SEGURANÇA DA INFORMAÇÃO

NORMAS DE UTILIZAÇÃO DE RECURSOS COMPUTACIONAIS

1. Objetivo

Definir as políticas e diretrizes para o uso adequado dos recursos computacionais colocados à disposição dos usuários, minimizando os riscos associados a:

- Acesso não autorizado a sistemas e informações da empresa;
- Utilização para finalidades não permitidas;
- Utilização de software ilegal;
- Danos causados por vírus;
- Mau uso dos recursos computacionais.

2. Definição

Definem-se como recursos computacionais todos os sistemas, softwares, aplicativos, microcomputadores, equipamentos portáteis, impressoras, equipamentos de fax, telefones, periféricos, mídias magnéticas, redes de computadores, correio eletrônico, internet, enfim, todos os recursos e ferramentas de produtividade colocados à disposição dos usuários pela área de TI, com a finalidade única e exclusiva de ajudar a desenvolver as atividades de interesse da empresa.

3. Área de aplicação

Todas as unidades de negócio da Tecmesul, todos os colaboradores e pessoas físicas ou jurídicas que forem prestar serviço à empresa e, para tanto, se utilizam de recursos computacionais conectados à rede de computadores da empresa ou dos meios convencionais de processamento, comunicação e guarda de informações. Todos deverão assinar um dos modelos do termo de autorização, responsabilidade e confidencialidade.

4. Auditoria

Serão realizadas auditorias periódicas para verificação do grau de cumprimento desta política. A empresa, quando tiver razões empresariais legítimas, poderá estar monitorando e/ou registrando o envio/recebimento de mensagens do correio eletrônico, o acesso à navegação internet, aos sistemas aplicativos e aos softwares instalados nas estações de trabalho e equipamentos portáteis de qualquer usuário, respeitando a confidencialidade sobre o conteúdo dos itens auditados, mas dispensando, em razão da divulgação desta política, toda e qualquer notificação prévia ao emissor ou receptor da comunicação.

São consideradas razões empresariais legítimas, mas não se limitam a:

• Identificar e diagnosticar problemas de hardware e software;
• Prevenir o uso incorreto do sistema;
• Investigar conduta imprópria ou ilegal, atividade não ética ou inadequada;
• Assegurar conformidade com os direitos de propriedade, licenças e obrigações contratuais;
• Proteger os interesses empresariais da organização.

Qualquer irregularidade ou divergência em relação a esta norma deve imediatamente ser comunicada à área de TI, que tomará as medidas cabíveis para regularizar a situação.

5. Penalidades

O não-cumprimento deste padrão é considerado falta grave, sujeitando o infrator a uma ação disciplinar apropriada, conforme normas de sanções disciplinares adotadas pela empresa.

6. Disposições gerais

6.1. Software

6.1.1. Somente é permitida a utilização de cópias de software legal e que tenham passado pelo processo de homologação da área de TI.

6.1.2. O usuário não deve adquirir, instalar ou substituir qualquer software sem a devida autorização da área de TI.

6.1.3. As necessidades de software devem ser submetidas à área de TI, que efetuará um estudo de viabilidade da aquisição e homologação dos mesmos, como forma de garantir sua adesão aos padrões e à política de segurança da empresa.

6.1.4. Toda contratação de serviços de informática, tais como treinamento, desenvolvimento e consultoria, deve ser submetida à apreciação prévia da área de TI, que deverá providenciar uma análise custo/benefício para aprovação da diretoria da área.

6.1.5. Não é permitida a duplicação, empréstimo, transferência ou retirada de software para outros equipamentos, dentro ou fora da empresa.

6.1.6. Não é permitido o uso de jogos e protetores de tela (exceto os do windows ou distribuídos pela empresa). A utilização de programas de licença gratuita (freewares), de validade temporária (sharewares) ou fornecidos como demonstração (demos), só poderá ser feita em casos de comprovada necessidade do uso, de forma legal e suportada por autorização formal do diretor da área e da área de TI, desde que não haja programas para a mesma finalidade já adquiridos ou homologados pela empresa.

6.1.7. Para nenhum fim é permitido ao usuário à utilização de programas não autorizados que afetem a segurança da informação, tais como: programas para descobrir senhas, rastrear portas e acessos, rastreamento de teclados, cavalos de tróia, vírus, ferramentas utilizadas por hackers, etc.

6.1.8. Irregularidades ou divergências encontradas em softwares adquiridos antes da publicação deste padrão devem ser comunicadas à área de TI, que providenciará a regularização.

6.2. Hardware

6.2.1. O usuário é responsável direto pela conservação, guarda e utilização dos equipamentos mantidos à sua disposição.

6.2.2. Os equipamentos portáteis (notebooks, laptops, palmtops) devem ser mantidos pelos usuários em lugar seguro, com especial atenção contra roubos, avarias ou uso não autorizado de terceiros. Orientações sobre os cuidados que devem ser tomados na utilização de equipamentos portáteis deverão ser distribuídas para todos os usuários destes equipamentos pela área de TI.

6.2.3. As necessidades de hardware, bem como as expansões da infra-estrutura de informática (redes, servidores, novas tecnologias), devem ser submetidas à área de TI, que efetuará um estudo de viabilidade da aquisição e homologação dos mesmos, como forma de garantir sua aderência aos padrões e à política de segurança da empresa.

6.2.5. Não será permitido que micros conectados à rede tenham modens ativados. A instalação de modem deve ser restrita aos casos de comprovada necessidade e suportados por autorização formal do diretor da área. Sua utilização será permitida apenas quando o micro estiver desconectado da rede.

6.2.6. É vedada ao usuário a abertura ou tentativa de qualquer tipo de manutenção nos equipamentos.

6.2.7. Sempre que possível, antes do envio de equipamento para manutenção, venda ou doação, as informações neles contidas devem ser removidas.

6.3. Senhas

6.3.1. As senhas de acesso à rede, ao correio e aos sistemas deverão ser do conhecimento e uso exclusivo de cada usuário.

6.3.2. Nenhum usuário deverá tomar conhecimento de senhas de outros usuários, seja por meio de software, digitação ou qualquer outro meio.

6.3.3. O tamanho, as regras de formação e a periodicidade de troca das senhas devem obedecer às normas e recomendações definidas pela área de TI e publicadas na intranet.

6.3.4. O usuário deverá utilizar proteção de tela com senha, devendo acionar este recurso toda vez que se afastar do micro.

6.3.5. Os usuários de equipamentos portáteis e micros com unidades de disquete ou CD-ROM habilitados devem utilizar senha de acesso na inicialização de tais equipamentos.

6.3.6. Devem-se utilizar senhas de proteção em arquivos com informações de natureza altamente confidencial.

6.3.7. A senha de setup dos equipamentos deve ser de conhecimento exclusivo da área de TI.

6.4. Internet/correio eletrônico

6.4.1. O acesso aos serviços de internet e correio eletrônico, através dos micros conectados à rede, destina-se prioritariamente para fins de interesse da empresa, apenas para os usuários que possuírem autorização formal do gerente da área. O uso moderado, ocasional e responsável destes recursos para fins particulares é tolerado, desde que não interfira nas atividades profissionais do usuário e não comprometa o desempenho e a disponibilidade de tais recursos.

6.4.2. No uso dos serviços de internet e correio eletrônico, não é permitido o acesso, a baixa (download), a carga (upload), a armazenagem, o recebimento, o envio e a retransmissão de material (comunicação, arquivo, mensagem, etc.) Que possa ser considerado por qualquer pessoa como discriminatória, obscena, ilegal ou ofensiva, ou que tenha qualquer informação considerada confidencial ou de uso restrito dentro da empresa.

6.4.3. A baixa de software deve ser submetida à área de TI, para assegurar a não exposição da empresa a processos de utilização indevida.

6.4.4. Não é permitida a transmissão ou retransmissão de propagandas, de boatos, "correntes" ou coisas do gênero, bem como mensagens que contenham documentos anexos de remetentes desconhecidos.

6.4.5. Se houver necessidade de distribuir mensagens para grandes grupos de usuários e/ou arquivos de grande volume, deve-se estudar juntamente com a área de TI formas que não prejudiquem o tráfego da rede.

6.4.6. Não devem ser colocadas imagens contendo assinaturas nos documentos que circulam na intranet, internet ou no correio eletrônico.

6.4.7. O usuário deve estar ciente de que a empresa reserva-se o direito de monitorar a utilização e inibir o mau uso destes recursos.

6.5. Backup e guarda de dados na rede

6.5.1. Os documentos da empresa devem ser armazenados nos servidores da rede.

6.5.2. É responsabilidade da área de TI a guarda, segurança e o backup dos arquivos contidos nos servidores de rede.

6.5.3. É responsabilidade do usuário a guarda, segurança e o backup dos arquivos contidos em seu equipamento.

6.5.4. Os usuários de equipamentos portáteis devem providenciar cópias de segurança (backups) dos seus arquivos em unidades de disco (drives) da rede.

6.5.5. O usuário deverá utilizar racionalmente o espaço em disco reservado para seu setor, mantendo rotinas freqüentes de remoção de arquivos não mais utilizados e tendo sempre em mente que o espaço em disco é um recurso esgotável com alto custo de manutenção.

6.6. Antivírus

6.6.1. A área de TI irá instalar e manter atualizada a versão do antivírus nos equipamentos, orientando os usuários sobre as providências a serem tomadas em casos de contaminação.

6.6.2. Usuários devem manter o antivírus ativo e residente, notificando qualquer anormalidade à área de TI e ao usuário que enviou o arquivo infectado.

6.6.3. Todos os arquivos recebidos, provenientes de qualquer mídia, não importando sua origem, devem passar por um processo de verificação de vírus antes de sua utilização.

6.7. Políticas de rede (policies)

6.7.1. O usuário deverá sempre permitir que as políticas definidas para o seu perfil sejam implantadas em seu micro durante o processo de log on na rede, não devendo alterar quaisquer características/restrições impostas por tais políticas, sem autorização formal da área de TI.