Política de Segurança da Informação

SUMÁRIO

Introdução.....3
Normas de Segurança da Informação no Perímetro Interno do CREMEGO.....3
Compete a Coordenação de Redes/Suporte e Sistemas.....4
Normas de uso de chaves de acesso para Usuários.....4
Formação de Contas e Senhas.....4
Concessão da chave de acesso.....5
Tempo de vida de Contas e Senhas.....5
Uso de dispositivos externos.....5
Disposições Gerais.....5
Diretrizes quanto ao uso da internet.....6
Norma para utilização da internet.....6
Orientações.....8
Realização de Downloads.....8
Execução de jogos e rádios On-Line.....8
Senhas de Acesso.....9
Utilização do Correio Eletrônico.....9
Regras para o uso do Correio Eletrônico (e-mail).....10
Regras para criação de e-mails e listas de discussão de e-mails.....10
Normas para Armazenamento de Arquivos.....11
Direitos e deveres dos usuários.....12
Disposições Finais.....13
Penalidades.....13
Vigência e Validade.....13
Legislação.....14
Glossário:.....15

Introdução

Com o crescente aumento do uso da Internet, surgem preocupações diretamente ligadas aos dados ou informações de uma Instituição, assim, com o avanço dessa ferramenta em suas diversas formas de utilização, faz-se necessário uma Política que defina as diretrizes para a Segurança da Informação, para garantir a integridade, confidencialidade e disponibilidade das informações sob responsabilidade de uma Instituição.

Uma Política de Segurança descreve a conduta adequada para o manuseio, controle e proteção das informações, contra destruição, modificação, divulgação indevida e acessos não autorizados, sejam acidentalmente ou intencionalmente.

Esta Política se aplica às informações sob responsabilidade do Conselho Regional de Medicina do Estado de Goiás – CREMEGO, em qualquer forma ou meio que a informação seja apresentada ou compartilhada, que deverão estar sempre protegidas adequadamente, de acordo com controles definidos nesta política.

Estas Normas devem ser divulgadas para todos os funcionários da instituição e obedecidas por todos que utilizam os recursos de arquivamento, de disponibilidade, de consultas às informações disponibilizadas e armazenadas pelo Departamento de Informática, sendo de responsabilidade de cada um o seu cumprimento.

O cumprimento desta Política de Segurança será acompanhado e auditado pelo setor de Informática do CREMEGO. A instituição, mediante autorização expressa da alta direção, se reserva o direito de monitorar, automaticamente, a estação de trabalho, o tráfego efetuado através das redes de comunicação, incluindo o acesso à Internet e o uso do Correio Eletrônico.

A não observância dos preceitos desta Política implicará na aplicação de sanções administrativas.

Este documento será revisado a qualquer momento quando a segurança da rede assim o exigir.

Normas de Segurança da Informação no Perímetro Interno do CREMEGO

A segurança é um dos assuntos mais importantes dentre as preocupações de qualquer entidade: confidencialidade, integridade e disponibilidade da informação estão diretamente ligadas à segurança.

A Segurança da Informação são mecanismos que promovem a integridade de uma estrutura de rede na qual trafeguem informações e dados comuns e/ou restritos, incluídos os equipamentos que armazenam tais informações, bem como tornar estas informações confiáveis e garantir que o seu uso não trará nenhuma consequência danosa tanto para si como para outros funcionários.

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

Compete a Coordenação de Redes/Suporte e Sistemas

A Coordenação de Redes/Suporte/Sistemas tem atribuição para atuar sobre os equipamentos deste Conselho, com prévio aviso e autorização do Coordenador de Setor, o que concerne aos seguintes tópicos:

a) Realização de auditoria (local ou remota);
b) A instalação de softwares de monitoramento;
c) Com autonomia, o que concerne aos seguintes tópicos:
   - 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 desinstalação de quaisquer softwares considerados nocivos à integridade da rede;
   - O credenciamento/descredenciamento de usuários.

Normas de uso de chaves de acesso para Usuários

Esta norma tem como objetivo estabelecer os procedimentos adequados para a correta utilização das chaves de acesso no ambiente de Tecnologia da Informação do CREMEGO.

Esta deverá ser aplicada a todos os funcionários/estagiários que possuam chave de acesso (sem privilégios de "administrador") nos ativos do tipo estações de trabalho e servidores do ambiente de tecnologia da Informação do CREMEGO.

A identificação do funcionário/estagiário por senha ou outro meio é pessoal e intransferível, qualificando-o como responsável por todas as atividades desenvolvidas através dela, sendo pré-requisito para a liberação do uso o preenchimento do **RQ. 02 Termo de Compromisso de Confidencialidade de Informações e Proteção de Dados Pessoais e Sensíveis**, fornecido pelo Setor de Recursos Humanos do CREMEGO.

Formação de Contas e Senhas

a) As senhas para usuários deverão conter no mínimo 8 (oito) caracteres, sendo obrigatório o uso de letras e números. Como recomendação, sugere-se a utilização de maiúsculas, minúsculas e caracteres especiais ("$", "%","&");

b) Os sistemas e aplicações deverão prover algum mecanismo ou instrução que garanta que só sejam aceitas senhas com a formação acima citada;

c) Deverá ser evitada a composição de senhas com somente sequência numéricas (123...) e/ou alfabéticas (abc...), além de senhas de fácil dedução (nome da máquina, nome do usuário e data de nascimento e outros).

Concessão da chave de acesso

A chave de acesso é composta de uma conta (login) e uma senha. Para a definição do login é adotado a seguinte nomenclatura: primeira letra do sobrenome + o primeiro nome do usuário. Ex: Maria Ferreira Cardoso. Login: cmaria

A criação de conta deve ser solicitada pelo Coordenador do setor, que encaminhará para o e-mail informatica@cremego.org.br com os dados do funcionário.

Tempo de vida de Contas e Senhas

- O usuário deverá ser forçado a trocar a senha no seu primeiro login;
- A conta deverá ser bloqueada após a terceira tentativa sem sucesso de login;
- O tempo de vida das senhas deverá ser de, no máximo, 90 dias, quando deverá ser forçada a sua troca no primeiro login após esse período;
- Contas que ficarem inativas por mais de 60 dias serão bloqueadas automaticamente.

Uso de dispositivos externos

- É vedado aos usuários utilizarem as mídias removíveis tais como: Hds externos, pendrivers e carregar de celulares via porta USB nos computadores do CREMEGO, caso necessário realizar o trabalho, deverá procurar o coordenador de cada departamento ou Departamento de Informática para realizar checagem de vírus antes de sua utilização.

Disposições Gerais

- A chave de acesso é pessoal e intransferível, devendo ser mantida em sigilo. O usuário será responsabilizado pelo mau uso da chave de acesso;
- Os sistemas e aplicações deverão ter algum mecanismo que impeça a exibição na tela da chave do usuário;
- O Coordenador de Setor deverá comunicar ao Setor de Tecnologia da Informação acerca dos funcionários/estagiários que forem desligados do CREMEGO, para que a chave de acesso seja cancelada e a conta de e-mail encerrada;
- Deve-se atribuir as contas de usuário, somente os privilégios necessários à execução de sua atividade;
- Os usuários não terão contas com perfil administrador, nem contas do domínio com privilégio de administrador local da estação, exceto àquela cuja atividade funcional necessite de tal requisito. Para isto, deverá ser solicitada a chefia do setor com justificativa, que será avaliada pela administração da rede/sistemas e da segurança de informação.
- Os acessos e as falhas nas tentativas de logon deverão ser auditados;

- A eventual necessidade de instalação de softwares deve ser submetida por abertura de chamado, por e-mail ou por telefone, ao Setor de Tecnologia da Informação, à administração de rede e da segurança, para que haja um controle centralizado de softwares e licenças disponíveis para o Órgão;
- O Funcionário é pessoalmente responsável por todas as atividades realizadas por intermédio de sua chave de acesso.

Diretrizes quanto ao uso da internet

Esta norma tem como objetivo estabelecer responsabilidade e requisitos básicos de utilização da Internet nos setores do CREMEGO.

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

Com base nos procedimentos de proteção e integridade dos sistemas de informação, a Internet é classificada como conexão de alto risco. Os funcionários devem estar cientes da periculosidade da navegação na Internet, antes de acessá-la e de utilizar os seus recursos.

Considerando que o uso da Internet é fundamental para as atividades desenvolvidas no CREMEGO e observando-a como ferramenta que possibilita ameaças às informações da Instituição são de extrema importância que se estabeleça um conjunto de regras que possibilitem a utilização adequada desse importante recurso tecnológico.

Norma para utilização da internet

Todos os funcionários/estagiários do CREMEGO, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse do órgão, mantendo uma conduta profissional, especialmente em se tratando da utilização de bem público.

a) O CREMEGO possui mecanismos de autenticação, que determinam a titularidade de todos os acesos à Internet feita por seus funcionários;
b) É expressamente proibida a divulgação e/ou compartilhamento indevido de informações sigilosas em listas de discussão ou bate-papo;
c) O acesso à Internet por parte dos funcionários do CREMEGO deve ser feito exclusivamente por meio da única ligação existente entre a Internet e o Conselho, sendo vedado o acesso provedores de acesso privados para o acesso à rede mundial de computadores;
d) A privacidade no acesso à Internet é garantida, mas os endereços acessados serão registrados e o conteúdo das informações trafegadas por meio eletrônico poderá ser rastreado, registrado e/ou eliminado de forma automática, por softwares especiais, em busca de termos ou assuntos que se insiram no grupo de temas cujo acesso ou tráfego é proibido;
e) É vedado o acesso aos sites da Internet com conteúdo pornográfico ou ofensivo aos direitos humanos;

f) Todos os acessos à Internet serão passíveis de monitoração e identificação, sendo tais acessos arquivados e mantidos disponíveis para cálculos estatísticos, bem como eventuais auditorias;

g) Haverá geração de relatórios gerenciais dos sites acessados por funcionários num determinado período. A Diretoria poderá ter acesso a essas informações a qualquer tempo;

h) É vedada invasão de computadores alheios para obtenção de senhas e informações pessoais;

i) É vedada a utilização da banda de Internet para baixar músicas de qualquer tipo ou ouvir rádio pela Internet;

j) Qualquer usuário a quem se tenha dado o direito de se conectar à rede deve fazê-lo para uso exclusivo a serviço. É proibido fazer download de qualquer arquivo ou programa que não sejam de domínio público ou que não sejam apropriados para uso em serviço;

k) Utilizar falsa identidade ou Organização (domínio), de forma intencional;

l) O funcionário será responsável pelo uso dos serviços providos pelo CREMEGO para acesso à rede mundial - Internet, em observância a todas as leis, decretos e regulamentos nacionais, estaduais, e municipais aplicáveis de acordo com estas normas, bem como com a ordem pública;

m) O funcionário não poderá transmitir, difundir ou disponibilizar a terceiros informações, dados, conteúdos, mensagens, gráficos, desenhos, arquivos e som e/ou imagens, fotografias, gravações, software e, em geral qualquer classe de material que:

   i. De qualquer forma contrariem, menosprezem ou atentem contra os direitos fundamentais e as liberdades públicas reconhecidas constitucionalmente, nos tratados internacionais e no ordenamento jurídico como um todo;

   ii. Induzam, incitem ou promovam atos ilegais, denegridores, difamatórios, infames, violentos, terroristas ou, em geral contrários à lei;

   iii. Transgridam os segredos empresariais de terceiros;

   iv. Constituam publicidade de qualquer natureza ou conteúdo;

   v. Incorporem vírus ou outros elementos físicos ou eletrônicos que possam causar dano ou impedir o normal funcionamento da rede, do sistema ou de equipamentos informáticos (hardware e software) do CREMEGO ou de terceiros, ou que possam causar dano aos documentos eletrônicos e arquivos armazenados nestes equipamentos informáticos;

   vi. Provoquem, por suas características (tais como forma, extensão, etc.) dificuldades no normal funcionamento da rede local do CREMEGO, bem como da rede mundial Internet;

n) Não é permitida a utilização de software do tipo peer-to-peer (P2P), tais como Kazaa, Emule e afins;

o) Qualquer violação a esses direitos pelo servidor ou por terceiro utilizando-se de sua senha pessoal será de responsabilidade do funcionário, implicando a adoção das medidas legais aplicáveis, eximindo-se o CREMEGO de qualquer responsabilidade advinda de tal infração;

p) É de responsabilidade de cada funcionário zelar pelo fiel cumprimento ao estabelecido na presente norma;

q) Haverá geração de relatórios gerenciais dos sites acessados por usuários num determinado período. A Diretoria poderá ter acesso a essas informações a qualquer tempo;

r) O Usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de sua chave de acesso, salvo se comprovadamente tenha havido quebra da sua senha de segurança;

s) A não observância de qualquer item acima implicará nas sanções e penalidades legais, sem prejuízo de perdas e danos que der causa, inclusive as de ordem moral, bem como as de responsabilidade civil e criminal respectivas, conforme previsto no Regulamento de Pessoal do CREMEGO.

Orientações

O esquema de bloqueio de sites é baseado em sistemas automatizado, no entanto algumas páginas poderão ser bloqueadas indevidamente. Caso seja bloqueado um site cujo conteúdo esteja de acordo com esta norma, o funcionário pode solicitar o desbloqueio através do e-mail informatica@cremego.org.br, bastando informar na mensagem qual a URL bloqueada.

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, compromete sistemas que funcionam on-line e torna as navegações para os demais funcionários inviáveis.

Como o Conselho já possui um sistema que realiza naturalmente *downloads* constantes atualizações dos softwares, a tarefa de *downloads* deve ser vista com muito cuidado e sua realização feita somente em casos de extrema necessidade.

Portando o funcionário que utilizar-se da infraestrutura interna do CREMEGO para efetuar *downloads* de arquivos pessoais de documentos desnecessários poderá ter seus *downloads* monitorados e encaminhados a chefias e se necessário à diretoria.

Execução de jogos e rádios On-Line

Uma vez que não existem quaisquer pertinências com as finalidades institucionais propostas pelo CREMEGO, é terminantemente proibida a execução de músicas, jogos, vídeos ou rádios *on-line*, visto que esta prática toma parte da banda de navegação de internet, dificultando a execução de outros serviços do CREMEGO que necessitam deste recurso, porém, a liberação de alguns serviços específicos de vídeos ou rádio, necessário as atividades da Instituição, deverão ser liberados através de autorização do coordenador(a) de departamento e ou Superintendência.

Senhas de Acesso

Somente poderão acessar a Internet funcionários e estagiários que tenham autorização do coordenador(a) para esse fim.

A Coordenação de Setor deverá, através de memorando ou e-mail, indicar novos servidores que deverão ser credenciados para tal serviço, justificando quanto à necessidade do referido funcionário a utilizar este recurso, bem como solicitar a remoção de *login* de funcionários do respectivo setor que forem desligados do quadro de pessoal do CREMEGO.

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 estas cometidas e implicará nas sanções previstas no Regulamento de Pessoal do CREMEGO, que aprova os instrumentos de gestão de recursos humanos.

Utilização do Correio Eletrônico

Estabelecer responsabilidades e requisitos básicos de uso dos serviços de correio eletrônico, no ambiente de Tecnologia da Informação do CREMEGO.

Prover a comunicação é, sem dúvida, a essências das redes. As pessoas procuram se corresponder de maneira mais rápida e fácil possível. O correio eletrônico (e-mail) é uma das aplicações que ilustra esta procura. Entretanto, a funcionalidade de correio eletrônico fornecida pelo CREMEGO deve ser utilizada no interesse do serviço.

a) O acesso a mensagens de correio eletrônico é de exclusividade do funcionário detentor do endereço eletrônico, sendo garantida a inviolabilidade do conteúdo das mensagens eletrônicas, ressalvando com prévio aviso e autorização da Diretoria para a realização de auditorias;
b) Os funcionários do CREMEGO poderão ser titulares de uma única caixa postal individual no Servidor de Correio Eletrônico, com direitos de envio/recebimento de mensagens, via internet, enquanto perdurar o seu vínculo com o CREMEGO;
c) O usuário deve ter o máximo de certeza de que a mensagem enviada não seja considerada abusiva, obscena, ofensiva, rude ou preconceituosa;
d) É vedado o uso de e-mail para propaganda política, racial, financeira ou de qualquer outra natureza, pois fere o item do CONFLITO DE INTERESSES;
e) É vedado o uso de material pornográfico entre os e-mails da organização, tanto recebimento como envio;
f) É vedado o uso de e-mail para difamação ou calúnia de qualquer pessoa física ou jurídica, sendo usuários: Funcionários, Colaboradores (Representantes da Organização, Fornecedores ou Concorrentes, Terceirizados);

g) Verificar diariamente sua caixa de mensagens, excluindo aquelas cujo armazenamento não mais se faça necessário;

h) Limitar o acesso às informações (arquivo, diretórios, correio eletrônico, etc.) de sua responsabilidade somente às pessoas e usuários autorizados;

i) É vedado a instalação e utilização de sistema de correio eletrônico diferente do disponibilizado, pelo órgão nas estações de trabalho, inclusive aqueles disponíveis na Internet;

j) O funcionário ou terceiros prejudicados pela recepção de mensagens não solicitadas dirigidas a uma pluralidade de pessoas deverão comunicar o fato ao Setor de Tecnologia da Informação, a quem caberá efetuar diligências com o intuito de apurar os responsáveis, após comunicado e autorizado pela Presidente/Diretoria.

Regras para o uso do Correio Eletrônico (e-mail)

a) Não abrir anexos com as extensões .bat, .exe, .src, .lnk e .com, ou de quaisquer outros formatos alertados pelo setor de Tecnologia da Informação, se não tiver certeza absoluta de que solicitou esse e-mail;

b) Não reenviar e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/AOL/Symantec, criança desaparecida, criança doente, pague menos em alguma coisa, não pague alguma coisa, etc;

c) Não utilizar o e-mail da empresa para assuntos pessoais;

d) O envio/recebimento de mensagens para/da Internet, por meio de correio eletrônico, fica limitado a mensagens com no máximo, 15 (quinze) Mbytes, caso tenho necessidade de enviar um arquivo maior deverá comunicar ao Departamento de TI para alternativa viável;

e) 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 ou enviados em demasia congestionar o navegador e faz com que o sistema não responda. Com isso, novas mensagens podem não ser recebidas até que as anteriores sejam baixadas por completo;

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

g) É vedada a utilização do correio eletrônico para veicular mensagens do tipo SPAM (e-mails em massa), exceto, com autorização da Diretoria, através do servidor de e-mail institucional para divulgação de atividade relacionadas aos serviços do Conselho.

Regras para criação de e-mails e listas de discussão de e-mails

O serviço de e-mails do CREMEGO será administrado pela Administração da Rede e Segurança em Tecnologia da Informação deste órgão que seguirá as normas abaixo:

a) A criação, alteração ou remoção de e-mail institucional será efetuada a partir de solicitação por memorando ou e-mail encaminhado pelos coordenadores de setores do CREMEGO;
b) A criação de grupos de discussão, no servidor de e-mail, a inscrição, remoção de e-mails nos grupos será executada a partir de solicitação por memorando ou e-mail encaminhado pelos coordenadores de setores do CREMEGO;
c) Os e-mails criados terão cota de armazenamento de tamanho fixo, de acordo com os procedimentos internos do setor de Tecnologia da Informação;
d) Os e-mails que passarem de seis (06) meses sem serem utilizados serão removidos do servidor;
e) Os funcionários deverão administrar sua caixa postal semanalmente: removendo mensagens desnecessárias para evitar que caixa de entrada fiquei cheia.

Normas para Armazenamento de Arquivos

Regras e requisitos básicos aplicados aos ativos de informação para armazenamento de arquivos no setor de Tecnologia da Informação do CREMEGO.

a) Os arquivos da rede do CREMEGO estão disponibilizados em unidades mapeadas na própria máquina do usuário, da maneira que se segue:
   i. Pasta da Setor mapeada – é uma área do disco rígido de um dos servidores, que disponibiliza para os usuários as pastas e documentos relativos ao setor onde trabalha. É feito backup (cópia de segurança) diário destes arquivos, possibilitando ao usuário a recuperação dos mesmos em caso de perda acidental; esta pasta não deverá ser utilizada, em hipótese alguma, para gravação de arquivos particulares de qualquer tipo, arquivos de instalação ou quaisquer outros que não sejam os de trabalho.
      1. Fica proibido salvar arquivos ou pastas com nomes de usuários ou pessoas na pasta de trabalho do Setor.
      2. Compete ao setor de Informática a realização de backup (cópia de segurança) diário do conteúdo desta pasta.
      3. Os arquivos que estiverem em desacordo com o exposto acima poderão ser apagados (excluídos) ou postos em quarentena sem prévio aviso aos usuários.
b) Meus Documentos – É uma unidade específica para que cada usuário guarde suas informações particulares que não serão vistas ou alteradas por outros usuários, exceto quando da realização de auditoria determinada e fundamentada pela Administração. A pasta Meus Documentos não deverá ser usada para gravação de arquivos de trabalho. Não é feito backup (cópia de segurança) destes arquivos, impossibilitando ao usuário a recuperação dos mesmos em caso de perda acidental ou formatação da máquina;
c) É proibido o uso da área de trabalho do sistema operacional em uso no CREMEGO para armazenamento de dados, ficando ao Setor de Informática isenta de responsabilidade em caso da perda de informações ali contidas;
d) É proibido o uso do drive C: (disco local) para a guarda de arquivos pessoais ou de trabalho, devendo os mesmos ser salvos nos locais já mencionados nos itens anteriores;

e) Para a recuperação de pastas ou arquivos excluídos ou antigos o autor ou representante deverá solicitar via e-mail ou memorando informando o máximo de detalhamento possível, para a localização e identificação do arquivo ou pasta excluída;

f) Evitar o armazenamento na rede de arquivos de instalação, imagens e arquivos sem uso. Tal procedimento sobrecarrega os discos dos servidores, tornando sua utilização mais lenta;

g) O funcionário do Departamento de Tecnologia da Informação não fará backup de máquina de usuário, por solicitação deste ou caso necessite formatar o disco rígido da estação de trabalho.

Direitos e deveres dos usuários

a) Proibida ludibriar a segurança dos recursos computacionais, sistemas ou softwares;

b) Fica permanentemente proibida a instalação de quaisquer softwares não-freeware sem licença de uso;

c) A gerência de rede e segurança poderá valer-se da autonomia citada no item 2.1 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);

d) Utilizar sistemas ou softwares ilegais ou não autorizados;

e) Conectar redes e computadores que não os previstos pelo Departamento de TI;

f) São de responsabilidade do usuário acionamento e o desligamento dos equipamentos de informática, pertencentes à mesma, no início e término de cada expediente;

g) Ao usuário não é permitido instalar programas de qualquer natureza nos microcomputadores. Qualquer necessidade de aplicativos deverá ser solicitada ao Setor de Informática;

h) É proibido o remanejamento e a remoção de qualquer equipamento de informática sem aviso prévio ao Departamento de TI;

i) É vedada a manipulação dos equipamentos de rede (switches, hubs, fiação, cabeamento de rede, entre outros) por pessoal não pertencente ao Departamento de TI;

j) Uma vez que cabe a administração autorizar qualquer tipo de compra referente à informática (Software ou Hardware), caberá ao Departamento de TI em conjunto com Setor Interessado elaborar o termo de referência acerca dos assuntos de compra ou contratação de serviço;

k) O Setor de Informática se desobriga a dar suporte a software ou hardware que não tenha sido adquirido por seu intermédio ou com seu parecer;

l) Não conectar ou desconectar nenhum periférico sem a devida autorização do Departamento de TI. Tal procedimento pode danificar o mesmo, exceto pen drivers e equipamento plug & play;

m) É terminantemente proibido ao usuário o acesso ou manutenção no interior do gabinete do computador, assim como troca ou retirada de componentes do mesmo. Caso necessário deverá ser acionado Departamento de TI;

n) A Administração e Segurança da Rede não possuem rotina de backup para estações de trabalho, ou seja, todo material institucional produzido e/ou alterado deverá ser gravado, necessariamente, no servidor de arquivo;

o) Utilizar apenas os softwares autorizados, que forem legalmente adquiridos e instalados pelo Departamento de TI. É terminantemente proibida a utilização de cópias ilegais de software nos

computadores do CREMEGO, bem como a solicitação de cópias de softwares legalmente adquiridos pelo CREMEGO para uso particular;

p) Não é permitido cópia de softwares pertencentes ao CREMEGO;

Disposições Finais

Conforme o item 01 das diretrizes gerais da Política de Segurança da Informação do CREMEGO, esse se reserva no direito de monitorar o tráfego através das suas redes de comunicação, incluindo o acesso à Internet.

A monitoração do cumprimento das normas de utilização da Internet será executada, após autorização da Administração conforme os itens abaixo:

a) Técnicos do setor de Rede e Segurança da Informação identificarão os usuários que descumprirem qualquer item desta norma de segurança;
b) O CREMEGO se reserva no direito de verificar, sempre que julgar necessário, a obediência às normas ou procedimento citados neste documento;
c) O uso indevido dos serviços de correio Eletrônico, tratados neste documento, é passível de sanção disciplinar, de acordo com a legislação vigente e demais normas aplicadas à matéria;
d) Será de responsabilidade de cada usuário zelar pelo fiel cumprimento ao estabelecido na presença norma, devendo também assinar o **RQ. 02 Termo de Compromisso de Confidencialidade de Informações e Proteção de Dados Pessoais e Sensíveis**;
e) O usuário arcará pelos danos causados pelo mau uso dos computadores e dos recursos do CREMEGO, mediante apuração cabível, nos termos da lei;
f) As transgressões serão tratadas conforme regras do **Regulamento de Pessoal do CREMEGO**.

Penalidades

O funcionário que apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, arquivo ou programa de computador, de forma indevida ou não autorizada, fizer uso indevido dos equipamentos de informática, bem como praticar ato em desacordo com os termos da presente norma fica sujeita as punições cabíveis nas consolidações das leis trabalhistas, desde que autorizada fundamentadamente a abertura do processo pela administração.

O(s) funcionário(s) infrator poderá ser notificado e a ocorrência da transgressão imediatamente comunicada ao seu chefe imediato, à diretoria correspondente e à Presidência.

Todos os funcionários ao tomarem conhecimento de qualquer incidente de segurança da informação devem informar o ocorrido, imediatamente, ao Departamento de TI pelo e-mail (informatica@cremego.org.br).

Vigência e Validade

A presente política passa a vigorar a partir da data de sua homologação pela Diretoria do CREMEGO sendo válida por tempo indeterminado.

Legislação

- Lei Federal nº 8159 de 08 de janeiro de 1991 (Dispõem sobre a Política Nacional de Arquivos Públicos e Privados);
- Lei Federal nº 9279 de 14 de maio de 1996 (Dispõe sobre Marcas de Patentes);
- Lei Federal nº 9610 de 19 de fevereiro de 1998 (Dispõe sobre o Direito Autoral);
- Decreto nº 3505 de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal;
- Lei Federal nº 10.406 de 10 de janeiro de 2002 (Institui o Código Civil);
- Decreto nº 4453, de 27 de dezembro de 2002 (Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado no âmbito da Administração Pública Federa). • Portaria n.º 37, de 14 de agosto de 2009;

Obs.: Conforme a necessidade e as medidas para minimizar e combater ocorrências, outras legislações poderão ser aplicadas à matéria, conforme as legislações do país.

REGES PAULO DE MOURA COSTA:50876546149

Assinado de forma digital por REGES PAULO DE MOURA COSTA:50876546149
Dados: 2022.04.05 09:04:23 -03'00'

Coordenador da Divisão de Sistemas

MARCO AURELIO FERREIRA FELIX:89606051153

Assinado de forma digital por MARCO AURELIO FERREIRA FELIX:89606051153
Dados: 2022.01.31 15:51:08 -03'00'

Coordenador da Divisão de Redes

Glossário:

Ativo. Tudo que tem valor para a organização.

Arquivos infectados. Aqueles que sofreram a ação de vírus eletrônico.

Caixa Postal / Correio eletrônico. Espaço em disco, onde são armazenadas as mensagens de correio eletrônico.

Criptografia. Ciência que consiste na codificação e decodificação de mensagens, de forma a garantir a segurança e o sigilo no envio de informações.

Controle. Forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.

Chave de Aceso. Código de aceso atribuído a cada usuário. Para cada chave de acesso é associada uma senha individual e intransferível, destinada a identificar o usuário, permitindo-o acessar os recursos disponíveis.

Download. baixar um arquivo ou documento de outro computador, através da Internet.

Ferramenta Tecnológica. Sistema (conjunto de programas) e/ou equipamento destinado a proteger, monitorar ou agregar valor aos ativos de informações.

E-mail. Mensagem eletrônica.

FTP. (*File Tranfer Protocol*) protocolo para envio e recebimento de arquivos.

IMAP. (*Intenet Message Acess Protocol*) protocolo de acesso a mensagens eletrônicas.

Internet. Associação mundial de redes de computadores.

Intranet. Rede Interna, de uso corporativo, que utiliza a mesma tecnologia da Internet, para que os funcionários possam acessar as informações dos seus respectivos órgãos.

IP. (*Internet Protocol)* protocolo que permite a comunicação entre máquinas em uma rede.

Peer-To-Peer. (P2P) é um tipo de programa que permite a distribuição de arquivos a outros usuários através da Internet.

Política de Segurança da Informação. documentos que provêm uma orientação e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

POP. (*Post Office Protocol*) protocolo usado por clientes de correio eletrônico para manipulação de arquivos de mensagens em servidores de correio eletrônico.

Rede. meio digital de transmissão de informação.

Servidor de Correio Eletrônico. Equipamento que prove o serviço de envio e recebimento de mensagens de correio eletrônico.

Sistemas Informatizados. Sistema constituído de programas e/ou equipamentos computacionais.

Software. programa de computador.

SMTP. (*Simple Mail Tranfer Protocol*) protocolo de comunicação usado para troca de mensagens na Internet, via correio eletrônico.

Spam. Qualquer mensagem, independentemente de seu conteúdo, enviada para vários destinatários, sem que os mesmo a tenha solicitado.

MARCO AURELIO FERREIRA FELIX:89606051153
Assinado de forma digital por MARCO AURELIO FERREIRA FELIX:89606051153
Dados: 2022.01.31 15:39:12 -03'00'