| | |
|---|---|
| **Processo** | **6.761-0/2011** |
| **Procedência** | **TRIBUNAL DE CONTAS DO ESTADO DE MATO GROSSO** |
| **Assunto** | **Dispõe sobre normas gerais para o manuseio de ativos de informação e recursos de tecnologia do Tribunal de Contas do Estado de Mato Grosso.** |
| **Relator Nato** | **Conselheiro Presidente VALTER ALBANO** |
| **Sessão de Julgamento** | **4-10-2011** |

# PROVIMENTO Nº 3/2011

Estabelece normas gerais para o manuseio de ativos de informação e recursos de tecnologia do Tribunal de Contas do Estado de Mato Grosso - TCE/MT.

**O TRIBUNAL DE CONTAS DO ESTADO DE MATO GROSSO,** no uso das atribuições que lhe são conferidas pelo inciso V, do artigo 4º, da Lei Complementar Estadual nº 269/2007 (Lei Orgânica do Tribunal de Contas do Estado de Mato Grosso) e pelo inciso XXVIII, do artigo 21, inciso V do artigo 78 e incisos II e III, do artigo 84, todos da Resolução nº 14/2007 (Regimento Interno do Tribunal de Contas do Estado de Mato Grosso),

**CONSIDERANDO** o disposto no art. 23 da Resolução nº 10/2010, que instituiu a Política de Segurança da Informação no âmbito do TCE/MT;

**CONSIDERANDO** a necessidade de estabelecer procedimentos e controles administrativos e tecnológicos a serem observados para o manuseio, tratamento, controle e proteção dos dados e informações produzidos, armazenados ou transmitidos, por qualquer meio pelos sistemas de informação do TCE/MT;

**RESOLVE:**

**Art. 1º.** Fica aprovado, na forma desta Instrução Normativa, as diretrizes com a finalidade de alcançar e manter a proteção adequada dos ativos do ambiente de Tecnologia da Informação, definindo as responsabilidades dos custodiantes de cada ativo tecnológico.

## TÍTULO I
## CONTROLE E CLASSIFICAÇÃO DOS ATIVOS DE INFORMAÇÃO

**Art. 2º.** Ficam sujeitos ao que estabelece esta Instrução Normativa todos os usuários internos e colaboradores dos recursos de tecnologia da informação do Tribunal de Contas do Estado de Mato Grosso, os quais terão a sua disposição, consideradas suas atribuições, estações de trabalho e demais *hardwares* e/ou *softwares*, a serem utilizadas para as atividades aprovadas pelo TCE/MT.

**Parágrafo único.** O uso das estações de trabalho é condicionado à assinatura do Termo de Responsabilidade de Utilização de Ativos e Recursos de Informática do TCE/MT.

**Art. 3º.** As estações de trabalho ou computadores portáteis deverão possuir versão do sistema operacional e demais *softwares* homologados e instalados pela Coordenadoria de Tecnologia da Informação.

**Art. 4º.** Todas as estações de trabalho ou computadores portáteis deverão possuir *software* antivírus homologado pelo TCE/MT, que de forma alguma poderão ser desinstalados ou reconfigurados e a sua atualização ocorrerá de forma automática via servidor.

**Art. 5º.** Os recursos de tecnologia da informação serão inventariados e controlados, sendo sua remoção ou remanejamento de responsabilidade do Serviço de Material e Patrimônio.

**Art. 6º.** As informações do TCE/MT são classificadas quanto a sua confidencialidade e disponibilidade, ainda que as mesmas não sejam explícitas, e os respectivos grau de sigilo e essencialidade são determinados em função de sua relevância para os processos internos ou serviços prestados pela instituição.

## TÍTULO II
## DOS CRITÉRIOS PARA CLASSIFICAÇÃO E MANUSEIO DAS INFORMAÇÕES

**Art. 7º.** As informações geradas, adquiridas ou trabalhadas pelo TCE/MT devem ter uma unidade que se responsabilizará pela classificação das informações quanto a sua confidencialidade e disponibilidade, bem como pela desclassificação quando estas não forem mais necessárias ou tornadas públicas.

**§ 1º.** A classificação quanto a confidencialidade de uma informação possui níveis determinados pela necessidade de sigilo, em função do seu teor ou dos seus elementos intrínsecos.

**§ 2º.** A classificação quanto a disponibilidade de uma informação possui níveis determinados pela sua relevância para a continuidade de processos internos ou serviços prestados pelo TCE/MT.

**Art. 8º.** Cada nível de classificação contemplará controles de segurança apropriados para o tratamento das informações, devendo ser previstos e utilizados controles diferenciados durante o ciclo de vida de uma informação, que compreende da criação, utilização ao descarte.

**Art. 9º.** Para a proteção dos recursos de Tecnologia da Informação, considerar-se-á o maior nível de informações nele armazenadas, processadas ou em trânsito.

**Art. 10.** Segundo a ótica da confidencialidade, as informações classificam-se em:

**I.** Restrita: Informação cujo conhecimento não autorizado pode acarretar dano à segurança da Instituição ou do Estado;

**II.** Confidencial: Informação cuja revelação não autorizada pode acarretar dano à sociedade, pessoas físicas e jurídicas, ou frustrar objetivos específicos;

**III.** Interna: Informação cuja revelação não autorizada pode comprometer as estratégias da Instituição;

**IV.** Pública: Informação divulgada para a sociedade, em conformidade com o modelo de transparência adotado pelo TCE/MT.

**§ 1º.** O Conselheiro relator poderá indicar, orientar e autorizar, a qualquer tempo, nos processos e documentos de sua competência, tanto a classificação de determinada informação como restrita quanto o levantamento do sigilo e a consequente reclassificação da informação.

**§ 2º.** A informação que não possua classificação explícita quanto a sua confidencialidade deverá ser tratada como interna.

**Art. 11.** As informações restritas ou confidenciais deverão ser identificadas por meio de etiquetas, em todas as suas mídias, sendo vedada aos usuários internos e colaboradores sua remoção, salvo quando autorizado pelo Conselheiro relator.

**Art. 12.** Os documentos ou relatórios impressos ou em meio digital deverão possuir a numeração das páginas, sequencialmente, e o total de páginas no rodapé, de forma que seja possível detectar a exclusão de qualquer página.

**Art. 13.** Em sendo necessária a utilização de serviços de correio ou mensageiro interno, as mídias contendo informações restritas ou confidenciais deverão estar acondicionadas em 2 (dois) envelopes de cor opaca, onde o envelope externo não deverá indicar a classificação da natureza das informações, já o interno conterá a etiqueta de classificação apropriada.

**Art. 14.** Mídias que contenham informações distintas devem ser identificadas pelo nível mais alto das informações armazenadas.

**Art. 15.** O envio de informações restritas ou confidenciais via correio eletrônico deverá ser evitado, entretanto, quando absolutamente necessário, o mecanismo poderá ser adotado desde que se tenha a certeza de a informação está sendo endereçada ao destinatário adequado e que o uso seja legítimo.

**Art. 16.** Os documentos ou relatórios contendo informações restritas ou confidenciais, quando não utilizados serão armazenados em gavetas ou armários, trancados.

**Art. 17.** É de responsabilidade do próprio usuário interno ou colaborador a guarda e/ou eliminação de eventuais rascunhos que o subsidiaram na elaboração do trabalho por ele produzido.

**Art. 18.** Ficarão responsáveis pelo sigilo de matérias em tramitação na instituição todos os usuários internos ou colaboradores que manusearam o respectivo processo.

**Art. 19.** A impressão de documentos ou relatórios contendo informações restritas ou confidenciais deverá ser controlada, preferencialmente realizada em impressoras locais, recomendando-se o seu recolhimento imediato quando concluída a tarefa, de forma a impedir que pessoas alheias ao negócio tomem conhecimento de seu conteúdo.

**Art. 20.** As informações restritas, confidenciais ou internas não deverão ser conversadas em locais públicos, ou na presença de pessoas alheias ao negócio, nem mesmo poderão ser tratadas via telefones fixos ou celulares.

**Art. 21.** As mídias ou documentos impressos contendo informações restritas, confidenciais ou internas, quando forem descartados, observaram a forma mais segura possível, preferencialmente mediante fragmentação, trituração ou incineração.

**Art. 22.** Os recursos de Tecnologia da Informação que armazenam ou trafegam informações restritas ou confidenciais deverão possuir controles de segurança adicionais, de forma a impedir acessos não autorizados.

**Parágrafo único.** A manutenção dos recursos tratado no *caput* deste será realizada ou assistida pela Coordenadoria de Tecnologia da Informação.

**Art. 23.** Havendo a necessidade de saída de um computador para manutenção externa, será extraída uma cópia de segurança dos arquivos (*backup*) do equipamento e, após, apagado o disco rígido, restaurando-se os arquivos quando do seu retorno.

**Art. 24.** Segundo a ótica da disponibilidade, as informações classificam-se em:

**I.** Indispensável: Informação indispensável para a continuidade de processos ou serviços prestados pela Instituição.

**II.** Complementar: Informação que apoia processos ou serviços prestados pela Instituição, não sendo essencial para sua continuidade.

**III.** Dispensável: Informação que pode ser omitida sem prejuízo a continuidade de processos ou serviços prestados pela Instituição.

**§ 1º.** Uma informação que não possua uma classificação explícita quanto a sua disponibilidade deve ser tratada como dispensável.

**§ 2º.** As informações quanto a disponibilidade, serão classificadas quando da sua criação ou aquisição, pelo respectivo gestor que também definirá o período de tempo em que é necessário que a mesma esteja disponível, considerando o uso de recursos de Tecnologia da Informação (sistemas e rede de comunicação).

**§ 3º.** Por padrão técnico, são considerados os seguintes graus de disponibilidade, que podem ser modificados pelos gestores para uma informação específica:

**I.** Indispensável: Alta disponibilidade (24 horas x 7 dias).

**II.** Complementar: Média disponibilidade (8 horas x 5 dias).

**III.** Dispensável: baixa disponibilidade.

**Art. 25.** Informações indispensáveis deverão ser resguardadas por um plano de continuidade de negócios, tendo em vista a garantia de alta disponibilidade e, juntamente com as complementares, possuirão política de *backup* (cópia de segurança), com medidas de prevenção e recuperação compatíveis com as mesmas.

TÍTULO III
DO GERENCIAMENTO DAS OPERAÇÕES
E COMUNICAÇÕES

**Art. 26.** Os usuários internos e os colaboradores se responsabilizarão pelas estações de trabalho e quaisquer *hardwares,* portáteis ou não, que vierem a utilizar, devendo tomar os cuidados necessários para preservar sua continuidade e garantir sua operação com segurança.

**Parágrafo único.** É proibida a utilização dos recursos de tecnologia da informação não específicos para sua finalidade, para testes ou utilização de ferramentas que possam causar, acidental ou intencionalmente, danos ao TCE/MT ou a terceiros.

**Art. 27.** Todo e qualquer documento de conteúdo relacionado aos processos internos ou serviços prestados pelo TCE/MT deverá ser armazenado no servidor de arquivos, em diretório de acesso restrito aos usuários internos e colaboradores que dele necessite para o desempenho de suas funções.

**Art. 28.** Os arquivos armazenados nas estações de trabalho, computadores portáteis e servidores de rede são de propriedade do TCE/MT, que se reserva o direito de auditá-los sem aviso prévio.

TÍTULO IV
DA CRIAÇÃO E ADMINISTRAÇÃO DE CREDENCIAIS DE ACESSO
AOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

**Art. 29.** O acesso aos recursos de Tecnologia da Informação do TCE/MT somente são permitidos mediante identificação e autenticação dos usuários internos e colaboradores, denominadas credenciais.

**§ 1º.** A conta de acesso (*login*) é o instrumento para identificação do usuário interno e colaborador na rede de comunicação ou sistemas específicos e caracteriza-se por ser pessoal e intransferível.

**§ 2º.** A senha de acesso é o instrumento de autenticação do usuário interno ou colaborador na rede de comunicação ou sistemas específicos que o qualifica como responsável por todos os acessos realizados através desta, salvo quando constatado e apurado incidente de segurança.

**Art. 30.** O acesso aos recursos de Tecnologia da Informação é condicionado em razão das funções desempenhadas pelo usuário interno ou colaborador, obedecendo o perfil do usuário e sua alocação, e liberado conforme as necessidades do TCE/MT.

**Art. 31.** A criação de credenciais de acesso deve ser realizada mediante solicitação formal da unidade de lotação do usuário interno ou colaborador à Coordenadoria de Gestão de Pessoas.

**Parágrafo único.** Para criação de credenciais de acesso, as solicitações devem conter, no mínimo, as seguintes informações:

**I.** Data da solicitação;

**II.** Tipo da solicitação (criação de conta, exclusão de conta, bloqueio de conta, desbloqueio de conta);

**III.** Recursos de Tecnologia da Informação liberados, com os níveis de acesso requeridos.

**Art. 32.** No caso de sistemas críticos, as solicitações, especificarão, ainda, além dos dias e horários em que estes serão acessados: Dados do solicitante; Matrícula; Unidade Administrativa; Cargo e Empresa (para prestadores de serviço).

**Art. 33.** As credenciais de acesso de prestadores de serviço devem especificar a data de validade da mesma, conforme período de vigência do contrato ou duração das atividades contratadas.

**Art. 34.** Consultorias que necessitem de acesso aos recursos de Tecnologia da Informação da Instituição, inclusive *internet*, terão autorização especial, com validade para o período de permanência, solicitada pelo Gestor da Unidade Administrativa contratante do serviço.

**Art. 35.** A nomenclatura da conta de primeiro acesso será padronizada pela Coordenadoria de Gestão de Pessoas, sendo que no momento da sua liberação ao respectivo usuário interno ou colaborador será fornecida pela Coordenadoria de Tecnologia da Informação uma senha temporária, obrigatoriamente alterada neste acesso.

**Art. 36.** As senhas de acesso aos recursos de Tecnologia da Informação, necessariamente, deverão ser alteradas em periodicidade não superior a 6 (seis) meses, vedada sua repetição, ou sempre que o usuário interno ou colaborador desejar.

**Parágrafo único.** Serão emitidos alertas após cada *logon* iniciando-se 14 (catorze) dias antes da data de expiração da senha.

**Art. 37.** As senhas devem ser compostas por, no mínimo 6 (seis) caracteres, preferencialmente mesclando letras e números, o que dificulta sua adivinhação por terceiros ou tentativas de ataques.

**Art. 38.** Não serão permitidas o uso de senhas "em branco" ou aquelas criadas em contrariedade às regras definidas.

**Art. 39.** As credenciais serão sumariamente bloqueadas após 5 (cinco) tentativas mal sucedidas de acesso, sendo seu desbloqueio condicionado a solicitação formal do usuário interno ou colaborador, descrevendo as circunstâncias do ocorrido para a Coordenadoria de Tecnologia da Informação, com ciência do líder da unidade administrativa.

**Parágrafo único.** Para o desbloqueio de uma credencial deverá ser adotado o procedimento disposto no art. 35.

**Art. 40.** As credenciais de acesso não utilizadas por um período de 60 (sessenta) dias serão automaticamente bloqueadas.

**Art. 41.** Em caso de afastamento prolongado, como férias e licenças, os usuários internos e colaboradores que fazem o uso dos recursos de tecnologia da informação críticos, providenciarão o bloqueio de suas credenciais junto à Coordenadoria de Gestão de Pessoas.

**Art. 42.** É vedado o acesso aos recursos de Tecnologia da Informação, inclusive *internet*, sem identificação e autenticação do usuário interno ou colaborador, bem como a utilização de credenciais de acesso em sessões de trabalho simultâneas.

**Art. 43.** A base de senhas deve ser armazenada com criptografia e nenhum usuário interno ou colaborador terá acesso ao seu arquivo, cabendo a Coordenadoria de Tecnologia da Informação, a cada 60 (sessenta) dias, verificar se há alguma conta fora dos padrões estabelecidos nesta norma e, imediatamente, providenciar a correção dos desvios encontrados.

**Art. 44.** Quando houver suspeita ou confirmação de quebra de sigilo de uma senha de acesso, esta deverá ser imediatamente alterada por seu detentor, notificando o ocorrido ao líder da unidade administrativa.

TÍTULO V

DOS CRITÉRIOS PARA A PREVENÇÃO CONTRA ACESSOS NÃO AUTORIZADOS ÀS INFORMAÇÕES, RECURSOS DE TECNOLOGIA E INSTALAÇÕES FÍSICAS DO TCE/MT

Seção I

Áreas de Segurança

**Art. 45.** As instalações da sala de *nobreak* e central de processamento e armazenamento de recursos de tecnologia da informação, indispensáveis para os serviços prestados pela Instituição, devem ser mantidas em áreas de segurança com permissões de acesso periodicamente revistas, de forma a impedir acessos não autorizados.

**Art. 46.** A sala de *nobreak* e da central de processamento e armazenamento de recursos de tecnologia da informação devem possuir sistema de alarme permanentemente ativo, além de sistema gravação de imagens, cujo arquivo será armazenado pelo prazo mínimo de 90 (noventa) dias.

**Art. 47.** Materiais combustíveis ou perigosos, equipamentos de contingência e mídias com cópias de segurança devem ser guardados de forma segura, a uma distância apropriada das áreas de segurança; e os suprimentos e materiais de expediente, somente serão armazenados nestes locais, quando devidamente requeridos.

**Art. 48.** Todo o trabalho realizado por colaboradores e terceiros deve ser supervisionado e registrado.

**Art. 49.** A utilização de equipamentos fotográficos, de vídeo, de áudio ou de qualquer outro equipamento de gravação deve ser formalmente autorizada.

**Art. 50.** A instalação elétrica, de cabeamento lógico e dos equipamentos de detecção e combate a incêndio devem ser feita de acordo com o especificado nas normas da ABNT.

**Art. 51.** É proibido o manuseio de alimentos e bebidas próximo a áreas de processamento, guarda e transporte de informação.

Seção II
Segurança nas Áreas de Trabalho

**Art. 52.** Os usuários internos e colaboradores devem zelar pela segurança das informações em sua área de trabalho, para tanto, adotando, ao menos, as seguintes cautelas:

**I.** Documentos e demais relatórios impressos, quando não utilizados, devem ser armazenados em gavetas ou armários, de forma a impedir seu conhecimento ou visualização por parte de pessoas alheias ao negócio;

**II.** Na hipótese em que se ausentar de sua estação de trabalho, esta deve ser bloqueada, com exigência de senha para posterior desbloqueio.

TÍTULO VI
DO PROCESSO DE IDENTIFICAÇÃO, MANUTENÇÃO, SUPORTE, HOMOLOGAÇÃO E TRANSPORTE DE ESTAÇÕES DE TRABALHO E EQUIPAMENTOS PORTÁTEIS

Seção I
Identificação e Controle

**Art. 53.** As estações de trabalho e equipamentos portáteis que sejam de propriedade do TCE/MT devem receber uma identificação única - etiqueta de patrimônio.

**Art. 54.** Os equipamentos de terceiros apenas poderão ser utilizados no processamento de informações no âmbito da rede corporativa da instituição, mediante requerimento do usuário ou colaborador externo à Secretaria de Gestão, que analisará em conjunto com a Coordenadoria de Tecnologia da Informação, a conveniência do uso dos mesmos.

**Art. 55.** A retirada, transferência ou substituição de estações de trabalho e equipamentos portáteis de propriedade do TCE/MT de suas alocações, deve ser previamente autorizada pela Coordenadoria de Tecnologia da Informação e informada ao Serviço de Material e Patrimônio.

**Art. 56.** Na hipótese da saída de qualquer estação de trabalho ou equipamento portátil de propriedade do TCE/MT das dependências da unidade administrativa onde se encontram alocados, excetuando os computadores portáteis que detenham responsabilidade e guarda individualizadas, deverá ser aberto correlato registro pelo Serviço de Material e Patrimônio.

**Art. 57.** Todas as estações de trabalho e equipamentos portáteis adquiridos devem ser vistoriados e homologados pela Coordenadoria de Tecnologia da Informação de acordo com as especificações técnicas do Edital de Compra, juntamente com o proposto pela empresa ganhadora do certame, e logo após a vistoria e aceite dos equipamentos, os mesmos devem ser encaminhados ao Serviço de Material e Patrimônio para tombamento.

**Art. 58.** A entrada de qualquer equipamento eletrônico excetuando os computadores portáteis de propriedade do TCE/MT, que o servidor detenha responsabilidade e guarda individualizadas nas dependências da instituição, deve ser registrada nas recepções da instituição, contendo o respectivo registro dos seguintes itens:

**I.** Nome do proprietário ou responsável pelo equipamento;

**II.** Descrição do equipamento;

**III.** Número de série;

**IV.** Marca e Modelo do equipamento;

**V.** Data e horário da entrada;

**VI.** Data e horário de saída;

**Art. 59.** As informações registradas quando da entrada, bem como as características do equipamento devem ser verificadas antes de ser autorizada à saída dos mesmos das dependências da instituição.

Seção II

Serviço de Material e Patrimônio

**Art. 60.** Todas as estações de trabalho e equipamentos portáteis que sejam de propriedade do TCE/MT, antes de serem disponibilizados para produção, devem ser inventariados pelo Serviço de Material e Patrimônio, unidade administrativa esta a quem competirá realizar o gerenciamento patrimonial dos mesmos.

**Art. 61.** Quaisquer incidentes ocorridos ou suspeitos com as estações de trabalho ou equipamentos portáteis inventariados devem ser registrados e comunicados a Secretaria de Gestão.

**Art. 62.** A unidade administrativa de Serviço de Material e Patrimônio deve comunicar a substituição ou transferência de qualquer equipamento inventariado ao seu responsável.

Seção III

Manutenção de Estações de trabalho e equipamentos portáteis

**Art. 63.** Toda solicitação de serviço referente à instalação, suporte e manutenção de estações de trabalho e/ou equipamentos portáteis deve ser registrada e destinada à Gerência de Suporte e Infraestrutura, que observará os respectivos períodos de garantia antes da realização de eventuais reparos.

**Parágrafo único.** O registro de solicitação/devolução de serviço/equipamento deve considerar os seguintes itens:

**I.** Nome do solicitante;
**II.** Unidade administrativa solicitante;
**III.** Descrição do equipamento;
**IV.** Número de Registro Patrimonial (RP)
**V.** Data e horário da abertura da solicitação;
**VI.** Data e horário do início do atendimento;
**VII.** Andamento da solicitação;
**VIII.** Data e horário do fechamento da solicitação;
**IX.** Data e horário do encerramento do atendimento;
**X.** Diagnóstico/Descrição do problema;
**XI.** Solução para o problema;
**XII.** Data prevista para entrega;
**XIII.** Assinatura do técnico responsável;
**XIV.** Assinatura do técnico que retirou o equipamento;
**XV.** Assinatura do técnico que devolveu o equipamento;
**XVI.** Assinatura do técnico responsável pelo serviço realizado;
**XVII.** Assinatura do usuário responsável pelo recebimento do equipamento.

**Art. 64.** Quando identificada a necessidade do envio de equipamento de informática para fora das instalações físicas do TCE/MT, com propósitos de manutenção ou substituição de periféricos de armazenamento de dados, as informações neles armazenadas, devem ser previamente removidas, e caso não seja possível, a Gerência de Suporte e Infraestrutura, implementará outros mecanismos que busquem garantir a confidencialidade e autenticidade das informações, tais como criptografia ou assinatura digital.

**Art. 65.** Procedimentos de manutenção física preventiva e de suporte das estações de trabalho e equipamentos portáteis devem ser implementados e periodicamente realizados por corpo técnico qualificado indicado pela Coordenadoria de Tecnologia da Informação.

Seção IV
Requisitos de Segurança

**Art. 66.** O transporte de equipamento de informática para fora das dependências do TCE/MT deve ser previamente comunicado ao Serviço de Material e Patrimônio, observando-se as especificações do fabricante.

**Art. 67.** As estações de trabalho e equipamentos portáteis devem possuir dispositivo contra variações de tensão da rede elétrica ou outras anomalias (*nobreak* ou estabilizador de tensão), que poderão ser utilizados individualmente nas máquinas ou na distribuição central da instalação elétrica.

**Art. 68.** Os equipamentos de informática devem possuir apenas conexões e dispositivos de conectividade necessários à sua finalidade, sendo os demais dispositivos que permitam conexão a redes não autorizadas, quer sejam internas ou externas ao TCE/MT, desabilitadas ou removidas.

**Art. 69.** No caso de *modems* ou dispositivos de conectividade não necessários, integrados à placa-mãe do equipamento, devem ser, sempre que necessário, desabilitados da BIOS.

**Art. 70.** A senha de proteção da configuração (*setup*) do equipamento de informática (CMOS) deve ser habilitada e devem ser do conhecimento apenas dos servidores indicados pelo líder da Gerência de Suporte e Infraestrutura do TCE/MT.

**Art. 71.** Medidas de segurança devem ser adotadas para evitarem que estações de trabalho e equipamentos portáteis fiquem expostos a vazamentos (distante de válvulas *sprinkler*, de canos de água ou gás), de calor excessivo (afastado de janelas onde haja incidência do sol), de campos eletromagnéticos (afastado de reatores), de quedas, e de outros agentes ameaçadores presentes no ambiente.

**Art. 72.** Deverão ser mantidos instalados nas estações de trabalho e equipamentos portáteis somente os *softwares* e sistemas necessários para o seu funcionamento.

**§ 1º.** A instalação de qualquer *software* necessário para o desenvolvimento das atividades no âmbito do TCE/MT deve ser homologada pela Coordenadoria de Tecnologia da Informação e atender ao contrato de licença de uso, ficando, terminantemente, proibidos de serem instalados aqueles sem licença de propriedade.

**§ 2º.** As estações de trabalho e equipamentos portáteis devem ser periodicamente inspecionadas pela Coordenadoria de Tecnologia de Informação, para verificar se os *softwares* e *hardwares* estão em consonância com a Política de Segurança da Informação do TCE/MT.

**Art. 73.** Devem ser removidos das estações de trabalho e equipamentos portáteis todos os softwares instalados sem autorização e ou não homologados pela Coordenadoria de Tecnologia da Informação;

**Art. 74.** Os procedimentos de instalação e configuração das estações de trabalho e equipamentos portáteis devem ser elaborados com documentação devidamente catalogada e mantida atualizada.

**Art. 75.** Todos os eventos envolvidos na instalação, configuração e manutenção dos equipamentos devem ser elaborados com o intuito de se evitar erros de operação, permitir a verificação de conformidade da configuração em relação as políticas de segurança adotadas e também facilitar a recuperação do sistema em caso de falhas de *software* ou *hardware*.

**Art. 76.** Ferramentas automatizadas devem, sempre que possível, ser utilizadas para padronização das configurações dos equipamentos.

**Art. 77.** Os *hardwares* e *softwares* dos equipamentos devem ser verificados com o intuito de garantir que sejam compatíveis com outros componentes de sistemas ou equipamentos existentes.

**Art. 78.** As estações de trabalho e equipamentos portáteis dos colaboradores e visitantes que necessitem obter acesso à rede corporativa do TCE/MT devem estar de acordo com os padrões de segurança.

**Art. 79.** A Gerência de Suporte de Sistemas configurará os equipamentos de acordo com os padrões seguidos pelo TCE/MT em conformidade com a Política de Segurança da Informação.

**Art. 80.** O processo de homologação e teste deve ser registrado, bem como os procedimentos e seus resultados acompanhados por um representante da unidade administrativa responsável pelo equipamento.

**Art. 81.** Os procedimentos de configuração de segurança das estações de trabalho e equipamentos portáteis devem ser documentados e mantidos atualizados, e, quando possível, os aparatos tecnológicos possuirão ferramentas de proteção contra *softwares* maliciosos, como antivírus, *firewall* pessoal.

Seção V
Equipamentos Portáteis

**Art. 82.** Os Equipamentos portáteis de propriedade do TCE/MT devem ser guardados em local seguro, com controle de acesso e garantia quanto à sua integridade e quando solicitado seu empréstimo, o solicitante deve responsabilizar-se pelo equipamento através da assinatura do Termo de Responsabilidade para Equipamento Portátil.

**§ 1º.** Antes de efetuar o empréstimo do equipamento, a área responsável pela sua guarda deve conferir a configuração de *hardware* e *software*, assim como atualizar e executar o antivírus.

**§ 2º.** Somente a equipe da Gerência de Suporte de Sistemas deve configurar os equipamentos portáteis para os usuários obterem acesso à rede corporativa do TCE/MT.

**Art. 83.** Na devolução do equipamento, o usuário e o responsável pela guarda devem conferir a configuração de *hardware* e *software*, assim como remover os arquivos manipulados pelo usuário.

**Art. 84.** Os equipamentos portáteis devem possuir ferramentas de bloqueio

e criptografia para sua proteção.

**Art. 85.** Deverá ser implementado procedimento para descarte seguro das informações armazenadas nos discos rígidos dos equipamentos portáteis antes da reutilização e do envio do mesmo para manutenção.

**Art. 86.** O equipamento portátil deve ser transportado pelo seu portador de forma que não desperte interesse de terceiros evitando furto ou roubo do equipamento e consequentemente das informações contidas no mesmo.

**Art. 87.** As informações institucionais armazenadas no disco rígido do equipamento portátil e periféricos devem ser protegidas por criptografia a fim de evitar acessos indevidos em caso de perda, roubo ou furto do equipamento.

## TÍTULO VII
## DAS NORMAS PARA O USO DO CORREIO ELETRÔNICO

**Art. 88.** As mensagens que apresentam o domínio "@tce.mt.gov.br" são consideradas documentos oficiais, sendo os usuários internos e colaboradores responsáveis pelo conteúdo das mensagens enviadas através de sua conta de correio eletrônico.

**Art. 89.** O TCE/MT, para fins de segurança e continuidade dos processos internos e serviços prestados pela Instituição, poderá rastrear mensagens e arquivos anexados das mensagens enviadas pelo correio eletrônico institucional.

**Art. 90.** A divulgação de informações da Instituição por meio do correio

eletrônico somente deve ocorrer se sua classificação permitir, preservando-se o grau de sigilo atribuído, conforme as regras insertas no art. 10 desta norma.

**Art. 91.** A criação de contas de correio eletrônico é realizada mediante solicitação, cuja respectiva nomenclatura deve ser padronizada pela Coordenadoria de Gestão de Pessoas.

**Art. 92.** Os usuários internos e colaboradores devem utilizar o correio eletrônico de forma a não prejudicar a continuidade dos serviços prestados pela Instituição e o trabalho de terceiros, não causar tráfego desnecessário na rede de comunicação e não sobrecarregar os sistemas de informações do TCE/MT.

**Art. 93.** O correio eletrônico deve ser utilizado para executar as funções relacionadas aos interesses do TCE/MT, todavia o uso pessoal ocasional é permitido quando não sobrecarrega os recursos de sistemas, não interfere com a produtividade dos usuários internos e colaboradores e não se enquadra como atividade não condizente à imagem da instituição, como por exemplo:

**I.** Envio de mensagens a um número indiscriminado de destinatários ou que possa ser caracterizado como prática de *spam*;

**II.** Envio de mensagens de conteúdo impróprio ao ambiente de trabalho, incluindo, mas não se restringindo a: materiais pornográficos, racistas, discriminatórios ou que incitem à violência;

**III.** Disseminação de mensagens do tipo corrente, campanhas de qualquer espécie ou atividades empresariais privadas.

**Art. 94.** O usuário interno ou colaborador não deve interceptar e/ou acessar

mensagens de correio eletrônico que tenham sido enviadas para outro usuário interno e colaborador, salvo que expressamente autorizado.

**Art. 95.** É proibido ocultar, suprimir, adulterar ou substituir a identificação do usuário interno ou colaborador das mensagens de correio eletrônico.

**Art. 96.** Em sendo incomodado por uma grande quantidade de mensagens de qualquer Instituição ou pessoa física, o usuário interno ou colaborador deve notificar o incidente de segurança para a Coordenadoria de Tecnologia da Informação para que sejam tomadas as ações pertinentes.

**Art. 97.** Deve ser evitado o envio de mensagens com arquivos em anexo, contudo, quando indispensáveis, o destinatário deve salvar os arquivos em sua pasta na rede, apagando-os do software de correio eletrônico, de maneira que o serviço não seja sobrecarregado.

**Art. 98.** O servidor de correio eletrônico deve ser configurado conforme critérios de segurança, inibindo o recebimento de arquivos executáveis ou quaisquer outros que possam conter *softwares* maliciosos com potencialidade de causar danos aos sistemas.

**Parágrafo único.** Todo arquivo texto, executável ou de dados que seja recebido via correio eletrônico deve ser analisado pelo *software* antivírus antes de ser utilizado.

**Art. 99.** Preferencialmente devem ser utilizados mecanismos que garantam a autenticidade das mensagens eletrônicas.

**Art. 100.** As mensagens devem ser escritas de maneira clara e concisa,

evitando-se parágrafos extensos, uso de maiúsculas ou de sinais de pontuação em exagero, observando-se ainda:

**I.** Os Assuntos (Subjects) devem ser claros e de acordo com o conteúdo da mensagem, para facilitar seu entendimento, recomendando-se manter o mesmo assunto em longas cadeias de respostas;

**II.** Durante o endereçamento de mensagens, recomenda-se atenção por parte dos usuários internos e colaboradores para que não sejam cometidos erros na escolha de destinatários;

**III.** O campo Para: (To) deve conter os endereços eletrônicos de pessoas das quais se espera alguma ação sobre o assunto em pauta;

**IV.** O campo Cc: (Com cópia) deve conter os endereços eletrônicos de pessoas que necessitem serem informadas sobre o assunto em pauta;

**V.** Evitar o uso do campo Cco: (Cópia Oculta), uma vez que este não permite a identificação do(s) destinatário(s) em questão por parte dos demais destinatários.

**Art. 101.** Deve ser evitado o envio de mensagens para um grande número de destinatários, sendo previstas exceções para as mensagens de comunicação ou avisos internos da Instituição.

**Art. 102.** A opção de confirmação de entrega e leitura de mensagens só deve ser utilizada em casos excepcionais, e com reserva.

**Art. 103.** O usuário interno ou colaborador deve informar à Coordenadoria de Tecnologia da Informação a ocorrência de qualquer incidente e potenciais ameaças à segurança da informação, inclusive mensagens de conteúdo impróprio.

## TÍTULO VIII

DAS NORMAS PARA O USO DA *INTERNET*

**Art. 104.** Toda e qualquer informação obtida única e exclusivamente através da *Internet* deve ser considerada suspeita, necessitando de confirmação por meio de fontes oficiais, tendo em vista a inexistência de processos de controle de qualidade e veracidade.

**Art. 105.** O TCE/MT não se responsabiliza pela segurança de transações eletrônicas, incluindo Comércio Eletrônico e *Internet Banking*, realizadas pelos usuários internos ou colaboradores por meio dos recursos de Tecnologia da Informação disponibilizados pela Instituição.

**Art. 106.** Os usuários internos ou colaboradores não devem fazer uso da *Internet* com o intuito de causar dano ao patrimônio da Instituição ou de terceiros.

**Art. 107.** O acesso à *Internet*, de terminal conectado à rede de comunicação do TCE/MT, deve ser realizado somente através desta, não sendo permitidas conexões por meio de placas, equipamentos de *fax-modem*, ou outras tecnologias móveis.

**Parágrafo único.** Exceções a regra constante no *caput* deste artigo, serão deliberadas pela Presidência, Corregedoria e Coordenadoria de Tecnologia de Informação.

**Art. 108.** Toda conexão à *Internet* passará por equipamentos de segurança garantindo o controle de acesso e a aplicação dos demais mecanismos de segurança aplicáveis.

**Art. 109.** O acesso a páginas não relacionadas aos processos internos ou serviços prestados pelo TCE/MT serão bloqueadas, sendo sua liberação condicionada à solicitação dos Líderes das Unidades Administrativas.

**Art. 110.** O acesso à *Internet* é condicionado a identificação e autenticação

do usuário interno ou colaborador.

**Art. 111.** O TCE/MT poderá monitorar os acessos às páginas da *Internet* com o intuito de identificar, bloquear e notificar formalmente os usuários internos ou colaboradores sobre as páginas com conteúdo impróprio para o ambiente de trabalho e casos detectados de queda de produtividade em função do uso abusivo desta ferramenta.

**Art. 112.** Não são autorizados acessos a páginas de conteúdo impróprio ao ambiente de trabalho, incluindo, mas não se restringindo a páginas de cunho erótico, racistas, discriminatórias e/ou que incitem à violência, bem como sites de redes sociais.

**Art. 113.** Os usuários internos ou colaboradores devem fechar as páginas *Internet* quando do término de pesquisas ou ausência prolongada de sua estação de trabalho, de forma que a performance dos recursos de Tecnologia da Informação não seja comprometida.

**Art. 114.** Não é permitida a conexão ou visualização de estações de rádio ou vídeos disponíveis na *Internet*, visto que estes recursos comprometem a performance dos recursos de Tecnologia da Informação.

**Art. 115.** Cópias de arquivos e/ou programas da *Internet* poderão ocorrer quando necessárias para o cumprimento das atividades de interesse do TCE/MT, proveniente de Instituições absolutamente seguras, mesmo assim, por cautela, deverão ser verificadas automaticamente quanto à presença de vírus eletrônico ou *software* malicioso.

**Parágrafo único.** Arquivos e/ou programas de interesse comum a várias

áreas do TCE/MT, poderão ser copiados pela Coordenadoria da Tecnologia da Informação que disponibilizará aos usuários internos e colaboradores via rede de comunicação.

**Art. 116.** Não é permitida a cópia de arquivos de música, vídeo ou jogos, instalação de programas do tipo *freeware* ou *shareware* nas estações de trabalho sem homologação e autorização formal da Coordenadoria de Tecnologia da Informação, como também a atualização de versão de programas licenciados pelo TCE/MT com arquivos oriundos da *Internet*.

**Art. 117.** Instalações de programas oferecidos quando do acesso a páginas *Internet* devem ser recusadas, uma vez que pode tratar-se de *softwares* maliciosos.

**Art. 118.** Os usuários internos e colaboradores, salvo se expressamente autorizados pela autoridade detentora de competência, não têm permissão para realizar alterações na página institucional do TCE/MT.

**Art. 119.** A Página institucional do TCE/MT deve possuir controles de segurança de forma a impedir a adulteração de seu conteúdo por *hackers* ou pessoas mal intencionadas, além de cópia de segurança arquivada em local distinto.

**Parágrafo único.** Os controles de segurança utilizados para a proteção da cópia da página institucional devem ser os mesmos adotados para a página principal.

**Art. 120.** Os recursos de Tecnologia da Informação que provêm serviços *Internet* devem ser dedicados e com acesso físico e lógico controlados, isolados da rede de comunicação interna.

**Art. 121.** Eventuais paralisações dos serviços de *Internet* para manutenção

preventiva deverão ser comunicadas com antecedência à Secretaria de Gestão e após a aprovação deverá ser divulgado à todas unidades gerenciais, para que a indisponibilidade deste recurso não afete a execução de processos internos ou serviços prestados pelo TCE/MT.

**Art. 122.** A Corregedoria poderá a qualquer tempo e sem aviso prévio, examinar os registros de acessos a *Internet* para verificação de atendimento à Política de Segurança da Informação, apuração de incidentes de segurança ou execução de demais atividades relacionadas à gestão da segurança corporativa.

**Art. 123.** Este Ato entra em vigor na data de sua publicação, revogando-se as disposições contrárias.

Participaram da votação os Senhores Conselheiros JOSÉ CARLOS NOVELLI, ALENCAR SOARES, WALDIR JÚLIO TEIS e DOMINGOS NETO.

Participaram, ainda, da votação o Auditor Substituto de Conselheiro LUIZ CARLOS PEREIRA, em substituição ao Conselheiro ANTONIO JOAQUIM, e o Auditor Substituto de Conselheiro LUIZ HENRIQUE LIMA, em substituição ao Conselheiro HUMBERTO BOSAIPO, conforme artigo 104, inciso I, da Resolução nº 14/2007.

Presente, representando o Ministério Público de Contas, o Procurador Geral Substituto Getúlio Velasco Moreira Filho.

**Publique-se.**

| | |
|---|---|
| **Processo** | **6.761-0/2011** |
| **Procedência** | **TRIBUNAL DE CONTAS DO ESTADO DE MATO GROSSO** |
| **Assunto** | **Dispõe sobre normas gerais para o manuseio de ativos de informação e recursos de tecnologia do Tribunal de Contas do Estado de Mato Grosso.** |
| **Relator Nato** | **Conselheiro Presidente VALTER ALBANO** |
| **Sessão de Julgamento** | **4-10-2011** |

**PROVIMENTO Nº 3/2011**

Sala das Sessões do Tribunal de Contas do Estado de Mato Grosso, Cuiabá, 4 de outubro de 2011.

CONSELHEIRO VALTER ALBANO
Presidente

GETÚLIO VELASCO MOREIRA FILHO
Procurador Geral Substituto