CONASS
Conselho Nacional de Secretários de Saúde

Regulamento sobre Gestão de Tecnologia e Informação

Seção I
Das Disposições Preliminares

Art. 1º - Este regulamento visa definir os requisitos básicos necessários ao acesso e manipulação dos ativos de informação e de processamento do Conselho Nacional dos Secretários de Saúde – CONASS, sendo parte integrante da Política de Segurança da Informação.

Art. 2º - Seu conhecimento deve ter abrangência ampla e irrestrita, no âmbito corporativo, por todo funcionário, independente do nível hierárquico ocupado pelo mesmo.

Art. 3º - O presente regulamento visa também garantir a confiabilidade, integridade, disponibilidade e inviolabilidade das informações pertencentes ao Conselho. As mesmas deverão ser protegidas, contra adulterações, cópias irregulares, ataques internos e externos, acidentes naturais como enchentes, raios, excesso de umidade e outros adversos como variação abrupta de energia e incêndios.

Parágrafo Único – O presente regulamento, encontra-se fundamentado na NBR ISSO 270001, que trata exclusivamente de Política de Segurança em Tecnologia da Informação. O fato de algum evento não ter sido citado explicitamente neste regulamento, não exime a responsabilidade do funcionário pelo ato praticado.

Seção II
Das Definições

Art. 4º - Para fins deste regulamento, considera-se:

I - Ativo de Informação – é o patrimônio, composto por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos do Conselho;

II - Ativos de Processamento – é o patrimônio composto por todos os equipamentos e programas necessários para a execução dos sistemas e processos, tanto os produzidos internamente quanto os adquiridos;

III - Controle de Acesso – não restrições ao acesso às informações de um sistema ou a locais sensíveis. Sendo estes controlados segundo diretrizes definidas pelo Conselho;

IV - Custódia – consiste na responsabilidade de se guarda um ativo para terceiros. Entretanto, a custódia não permite automaticamente o acesso ao ativo, nem o direito de conceder acesso a outros;

V - Direito de Acesso – a privilégio de acesso a um ativo que está condicionado ao processo, pessoa e o cargo que o mesmo ocupa;

VI - Ferramentas – é um conjunto de equipamentos, programas, procedimentos, normas e demais recursos através dos quais se aplica a Política de Segurança da Informação;

VII - Incidente de Segurança – é qualquer evento ou ocorrência que promova uma ou mais ações que comprometa ou que seja uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo do Conselho;

VIII - Política de Segurança – é um conjunto de diretrizes destinadas a definir a proteção adequada dos ativos de informação e de processos do Conselho;

IX - Proteção dos Ativos – são processos e procedimentos de controle, uso e guarda que permitem a proteção, integridade e a inviolabilidade dos ativos do Conselho;

X - Responsabilidade – é definida como as obrigações e os deveres da pessoa que ocupa determinada função em relação ao acervo de informação e os ativos colocados à sua disposição para desempenho das suas funções.

Art. 5º - Das expressões em língua estrangeira:

I - Password – senha de acesso;

II - User-ID – conta do funcionário ou identificação do funcionário;

III - Modem – equipamento utilizado para Comunicação de dados entre redes e/ou computadores;

IV - Foward – encaminhamento;

V - Firewall – barreira de proteção entre redes de computadores;

VI - IDS – Sistema Detector de Intrusão, junto com o firewall enfatiza a segurança de redes contra ataques;

VII - Proxy – permite o controle de perfis e armazena os endereços visitados para agilizar o acesso à Internet;

VIII - Site – endereço de uma página WEB na Internet;

IX - Logs – trilhas de auditória.

Seção III
Da Gestão de Segurança da Informação

Art. 6º - As informações exatas, atuais, relevantes e corretamente protegidas são absolutamente essenciais para o Conselho, com o fim de garantir que a informação seja adequadamente manipulada, todos os acessos, usos e processamentos de informações deve ser feito de acordo com a Política de Segurança em vigor.

Art. 7º - A não ser que existam exceções documentadas por escrito, todos os programas e documentações gerados pelos funcionários, consultores ou prestadores de serviços são de propriedade do Conselho.

Art. 8º - O Conselho tem a propriedade legal de todos os arquivos armazenados em seus computadores e redes, bem como de todas as mensagens transmitidas via seus sistemas. O Conselho se reserva o direito de acessar essa informação quando julgar conveniente, não podendo ser alegado quebra de sigilo.

Art. 9º - Os funcionários, usuários da rede de computadores do Conselho devem sempre dar o crédito apropriado da fonte de informação.

Art. 10 - Todos os funcionários que submetem informações ao público, por exemplo, site internet do Conselho e outros tipos de publicações garantem ao mesmo o direito de editar, copiar, repudiar e distribuir tal informação. Se outros, além do funcionário que submete essa informação, possuírem o direito de propriedade de tal informação, o funcionário que submeter esse material deve indicar este fato no momento da publicação.

Art. 11 - O Conselho apoia fortemente a estrita conformidade às observações de licenciamento e direitos autorais que os fabricantes de software veiculam em seus produtos. Se os funcionários fazem tais cópias de software não autorizadas, eles o fazem por iniciativa e interesses próprios, pois, tais cópias são terminantemente proibidas no âmbito interno. Da mesma forma, a reprodução de todo material protegido pelas leis do Direito autoral só é permitida dentro da extensão legal considerada "uso justo" ou com a permissão de autor ou editor.

Art. 12 - A não ser que seja outra forma, especificado por contrato, toda informação confidencial ou proprietária que tiver sido confiada por terceiros ao Conselho deve ser protegida com se fosse uma informação confidencial.

Art. 13 - As informações do Conselho (informação sobre processo, base de dados, sistemas de informação, documentação, etc.) devem ser usadas apenas para as atividades do mesmo.

Seção IV
Da Privacidade dos dados

Art. 14 - Todas as mensagens enviadas através dos computadores e sistemas de comunicação do Conselho são de propriedade do mesmo. A fim de manter e gerenciar essa propriedade, os dirigentes se reservam o direito de examinar toda informação armazenada ou transmitida por esses sistemas.

Art. 15 - Tendo em vista que os computadores e sistemas de comunicação do Conselho devem ser utilizados unicamente para o propósito das atividades laborais, os funcionários não devem ter nenhuma expectativa de privacidade associada à informação que eles armazenam ou enviam através desses sistemas. Esta monitoração, quando necessária será feita, pela área ou pessoa que possua esta prerrogativa.

Art. 16 - Usando os sistemas do Conselho, os funcionários consentem implicitamente que toda a informação armazenada por eles nos sistemas do Conselho seja divulgada para fins legais.

Art. 17 - Os funcionários, usuários da rede de computadores do Conselho estão proibidos de coletar informações privadas (raça, religião, opiniões políticas, opção sexual, etc.) a não ser que a coleta dessas informações tenha sido aprovada previamente por sua chefia imediata.

Art. 18 - A qualquer momento e sem comunicação antecipada, os responsáveis pela auditoria de segurança poderão examinar arquivos e diretórios pessoais, arquivos nos discos rígidos e outras informações armazenadas nos sistemas do Conselho. Este exame é realizado para garantir o cumprimento das políticas internas, apoiar a execução de investigações internas e auxiliar no gerenciamento dos sistemas de informação do Conselho.

Art. 19 - A Equipe Técnica registra constantemente os Sites visitados pelos funcionários, arquivos baixados da Internet e trocas de informações realizadas através desta rede. As chefias imediatas possuem prerrogativas e meios para acessarem estas informações.

Art. 20 - Informações sobre as atividades dos funcionários poderão ser coletadas anonimamente para cálculo dos níveis de utilização dos sistemas, para identificar áreas problemáticas ou para ampliar de outra forma as informações sobre os sistemas.

Art. 21 - Quando em dúvida sobre a execução de qualquer ação particular assistida computacionalmente, os funcionários deverão informar àqueles que serão afetados pela ação. A comunicação deve incluir uma descrição da ação proposta, a intenção da ação e os potenciais impactos que poderá haver aos

destinatários da comunicação. Antes que a ação seja executada, os afetados devem dar seu consentimento claro e inequívoco ou no mínimo terem a oportunidade de ser opor antes que a ação seja executada. Na ausência de tais consentimentos, a permissão de um dirigente deverá ser obtida para execução da ação.

Seção V
Da Confidencialidade dos dados

Art. 22 - Todas as informações do Conselho devem ser protegidas de exposição a terceiros. Pessoas externas não podem ter acesso às informações internas do Conselho, quando houver necessidade de prover acesso às pessoas externas a qualquer informação do Conselho este acesso será liberado apenas após uma autorização formal da gerência responsável.

Art. 23 - Se uma informação sensível é perdida, exposta a pessoas não autorizadas ou suspeita de ter sido perdida ou exposta a pessoas não autorizadas, seu proprietário e gerência responsável devem ser notificados imediatamente.

Art. 24 - Os funcionários não devem divulgar para qualquer pessoa estranhar ao quadro do Conselho, os sistemas de controle da informação que são utilizados, bem como a forma como esses controles são implementados. Exceções serão feitas, apenas, se houver uma permissão prévia da Gerência, neste ato a mesma torna-se corresponsável por esta divulgação.

Seção VI
Da Integridade dos dados

Art. 25 - Os dados e programas de produção devem ser alterados apenas por pessoas autorizadas de acordo com os procedimentos estabelecidos.

Art. 26 - É proibido falsificar, ocultar, suprimir ou substituir a identidade de um funcionário de um sistema de comunicação eletrônico. O nome do funcionário, o endereço de correio eletrônico, o nome do Conselho e informação relacionada incluídas nas mensagens devem refletir o real remetente das mensagens.

Art. 27 - O Conselho se reserva o direito de remover de seus sistemas de informação qualquer material visto como ofensivo ou potencialmente ilegal.

Art. 28 - Os comentários que os funcionários postam em um sistema de correio eletrônico, num fórum de discussões ou em outros sistemas eletrônicos não são, necessariamente, declarações formais ou a posição oficial do Conselho.

Art. 29 - Hostilização sexual, étnica e racial – incluindo chamadas telefônicas não desejadas, correio eletrônico e correio interno, são estritamente proibidas.

Seção VII
Da Segurança de pessoal

Art. 30 - A Área Administrativa deve adotar critérios rígidos para o processo seletivo de candidatos, com propósito de selecionar pessoas reconhecidamente idôneas e sem antecedentes que possam comprometer a segurança ou credibilidade do Conselho.

Art. 31 - A área Administrativa, no processo de contratação, deve dar ao funcionário o conhecimento da Política de Segurança, entregar as Normas de Segurança, colher assinatura de concordância de trabalho sob as condições imposta e arquivá-las na respectiva pasta funcional. Esta assinatura implica que o funcionário se compromete a seguir rigorosamente o que está determinado nesta Norma de Segurança.

Art. 32 - A Área Administrativa providenciará o crachá de identificação do funcionário, que é o instrumento que permite o acesso às áreas autorizadas.

Art. 33 - Os Gestores das áreas são responsáveis por definir as atribuições de cada função, de acordo com a característica das atividades desenvolvidas, a fim de determinar-se o perfil necessário do funcionário ou prestador de serviço para desempenho de suas atividades, considerando-se os seguintes itens:

I - A descrição sumária das tarefas inerentes à função;
II - As necessidades de acesso a informações sensíveis;
III - O grau de sensibilidade da área onde a função é exercida;
IV - As necessidades de contato de serviço interno e/ou externo;
V - As características de responsabilidade, decisão e iniciativa inerente à função;
VI - A qualificação técnica necessária ao desempenho da função.

Art. 34 - A Área Administrativa deve elaborar levantamento que permitam a "priori", ter dados que possam avaliar a idoneidade, o caráter e o perfil psicológico do candidato.

Art. 35 - É realizada, com propósito de confirmar e/ou identificar dados não detectados ou não confirmados durante a pesquisa para a sua admissão.

Art. 36 - Deve ser motivo de registro, por parte dos chefes imediatos, atos, atitudes e comportamentos positivos e negativos relevantes, verificados durante o exercício profissional dos seus funcionários.

Art. 37 - Todo o funcionário que constatar algum comportamento incompatível ou que possa gerar comprometimento à segurança corporativa, deverá comunicar a chefia imediata sob pena de ser solidário na transgressão da Política de Segurança do Conselho.

Art. 38 - As chefias imediatas assegurarão que todos os funcionários tenham conhecimento e compreensão da Política de Segurança e de suas Normas.

Art. 39 - É de dever dos chefes imediatos promover ações no sentido de manter, em alto grau, a conscientização de sues funcionários sobre a responsabilidade individual, no cumprimento destas Normas de Segurança.

Art. 40 - O acesso de ex-funcionários às instalações, quando necessário, será restrito às áreas de acesso público. O chefe imediato de cada funcionário em processo de desligamento do Conselho é responsável pelo cumprimento dos procedimentos constates na Norma de Segurança.

Seção VIII
Da Segurança do Ambiente

Art. 41 - Todo funcionário deve ser previamente identificado com a finalidade de obter permissão de acesso aos ativos de informação e processamento do Conselho.

Art. 42 - Nas áreas com acesso físico controlado, ficam sob a responsabilidade de cada Gerência a atribuição e revogação dos direitos de acesso dos funcionários. O acesso das pessoas não credenciadas às áreas controladas é da responsabilidade de cada Gerencia envolvida e deve ser sempre efetuada através de supervisão ou acompanhamento por pessoa indicada.

Art. 43 - O ambiente operacional, integrado pelos ativos de informação e de processamento será constantemente monitorado pelo responsável pela segurança, sendo constada qualquer irregularidade, a chefia responsável será formalmente notificada, devendo tomar as providências cabíveis. A falta de providencia por parte da chefia imediata atribui-lhe a responsabilidade solidária advinda do fato.

Art. 44 - A Equipe Técnica tem prerrogativa para desabilitar temporariamente o acesso à rede de qualquer funcionário, desde que possua indícios de que o mesmo está violando as Normas de Segurança. Neste caso, será gerado um relatório contendo o motivo para o bloqueio da conta. Este relatório deverá ser encaminhado à chefia imediata para anuência e avaliação.

Art. 45 - As senhas de acesso são de uso individual e restrito. O compartilhamento das senhas é terminantemente proibido, pois expõe o funcionário à responsabilidade pelas ações que outras pessoas realizarão com sua senha de acesso. Caso ocorra tal compartilhamento, seja de natureza autorizada ou não, o funcionário possuidor da senha compromissada assumirá todas as responsabilidade e consequência advindas deste ato.

Art. 46 - Todas as senhas de acesso à rede e demais sistemas corporativos devem ter no mínimo sete (7) caracteres.

Art. 47 - Toda senha de acesso deve ser imediatamente alterada caso haja suspeita ou conhecimento que tenham sido expostas a pessoas desautorizadas. A exposição indevida da senha de acesso é de responsabilidade do funcionário proprietário da mesma e a ele serão atribuídas as consequências inerentes.

Art. 48 - As senhas definidas devem ser de difícil dedução por outros usuários e/ou programas específicos à quebra de senhas. Senhas fáceis de serem deduzidas representam um ponto de alta vulnerabilidade para a segurança do ambiente corporativo, por exemplo, o CPF, o nome da esposa, fragmento de um endereço ou datas de aniversário, dentre outras senhas óbvias, não devem ser utilizadas. As senhas não devem ser uma palavra encontrada no dicionário ou alguma outra linguística. Por exemplo, nome próprios, lugares, termos técnicos e gírias não devem ser utilizados.

Art. 49 - Não é aconselhável o uso de senhas de acesso fixa que sejam geradas pela combinação de um conjunto de caracteres que não se altera e, com um conjunto de caracteres que é periodicamente alterado, por exemplo, os funcionários não podem empregar senhas de acesso semelhantes a "SocramJam" em janeiro, "SocramFev" em fevereiro ou outras combinações no gênero.

Art. 50 - Os funcionários devem escolher senhas de fácil memorização, mas que sejam ao mesmo tempo difíceis de serem descobertas por outras pessoas. Por exemplo:
I - Combinar número e pontuação em uma palavra regular;
II - Criar acrônimos a parti de palavras de uma música, um poema ou outra sequência de palavras conhecida;
III - Misturar caracteres alfabéticos e não alfabéticos. Os caracteres não alfabéticos são os números (0-9) e sinais de pontuação. Não podem ser utilizados caracteres de controle ou outros caracteres não imprimíveis porque os mesmos podem causar problemas de transmissão na rede ou chamada não intencional a certos utilitários do sistema.
IV - Mistura várias palavras em caixa altas e caixa baixa;
V - Encadear várias palavras formados o que é conhecido como "frases de acesso". Por exemplo, "Nas próximas férias em dezembro irei para a Europa!" geraria a senha: "Npfe12ipaE!".

Art. 51 - Os funcionários não devem construir senhas de acesso que sejam idênticas ou substancialmente similares às senhas de acesso que foram empregadas anteriormente.

Art. 52 - Todo funcionário que esquecer sua senha de acesso terá novamente uma senha inicial atribuída pela Equipe Técnica para que possa realizar um primeiro "log-on" e imediatamente trocaram a sua senha de acesso. Desde que devidamente identificado pela Equipe Técnica. A senha de acesso não deve ser trocada sob-hipótese alguma através de contato telefônico direto entre funcionário e técnico responsável pela troca de senha.

Seção IX
Dos Vírus de Computador

Art. 53 - Se os funcionários suspeitar de uma infecção por vírus, eles devem imediatamente desliga o computador envolvido, desconectá-lo da rede e solicitar o atendimento da Equipe Técnica. Esta orientação irá minimizar o dano aos seus arquivos e a propagação na rede, bem como garantir que seja registrada a informação necessária para evitar reinfecção.

Art. 54 - Os funcionários, usuários da rede não devem executar ou desenvolver quaisquer programa ou processo que consumam recursos significativos do sistema ou interfiram de outra forma nas atividades do Conselho. Também não devem intencionalmente executar ou tentar introduzir qualquer código projetado para auto replicar-se, danificar ou de qualquer outra maneira obstruir o acesso à rede do Conselho. Tais aplicativos podem ser considerados um vírus, worm, cavalo de Tróia, etc.

Art. 55 - Os funcionários não devem baixar arquivos da internet ou de quaisquer outros ambientes externo ao Conselho. Esta recomendação é necessária porque tais arquivos poderão conter vírus, worms, cavalo de Tróia que podem comprometer os sistemas e informações. Caso haja uma legítima necessidade de obter uma aplicação de terceiros o fato deve ser comunicado à Equipe Técnica para que este estabeleça os procedimentos de segurança necessários a essa operação.

Art. 56 - A fim de evitar a infecção por vírus, os funcionários não devem usar qualquer software adquirido externamente de uma pessoa ou outra organização que não seja um fornecedor de confiança. A única exceção para isso é quando tal software teve sido testado e aprovado pela Equipe Técnica.

Art. 57 - As unidades (disquetes, pen-drivers, CDs-ROMS) de origem externa não podem ser usadas nas estações de trabalho do Conselho ou nos servidores de rede antes de serem submetidos à varredura do software antivírus adotados no Conselho e constatar-se ausência de vírus.

Art. 58 - Todos os arquivos transferidos ou acessados de fontes não confiáveis (ex. internet ou qualquer rede externa) devem ser examinados pelo próprio funcionário, através de varredura pelo software de detecção de vírus utilizado pelo Conselho. Este exame deve acontecer antes que o arquivo seja executado ou aberto por outro programa, como por exemplo, um processador de texto e também, antes e depois que o material tenha sido descompactado.

Seção X
Do Correio eletrônico

Art. 59 - O Conselho utiliza rotineiramente ferramentas que pesquisam o conteúdo das mensagens de correio eletrônico a fim de identificar palavras chaves selecionadas, tipos de arquivos e outras informações. Os funcionários deverão restringir suas mensagens, unicamente aos assuntos relacionados

com o Conselho. Deve ser observada a natureza não sigilosa das comunicações nos serviços de correio eletrônico.

Art. 60 - Os funcionários não devem usar uma conta de correio eletrônico associada a outro indivíduo para enviar ou receber mensagens.

Art. 61 - O sistema de correio eletrônico é disponibilizado para ser usado nas atividades do Conselho e somente seu uso profissional está autorizado. É desaconselhável o uso de Correio Eletrônico externo através de utilização da infraestrutura de comunicação do Conselho. Tal recomendação leva em consideração principalmente a grande quantidade de vírus, cavalos de tróia, worms e exploits oriundos dos provedores externos.

Art. 62 - Os funcionários estão proibidos de enviarem ou encaminharem quaisquer mensagens via os sistemas de informações do Conselho que possa ser considerada como difamatória, inoportuna ou de fim explicitamente sexual. Os funcionários também são proibidos de enviarem ou encaminharem mensagens ou imagens que possam ter conotação ofensiva de raça, sexo, nacionalidade, orientação sexual, religião, filiação política ou deficiência física.

Art. 63 - Com a finalidade de minimizar a contaminação por vírus, otimiza o tráfego de rede e o espaço de armazenamento em disco no servidor de correio eletrônico, são filtradas de forma automática, mensagens que possuam arquivos anexados com as seguintes extensões: JPG,JPEG,MP3,BAT,EXE,COM,INI,PIF,AVI,MPEG,BMP E PPS. Poderão ser adicionadas, a esta lista, sem aviso prévio, qualquer outra extensão que a Equipe Técnica julga conveniente.

Art. 64 - É praticada a aplicação de filtros para o recebimento de mensagens classificadas como SPAM, que além de imputarem tráfego espúrio, em nada contribuem, nas atividades laborais dos funcionários. Fato que implica por parte do funcionário no não encaminhamento das mensagens classificadas como tal e/ou que tentem sobrepor às barreiras existentes.

Art. 65 - A não ser que a mensagem esteja criptografada, considere o correio eletrônico como sendo equivalente a um cartão postal. Os funcionários devem evitar enviar números de cartões de crédito, senhas, informações de pesquisas e desenvolvimento e outros dados sensíveis via correio eletrônico. O Conselho não se responsabiliza pelas informações pessoais, fornecidas pelos seus funcionários através da Internet ou qualquer outra rede pública.

Seção XI
Do Acesso à Internet

Art. 66 - Os sistemas de acesso à Internet são configurados para evita que os funcionários se conectem em sites não relacionados às atividades do Conselho. Os funcionários que usam os sistemas de informações não têm permissão para acessar um site cujo conteúdo seja de explicitação sexual, racismo ou outro material potencialmente ofensivo. A capacidade para conectar um site específico não implica em permissão para acessar o mesmo.

Art. 67 - O acesso de qualquer computador da rede do Conselho à Internet é feito através de um equipamento firewall. Outras formas de acessar a Internet, como conexão dial-up, Modems WAP, ou outros dispositivos do gênero, são proibidas de serem utilizadas.

Art. 68 - O acesso à Internet é reservado para aqueles que têm uma necessidade demonstrável para tal, ou que sejam autorizadas por seu chefe imediato.

Art. 69 - A não ser que seja expressamente autorizado pela gerência responsável, os funcionários são proibidos de participarem em grupos de discussão na Internet, sala de conversação e outros fóruns públicos eletrônicos, quando utilizando os sistemas do Conselho.

Art. 70 - Embora seja um ambiente informal de comunicações, as leis de copyright, patentes e marcas são aplicáveis. Por essa razão, os funcionários que usam os sistemas do Conselho devem, por exemplo:

I - Reeditar material apenas após ter obtido permissão da fonte;
II - Citar material de outras fontes somente se essas outras fontes forem identificadas;
III - Revelar informações internas do Conselho na Internet apenas se a informação tive sido oficialmente aprovada para liberação ao público.

Art. 71 - As informações do Conselho, de caráter sigiloso ou reservado, nunca deverão ser enviadas através da Internet a não ser que tenha sido primeiramente criptografadas por métodos aprovados.

Art. 72 - Toda informação obtida na Internet deverá ser analisada com atenção, pois a grande maioria dos sites não possui um sistema de segurança que garante a integridade e confiabilidade de seus dados.

Art. 73 - Os funcionários não devem colocar material do Conselho (software, memorando internos, publicações, etc.) em qualquer computador publicamente acessível à Internet a não se que tal postagem tenha sido primeiramente aprovada pela gerencia responsável.

Art. 74 - Os funcionários não devem transferir software que tenha sido licenciado de terceiros ou que tenham sido desenvolvidos pelo Conselho para qualquer computador via Internet a não ser que haja uma autorização da gerência responsável.

Seção XII
Da Conexão Intranet

Art. 75 - Antes que qualquer informação seja colocada na Intranet do Conselho, esta deve previamente ter a anuência da chefia imediata e autorização do Gestor da Área.

Art. 76 - O conteúdo divulgado na Intranet é propriedade do Conselho.

Art. 77 - Todo o conteúdo divulgado na Intranet é propriedade do Conselho a não ser que haja uma determinação em contrário dos dirigentes do Conselho.

Art. 78 - Antes de divulgar qualquer material na Intranet, o Gestor da Intranet deve realizar uma verificação de toda informação e programas a fim de garantir que os mesmos não contêm vírus, cavalos de Tróia e outros códigos maliciosos. Deve também confirma a exatidão, atualidade e relevância da informação para as atividades do Conselho antes de divulgá-las. Da mesma forma, todas as questões legais, como divulgação de informação confidencial e o ato infringirem direitos autorais devem ser resolvidas antes da publicação.

Art. 79 - Antes de divulgação na Intranet do Conselho, toda as páginas desenvolvidas devem ter sido testadas pelo Gestor da Intranet para detecção de problemas operacionais e de segurança de acordo com um processo aprovado pela Equipe Técnica.

Seção XII
Da Segurança dos ativos de informação

Art. 80 - Os computadores e sistemas de comunicações não devem ser utilizados para fins pessoais. Os recursos computacionais, colocados à disposição do funcionário deverão estar alocados corretamente no centro de custo de atividade do funcionário e o respectivo Termo de Responsabilidade assinado por este. Na ausência deste registro, o superior imediato assume esta responsabilidade.

Art. 81 - Todo o funcionário, indicado no Termo de Responsabilidade ou a chefia imediata, na ausência de indicação, responde pelo mau uso ou dano causado nos equipamentos.

Art. 82 - Quando deixados desacompanhados, o processo de log-off ou lock deve sempre ser realizado nos computadores conectados à rede do Conselho.

Art. 83 - Se o funcionário tiver privilégios de administração em estação de trabalho, não deve adicionar e/ou remove outros usuários aos grupos de administração local. Somente a Equipe Técnica detém esta prerrogativa. É proibida a utilização de qualquer outro artifício (Ex. Queries SQL Root Kit, Deamons, etc.) que adicione um usuário ou grupo de administração local da estação de trabalho, exceto as de maneira convencional.

Art. 84 - O compartilhamento de recursos nas estações de trabalho deve ser atribuído única e exclusivamente para facilitar e/ou agilizar o trabalho das atividades laborais, não devendo ocorrer em qualquer outra situação.

Art. 85 - Os funcionários não podem alterar a configuração das estações de trabalho. Isto inclui software (parâmetros do sistema operacional, alteração de contas dos grupos locais, etc.), e hardware (instalações e configurações de dispositivos, BIOS etc.)

Art. 83 - Os funcionários estão proibidos de armazenar ou utilizar arquivos multimídias nas estações de trabalho. Estão inclusos nesta categoria às seguintes extensões:

I - Áudio: MP3, OGM;
II - Vídeo: AVI, MPEG, JPEG, OGG;
III - Imagem: JPG, GIF, BMP;
IV - Apresentação: PPS;
V - São exceções a esta regra os dados autorizados pela gerência imediata e dados necessários para as atividades profissionais no âmbito do Conselho.

Parágrafo Único - Outras extensões podem ser atribuídas aos aplicativos multimídia, os funcionários devem estar atentos que esta proibição não se aplica somente às extensões citadas e sim a qualquer outra que esteja relacionada com aplicativos usuais.

Art. 84 - São terminantemente proibidos, prática, armazenamento e compartilhamento de jogos de qualquer natureza, nos computadores do Conselho.

Art. 85 - Os funcionários não podem instalar programas novos ou atualizações nas estações de trabalho. Somente a Equipe Técnica está autorizada a realizar instalações e remoção de programas.

Art. 86 - Os softwares que apoiam as aplicações de produção (incluindo sistemas operacionais, web browsers e programas utilitários) devem ser adquiridos de um fornecedor previamente homologado. Os softwares livres também conhecidos como "freeware" não são permitidos a não ser que sejam especificamente avaliados e aprovados pela Equipe Técnica.

Art. 87 - Os funcionários não podem utilizar técnicas de mascaramento dos programas proibidos, com objetivo de burla os sistemas de auditoria.

Art. 88 - Os funcionários não podem alterar a conexão das estações à rede corporativa, tal como trocar o ponto físico ou operação similar diretamente nos ativos de rede.

Art. 89 - A utilização de computadores portáteis (notebooks, handhelds, iPads, etc) na rede corporativa deve estar sujeita à autorização formal da Equipe de Técnica.

Art. 90 - As atualizações de segurança, manutenção deveram ser realizadas a cada 15 dias pela equipe de Suporte Técnico:

I - Verificar Atualização de Antivírus;

II - Atualização de Sistema Operacional;

III - Limpeza de Disco;

IV- Atualização de aplicativos diversos.

Art. 91 - Os funcionários e visitantes não deve fumar, comer ou beber próximos aos equipamentos de informática.

Art. 92 - Deve ser observada a voltagem que o equipamento está ajustado antes de conectá-los à rede elétrica, de modo a evitar em voltagem errada, que pode causar danos.

Art. 93 - Os funcionários devem ter cuidado no manuseio de teclado, mouse e cabos de conexão, para evitar danos aos equipamentos. Os funcionários não devem alterar as conexões de teclado, mouse e demais periféricos, nem trocá-los de máquina.

Art. 94 - Qualquer movimento de equipamento, troca de responsável ou qualquer ato que implique na mudança dos dados cadastrais de inventário, deve ser solicitado e informado à Área Administrativa que tomará as providências cabíveis para a demanda.

Seção XIII
Da Segurança dos ativos de processamento

Art. 95 - Os funcionários que utilizam os sistemas de informações do Conselho estão proibidos de obter acesso não autorizado a qualquer outro sistema de informação interno ou de qualquer forma danificar, alterar ou descontinuar as operações desses sistemas. Da mesma forma, os funcionários estão proibidos de capturar telas ou obter por outros meios, senhas, chaves de criptografia ou qualquer outro mecanismo de controle de acesso que possa possibilitar o acesso não autorizado.

Art. 96 - As permissões de controle de acesso, aos arquivos para todos os sistemas do Conselho devem ser configuradas, por padrão, para bloquear o acesso a pessoas não autorizadas.

Art. 97 - Os funcionários não devem ler, modificar, remover ou copiar arquivo que pertença a outro funcionário sem primeiramente obter permissão do proprietário do arquivo. A não ser que o uso geral esteja claramente permitido, a habilidade para ler, modificar, remover ou copiar um arquivo pertencente a outro funcionário não implica em permissão para realmente executar estas atividades.

Art. 98 - O Conselho ser reserva o direito de revogar os privilégios do sistema de qualquer funcionário a qualquer momento. Não serão permitidas condutas que interfiram com a operação normal e adequada dos sistemas de informação

do Conselho e que adversamente afetem a capacidade de outras pessoas utilizarem esses sistemas de informação, bem como condutas que sejam prejudiciais ou ofensivas.

Art. 99 - Os funcionários não podem testar ou tentar comprometer os controles internos a não ser que haja uma aprovação prévia por escrito.

Art. 100 - Os funcionários não podem explorar as vulnerabilidades ou deficiências nos sistemas de segurança da informação com a finalidade de danificar os sistemas ou as informações, obter recursos além daqueles que lhe foi autorizado, retirar recursos de outros funcionários ou ganhar acesso a outros sistemas para os quais não tenham recebidos autorização. Todas as vulnerabilidade e deficiências deveram ser imediatamente relatadas à Equipe Técnica.

Seção XIV
Da Segurança das Comunicações

Art. 101 - É proibida a instalação de linhas de voz ou dados adicionais, sem que tenha sido obtida uma autorização prévia para tal.

Art. 102 - Os funcionários não devem instalar Servidores ou serviços de roteamento com conexões de modem para redes externas do Conselho ou outros sistemas multiusuários para comunicação da informação sem a aprovação de Equipe Técnica.

Art. 103 - Somente é permitido utilizar os recursos de criptografia aprovados pela Equipe Técnica. Não é permitido aos funcionários empregarem outros sistemas de criptografia, ou certificados digitais, para atividades de produção ou informações. Todo dado sensível do Conselho transmitido através de qualquer rede de comunicação, deve ser enviado na forma criptografada.

Art. 104 - Informações relativas ao acesso aos computadores do Conselho e sistemas de comunicações, como números telefônicos das conexões dial-up, são consideradas confidenciais, estas informações não devem ser disponibilizadas na Internet, relacionadas em lista telefônicas, colocadas em cartões de visita ou disponibilizadas de outra maneira a terceiros sem a permissão por escrito da gerência responsável. Os números de telefone, fax e endereços de correio eletrônicos são exceções permissíveis desta norma.

Art. 105 - Os funcionários são proibidos de conectarem modems WAP às estações de trabalho que estejam simultaneamente conectadas a rede local (LAN) e outra rede de comunicação externa.

Art. 106 - É proibido o uso de modems locais e/ou remotos para estabelecer conexões discadas diretas. Todas as conexões, dial-up com os sistemas a redes do Conselho devem ser roteadas através de equipamento específico, configurado e mantido pela Equipe Técnica.

Seção XV
Conformidade com as Políticas e Normas de Segurança

Art. 107 - Todo funcionário deve entender as Políticas e Normas de Conselho relativas à Segurança da Informação e devem aceitar por escrito em executar seu trabalho de acordo com as mesmas, mediante assinatura do "Termo de Aceite".

Seção XVI
Da Comunicação dos incidentes de segurança

Art. 108 - Toda suspeita de incidentes de segurança deve ser reportado o mais rapidamente possível através dos canais de comunicação estabelecidos no documento de Política de Segurança do Conselho.

Art. 109 - As páginas de abertura de todos os sites do Conselho devem incluir informações para contato (endereço de e-mail, número de telefone, etc.).

Art. 110 - Toda suspeita de infecção dos computadores pessoais por vírus deve ser comunicada imediatamente à Equipe Técnica.

Art. 111 - Todos os maus funcionamentos de software devem ser imediatamente reportados à Equipe Técnica.

Seção XVII
Das Responsabilidades e Deveres

Art. 112 - As responsabilidades dos níveis gerenciais compreendem dentre outras as seguintes:

I - Gerenciar o cumprimento da Política e Normas de Segurança, por parte dos funcionários sob sua chefia;
II - Identificar e comunicar a quem de direito os desvios praticados e adotar as medidas corretivas apropriadas;
III - Impedir o acesso dos funcionários demitidos ou demissionários aos ativos de informação sob sua responsabilidade;
IV - Proteger, em nível físico e lógico, os ativos de informação sob sua responsabilidade;
V - Garantir que o pessoal sob sua supervisão compreenda e desempenhe a obrigações de proteger a informação do Conselho;
VI - Comunicar formalmente à Equipe Técnica que efetua a concessão de privilégios aos usuários, qual o perfil de acesso dos funcionários a ele subordinados;
VII - Comunicar formalmente à Equipe Técnica que efetua a concessão de privilégios aos usuários, quais os funcionários demitidos ou transferidos, para exclusão no cadastro dos usuários;
VIII - Comunicar formalmente à Equipe Técnica que efetua a concessão de privilégios a usuários, aqueles que estejam respondendo a processos,

sindicância ou que estejam licenciados, para inabilitação no cadastro dos usuários;
IX - Dar conhecimento aos responsáveis pela segurança da ocorrência de qualquer irregularidade ou desvio das Políticas e Normas de Segurança, estando a ele correlacionadas ou não.

Art. 113 - Os deveres dos funcionários compreendem dentre outros os seguintes:

I - Cumprir a Política e Normas de Segurança, sob pena de incorrer sanções disciplinares e legais cabíveis;
II - Preservar a integridade e guarda sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações;
III - Utilizar os Sistemas de Informações e os recursos a ela relacionados somente para a execução das atividades correlacionadas com o desempenho de seu trabalho;
IV - Cumprir as regras específicas de proteção estabelecidas aos ativos de informação;
V - Manter o caráter sigiloso da senha de acesso aos recursos e sistemas do Conselho;
VI - Não compartilhar, sob qualquer forma, informações sigilosas com outros que não tenham a devida autorização de acesso;
VII - Responder, por todo e qualquer acesso, aos recursos do Conselho bem como pelos efeitos desses acessos efetivados através do seu código de identificação, ou outro atributo para esse fim utilizado;
VIII - Respeitar a proibição de não usar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material, em violação da legislação de propriedade intelectual pertinente;
IX - Comunicar ao seu superior imediato o conhecimento de qualquer irregularidade ou desvio da Política e Norma de Segurança do Conselho.

Art. 114 - As responsabilidades da Equipe Técnica compreendem dentre outras as seguintes:

I - Estabelecer as regras de proteção dos ativos;
II - Avaliar e/ou decidir quanto às medidas a serem tomadas no caso de violação das regras estabelecidas;
III - Revisar periodicamente as regras de proteção estabelecidas;
IV - Restringir e controlar o acesso e os privilégios de usuários remotos e externos;
V - Executar as regras de proteção estabelecidas pela Política de Segurança;
VI - Detectar, identificar e registrar as violações ou tentativas de acesso não autorizadas;
VII - Definir e aplicar, para cada usuário, restrições de acesso à rede, como horário e dias autorizados, entre outras;
VIII - Manter registro (logs) de atividades de usuários;
IX - Limitar o prazo de validade das contas de Prestadores de Serviços Externos ao período da prestação de serviços prestados;
X - Excluir as contas inativas;

XI - Fornecer senhas de contas privilegiadas somente aos funcionários que necessitarem efetivamente dos privilégios, mantendo-se o devido registro e controle.

Art. 115 - Os deveres os Prestadores de Serviços compreendem dentre outros os seguintes:

I - Seguir as cláusulas previstas no contrato, que contemplem a responsabilidade dos prestadores de serviços no comprimento da Política e Normas de Segurança da Informação;
II - Cumprir a Política e Normas de Segurança, sob pena de incorrer nas sanções disciplinares e legais cabíveis;
III - Preservar a integridade e guarda sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações;
IV - Utilizar os Sistemas de Informação e os recursos a ela relacionados somente para a execução das atividades correlacionadas com o desempenho de seu trabalho;
V - Cumpri as regras específicas de proteção estabelecidas aos ativos de informação;
VI - Manter o caráter sigiloso da senha de acesso aos recursos e sistemas do Conselho;
VII - Não compartilha, sob qualquer forma, informações sigilosas com outros que não tenham a devida autorização de acesso;
VIII - Responder, por todo e qualquer acesso, aos recursos do Conselho bem como pelos efeitos desses acessos efetivados através do seu código de identificação, ou outro atributo para esse fim utilizado;
IX - Respeitar a proibição de não usar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material, em violação da legislação de propriedade intelectual pertinente;
X - Comunicar ao seu superior imediato o conhecimento de qualquer irregularidade ou desvio da Politica e Normas de Segurança do Conselho.

Art. 116 - Cada área que detém os ativos de processamento e de informação é responsável por eles, devendo prover a sua proteção de acordo com a Política de Segurança de Informação;

Art. 117 - Todos os ativos de informações deverão ter claramente definidos os responsáveis pelo seu uso;

Art. 118 - O fato de algum evento não ter sido citado explicitamente nesta Norma, não exime a responsabilidade do funcionário pelo ato praticado.

Seção VXIII
Das Sanções

Art. 119 - Aos funcionários que, de forma intencional ou não, desrespeitarem as normas estabelecidas neste documento, serão aplicadas as seguintes sanções:

CONASS
Conselho Nacional de Secretários de Saúde

I - Advertência escrita;
II - Suspensão do direito de uso de serviços oferecidos pela rede do Conselho por tempo indeterminado;
III - Demissão.

Parágrafo único - De acordo com a gravidade analisada e de posse dos registros comprobatórios, o assunto será encaminhado ao Superior Hierárquico da área de ocorrência, para tomar as medidas cabíveis para o caso em questão.

Brasília, 04 de fevereiro de 2014.

JURANDI FRUTUOSO SILVA
Secretário Executivo