à segurança.

Segurança da Informação nada mais é que mecanismos que promovam a integridade de uma estrutura de rede na qual trafeguem informações e dados comuns e/ou restritos, e nela incluídos os equipamentos que armazenam tais informações. É tornar estas informações confiáveis e garantir que o seu uso não trará nenhuma consequência danosa tanto para si como para outros usuários.

Temos nesse documento um conjunto de instruções e procedimentos para normatizar, melhorar e disciplinar o uso dos recursos da rede.

2. AUTONOMIA DA GERÊNCIA DE INFORMÁTICA

A Gerência de Tecnologia da Informação tem total autonomia para atuar sobre os equipamentos desta municipalidade, sem prévio aviso, o que concerne aos seguintes tópicos:

- Realização de auditoria (local ou remota)
- A definição de perfis de usuários cujos privilégios não permitam a realização de atividades tidas como nocivas ao sistema operacional ou à rede como um todo;
- A instalação de softwares de monitoramento;
- A desinstalação de quaisquer softwares considerados nocivos à integridade da rede;
- O credenciamento/descredenciamento de usuários;

Não é pertinente à GTI o manuseio de arquivos não executáveis.

3. DIRETRIZES QUANTO AO USO DA INTERNET

A internet deve ser utilizada para fins de complemento às atividades do setor, para o enriquecimento intelectual de seus servidores ou, no caso dos pesquisadores, como ferramenta para busca por informações que venham contribuir para o desenvolvimento de seus trabalhos.

Jamais devem ser utilizados para a realização de trabalhos de terceiros ou de atividades paralelas.

O uso para fins pessoais, como a consulta a movimento bancário ou acesso a e-mail pessoal, deve ser realizado fora do horário de expediente, e com o consentimento do chefe ou responsável pelo setor.

3.1 A REALIZAÇÃO DE DOWNLOADS

O processo de realização de downloads exige boa parte da banda de navegação do servidor e, quando realizado em demasia, congestiona o tráfego e torna a navegação para os demais usuários inviável.

Downloads muito grandes podem congestionar o fluxo de tráfego e comprometer sistemas que funcionam on-line.

3.2 EXECUÇÃO DE JOGOS E RÁDIOS ON-LINE

Uma vez que não existe qualquer pertinência com as finalidades institucionais propostas por esta unidade central, é terminantemente proibida a execução de jogos, músicas ou rádios on-line, visto que esta prática toma toda a banda de navegação de internet, dificultando a execução de outros serviços que necessitam deste recurso.

3.3 SENHAS DE ACESSO

Somente poderão acessar a Internet usuários que tenham sido credenciados com suas senhas de acesso.

Cada setor deverá, através de memorando, indicar novos servidores que deverão ser credenciados para tal serviço, justificando quanto à necessidade do referido funcionário utilizar-se deste recurso.

A senha de acesso tem caráter pessoal, e é intransferível, cabendo ao seu titular total responsabilidade quanto seu sigilo.

A prática de compartilhamento de senhas de acesso é terminantemente proibida e o titular que fornecer sua senha a outrem responderá pelas infrações por este cometidas, estando passível das penalidades aqui previstas.

Caso o usuário desconfie que sua senha não seja mais segura, ou de seu domínio exclusivo, poderá solicitar à Gerência de Informática a alteração desta.

3.4 RECOMENDAÇÕES SOBRE O USO DO CORREIO ELETRÔNICO (E-MAIL)

- Não abrir anexos com as extensões .bat, .exe, .src, .lnk e .com, ou de quaisquer outros formatos alertados pela Gerência de Informática, se não tiver certeza absoluta de que solicitou esse e-mail

- Desconfiar de todos os e-mails com assuntos estranhos e/ou em inglês. Alguns dos vírus mais terríveis dos últimos anos tinham assuntos como: ILOVEYOU, Branca de neve pornô, Ramsomware, etc.·.
- Não reenviar e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/Symantec/Bancos, criança desaparecida, criança doente, pague menos em alguma coisa, não pague alguma coisa, etc.·.
- Não utilizar o e-mail da empresa para assuntos pessoais;
- Evitar enviar anexos muito grandes;

- Após 3 (três) tentativas de acesso à caixa de e-mail com senha ou nome de usuário incorreto, o referido e-mail é automaticamente bloqueado. Caso isto ocorra, o usuário deve entrar em contato com a Gerência de Informática e relatar o acontecido, solicitando o desbloqueio.

- Adotar o hábito de ler sua caixa de e-mails diariamente (pela manhã e à tarde), de modo a evitar que se acumulem os e-mails. E-mails a serem lidos em demasia lidos congestionar o navegador e fazer com que o sistema não responda. Com isso, novas mensagens não serão recebidas até que as anteriores sejam baixadas por completo.

- Utilizar o e-mail para comunicações oficiais internas, as quais não necessitem obrigatoriamente do meio físico escrito. Isto diminui custo com impressão e aumenta a agilidade na entrega e leitura do documento.

Fls. nº 007
Processo.
Mat.. Dec. 7726/18
Ass:..

5. A INSTALAÇÃO DE SOFTWARES

Qualquer software que, por necessidade do serviço daquele setor, necessitar ser instalado, deverá ser comunicado com antecedência à Gerência de Informática.

Fica permanentemente proibida a instalação de quaisquer softwares não freeware sem licença de uso.

A Gerência de Informática poderá valer-se da autonomia citada no item 2 deste instrumento para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à Lei 9.609/98 (Lei do Software).

6. PENALIDADES

O usuário que infringir qualquer uma das diretrizes de segurança expostas neste instrumento estará passível das seguintes penalidades (sem prévio aviso):

- Descredenciamento da senha de acesso a Internet;
- Cancelamento da caixa de e-mail;
- Desativação do ponto de rede do setor;

O(s) usuário(s) infrator poderá ser notificado e a ocorrência da transgressão imediatamente comunicada ao seu chefe imediato.

A Gerência de Informática poderá valer-se da autonomia de gestora da informação para deliberar privilégios a quaisquer usuários desta municipalidade, ou indeferi-los.

7. MEMBROS DA EQUIPE DE SEGURANÇA

Os servidores abaixo qualificados estão diretamente responsáveis pela implantação e implementação da presente política, devendo reportar-se a eles todo e qualquer usuário e/ou setor para tratar de assuntos pertinentes à segurança da informação de que trata este instrumento.

Joathan Pimenta Pereira – jppereira@prefeituradeaguiabranca.es.gov.br
Gabriel Faria Scardini – gfscardini@prefeituradeaguiabranca.es.gov.br

8. VIGÊNCIA E VALIDADE

A presente política passa a vigorar a partir da data de sua homologação e publicação como Portaria Interna da Prefeitura Municipal de Águia Branca sendo válida por tempo indeterminado.

Águia Branca/ES, 27 de Julho de 2018.

Angelo Antonio Corteletti
Prefeito Municipal

Liliane Monfardini de Almeida Bressanelli
Secretária de Administração

Joathan Pimenta Pereira
Analista de Informática

Joathan Pimenta Pereira
Analista de Informática
Gerência de Tecnologia da Informação
Matrícula: 64539

Hadeon Falcão
Controlador Municipal