

## INSTRUÇÃO NORMATIVA

N.º 002/2014

*Criação da Política do Uso das  
Tecnologias de Informação do  
SESI/RR.*

### POLÍTICA DE USO DAS TECNOLOGIAS DE INFORMAÇÃO

#### 1. DISPOSIÇÕES GERAIS

A Política do Uso das Tecnologias de Informação é um documento em que se formalizam as regras de conduta e gestão, quanto ao acesso e utilização dos Sistemas de Tecnologia da Informação, seja na forma da utilização dos equipamentos de informática, no acesso a sistemas e informações da Entidade, além de definir regras e parâmetros operacionais para utilização do parque de informática e sistemas disponíveis, estabelecendo critérios para sua administração, visando uma padronização dos métodos utilizados, controle e eficiência no atendimento de solicitações, bem como na manutenção da estrutura de segurança desse sistema.

#### 2. OBJETIVOS

- Assegurar melhores resultados para a Entidade e usuários do sistema de informática;
- Otimizar, preservar e resguardar a Entidade de eventual uso indevido dos recursos de informática;
- Estabelecer referencial para orientar às ações referentes ao Uso das Tecnologias de Informação, a fim de reduzir riscos, garantir a integridade, o sigilo e a disponibilidade do Sistema de Tecnologia da Informação;
- Disciplinar o uso da Internet, Intranet, segurança de dados em rede, a rastreabilidade dos arquivos, armazenamento das informações e a utilização dos equipamentos;
- Definir uma política de segurança visando à proteção às informações e equipamentos desta Entidade, estabelecendo parâmetros para a correta e segura utilização do parque de Informática por parte dos usuários, sejam eles, colaboradores, prestadores de serviço, estagiários e clientes;



- Estabelecer critérios e prioridades no que tange a informação, orientando sobre as necessidades de informação necessárias para manutenção e preservação dentro da instituição.

### 3. TERMINOLOGIAS

Para efeitos da presente Política, no tocante às regras e diretrizes, são consideradas as seguintes terminologias:

**SESI-RR** – No Serviço Social da Indústria - Departamento Regional de Roraima, inclui-se o Centro de Atividades do Trabalhador Senador Fernando Bezerra (CAT), o Centro de Educação do Trabalhador João Mendonça Furtado (CET), a Unidade Indústria do Conhecimento (Praça Mané Garrincha) e o Centro de Atividades do Trabalhador Waldir Peccini (Distrito Industrial).

**Hardware** – Toda e qualquer parte física do microcomputador, incluindo seus componentes internos, tais como processador, memórias, unidades de disco fixo, leitores / gravadores de CD / DVD, ou de seus periféricos, como monitores, teclado, mouse, impressoras, scanners, *nobreaks*, estabilizadores e outros. Também se incluem nesta definição computadores portáteis (*notebooks*), equipamentos de rede, de projeção, palm tops, servidores e discos removíveis (cartões de memória e *pendrives*).

**Software** - É todo e qualquer programa de computador, isto é, a parte lógica do computador. São as instruções e programas, bem como os dados a eles associados, empregados durante a utilização do sistema.

**Estação de Trabalho** – Microcomputador, composto pelo Hardware e Software disponibilizados pelo SESI-RR a seus usuários.

**Usuários** – Colaborador, estagiário, prestador de serviço que atende nas instalações do SESI-RR, temporários, instrutores, alunos, clientes e demais pessoas autorizadas a utilizar a rede e/ou os equipamentos de informática do SESI-RR.

**Rede Corporativa de Computadores** - Conjunto de computadores conectados, permitindo a troca de dados e informações entre eles.

**Internet** - Rede mundial de computadores que interliga usuários a empresas, governos, escolas, agência, universidades e outros indivíduos, permitindo a comunicação, disseminação e compartilhamento de informações entre computadores.

**Intranet** - Rede privada ligando computadores locais, usada por determinada instituição / empresa para o compartilhamento de informações entre profissionais e setores, e que também permite acesso a Internet.

**Correio Eletrônico** - Sistema que permite ao usuário enviar mensagens instantâneas por meio de um computador, para uma ou mais pessoas, em qualquer lugar por meio da Internet ou da Intranet. Pode ser referido como *e-mail*.

**Site** - Palavra em inglês que significa local, lugar. Na Internet, designa um conjunto de páginas que representam uma pessoa, instituição ou empresa na rede.

**Download** - Consiste em fazer uma cópia de arquivo hospedado na rede para o seu computador pessoal.

**Conta Nomeada** - Conta de acesso ao correio eletrônico disponibilizada pelo SESI-RR para o usuário, que lhe permite acessar os recursos de correio eletrônico, enviando e recebendo mensagens.

**Conta setorial** - Conta de acesso à rede de dados disponibilizada pelo SESI-RR para um grupo de usuários, que permite o acesso, por meio desta conta, aos recursos e serviços de informática disponibilizados.

**Sistema Operacional** - É um software responsável por controlar todas as atividades internas de um conjunto de programas e sua interação com o Hardware. Ele gerencia os aplicativos, reconhece periféricos e administra o compartilhamento das informações em uma rede. Ex: Windows, Linux.

**Ocomon** - É o Sistema de Gerenciamento de Chamados utilizado pelo SESI-RR para solicitação e agendamento de eventos e manutenção de equipamentos.

**Integrator** - Sistema de Gestão de Serviços, utilizado pelo SESI-RR, para controle das informações de aquisição de produtos e serviços, controle de estoque, gerenciamento de atendimentos nas áreas de Saúde, Lazer e Educação.

**BRMA** - Sistema que disponibiliza acesso controlado à Internet, mediante informação da conta setorial, para fins de registro e log (arquivo de registro do sistema).

**Servidor de Arquivos** - Pasta compartilhada no servidor e mapeada nas estações, para fins de compartilhamento de arquivos na rede SESI-RR.

#### **4. DA PROPRIEDADE**

Todos os hardwares, softwares e periféricos de informática, bem como as informações geradas, trabalhadas ou transformadas pelos usuários, por meio

dos recursos computacionais do SESI-RR, é considerada propriedade desta instituição, não devendo ser compartilhada ou utilizada, para quaisquer outros fins externos ao ambiente corporativo, salvo com autorização da Alta Direção.

## 5. DO HARDWARE E DOS SOFTWARES

a) Todos os recursos de Informática a serem adquiridos pela entidade, serão autorizados pela Alta Direção, após análise técnica do Setor de T.I. em conjunto com a área solicitante, para verificação da efetiva necessidade de aquisição e compatibilidade com recursos já existentes;

b) Cabe ao usuário zelar pelos equipamentos que utiliza, não sendo permitida qualquer remoção, desconexão de partes, substituição ou qualquer alteração nas características físicas ou técnicas dos equipamentos integrantes da rede, salvo as executadas pelo Setor de T.I.;

c) Todos os softwares a serem instalados para uso da entidade devem, obrigatoriamente, ter passado por processo de licenciamento de uso e aquisição regulamentar, sendo vedado o uso de qualquer software não-licenciado, por parte de qualquer usuário;

d) O SESI-RR disponibilizará em cada estação de trabalho, um conjunto básico de softwares que ficarão sob a responsabilidade do(s) usuário(s) que os utilizam, não sendo permitida a remoção, alteração de configurações, atualização de versão ou a utilização de software similar ao do conjunto básico, salvo se estes procedimentos forem executados pelo Setor de TI, com expressa autorização da Alta Direção. Os softwares básicos são compostos por um sistema operacional de uso difundido, um navegador para uso da Internet, um processador de textos, uma planilha eletrônica e um programa antivírus, além de softwares específicos correlatos às funções da própria unidade do setor;

e) A instalação de outros softwares diferentes do conjunto básico de cada estação de trabalho é permitida, de acordo com a necessidade específica do usuário, e autorização da Direção da DITECOM, ficando a cargo do Setor de TI a instalação e controle destes softwares;

f) O SESI-RR poderá adotar o uso de softwares “livres” - assim designados àqueles que possuam o código fonte aberto e cujo uso não enseja o pagamento de licenças de uso. Tais softwares são desenvolvidos de acordo com a política de Software Livre, observadas as condições legais de utilização estabelecidas por seu desenvolvedor - em qualquer área, desde que autorizados pela Direção da DITECOM, seguindo padrão indicado pelo Setor de TI;



g) A nenhum usuário dos recursos de informática do SESI-RR é permitido realizar instalações de software, sem a anuência previa da Alta Direção e parecer técnico favorável do Setor de TI. Estão enquadrados posição nesta disposição: os aplicativos proprietários, desenvolvidos especificamente por programadores contratados; os softwares e aplicativos de propriedade do usuário; os softwares obtidos na internet através de *download*, promoções realizadas em feiras, revistas e aqueles distribuídos sob título de demonstração, que atendam as diretivas de licenciamento como “*freeware*”, “*trial*”, “*shareware*”, “*demo*”, ou outra equivalente;

h) Nos casos em que se verifique a instalação de software não autorizado, o Setor de TI deverá comunicar a chefia imediata, para que sejam adotadas as medidas cabíveis;

i) O setor de Tecnologia da Informação tem sob sua responsabilidade a verificação da atualização do programa antivírus de todo o parque tecnológico da entidade, gerenciada por rotinas definidas pelo servidor de antivírus;

j) Cada estação de trabalho contará com uma unidade particionada no disco rígido, designada unidade “D:”, destinada ao armazenamento temporário de arquivos e informações relevantes aos processos desenvolvidos pelo setor;

j.1) A unidade “D:”, não é contemplada pela política de Backup, devendo os arquivos relevantes e necessários ao desenvolvimento das atividades do setor serem armazenados em local adequado, conforme descrito na sessões 8. *DA DEFINIÇÃO DE DOCUMENTOS PROTEGIDOS* e 9. *DA UTILIZAÇÃO DO SERVIDOR DE ARQUIVOS, E POLITICA DE BACKUP* deste manual;

k) Os equipamentos de hardware e software deverão ser manipulados apenas por colaboradores e pessoal autorizado pelo SESI-RR.

## **6. DAS SENHAS SETORIAIS, NOMEADAS E DE SISTEMAS CORPORATIVOS**

a) Para a criação das senhas setoriais a Unidade/Setor deverão realizar solicitação ao setor de T.I., que procederá de imediato a criação da conta setorial e senha provisória de acesso;

a.1) A alteração da senha provisória para a definitiva só poderá ser realizada pelo coordenador/gestor junto ao setor de T.I., resguardando-se a sua confidencialidade;

a.2) A responsabilidade sobre o uso e a confidencialidade destas senhas fica a cargo dos seus usuários;

b) A solicitação de criação de toda e qualquer senha de acesso a Sistemas Corporativos – Ocomon, Integrator, Correio Eletrônico e qualquer outro que



venha a ser utilizado pela instituição - deve ser formalizada pela chefia imediata ao Setor de TI, via Ocomon, memorando ou email institucional, informando os seguintes dados do usuário: nome completo, número de matrícula e cargo/ função;

b.1) Quando da criação das contas de acesso à rede e aos sistemas corporativos, são atribuídas senhas padronizadas pelo Setor de TI, que deverão ser alteradas pelo usuário no primeiro acesso;

b.2) Recomenda-se, por motivos de segurança, que as senhas de acesso a rede seja alteradas a cada 60 dias;

c) O armazenamento e controle de senhas de acesso a sistemas corporativos externos (SMD, SCAE, SAPF, entre outros), email's setoriais, e quaisquer outras que sejam necessárias devem ser realizados pela Coordenação de Área, em conjunto com o Setor de TI, através de software específico a ser disponibilizado nas estações de trabalho das coordenações de área, e nas demais estações indicadas por esta coordenação;

c.1) A proteção das informações se dá através de uma única senha MASTER para acesso ao banco de dados de senhas armazenadas. Esta senha MASTER poderá ser compartilhada de acordo com a necessidade da coordenação;

d) Quando da ocorrência de desligamento do colaborador da instituição, o Setor de TI deverá ser imediatamente informado pelo DAF-DDH, para que sua conta nomeada, contas de sistemas corporativos internos ou externos sejam imediatamente bloqueadas, e sua conta de email tenha a senha alterada, a fim de que não hajam acessos indevidos, visando evitar riscos de segurança das informações institucionais;

d.1) A conta de e-mail vai permanecer ativa e disponível, com senha em responsabilidade da coordenação de área a qual pertencia o colaborador, por período de 90 dias, para que sejam efetuadas as consultas necessárias. Após este período, a coordenação será novamente consultada pelo setor de TI, a respeito da exclusão definitiva da conta de e-mail;

e) Ao se afastar de sua estação de trabalho, devem ser tomadas, por parte do colaborador, medidas para evitar o acesso não autorizado de terceiros ao conteúdo de seu microcomputador, ambiente de rede e sistemas corporativos, efetuando *logoff* das aplicações utilizadas ou o bloqueio da estação. No caso de conta setorial, esta responsabilidade se estende a todos os usuários desta conta;

f) Para fins de segurança, e evitar o acesso indevido as estações de trabalho e sistemas, será aplicado recurso para que a estação de trabalho seja bloqueada automaticamente após período de inatividade, que pode variar de

acordo com a atividade exercida em cada setor. O desbloqueio somente será efetuado ao informar a senha do colaborador, ou do Administrador do sistema;

f.1.) O período de inatividade antes do bloqueio de cada estação de trabalho pode ser alterado a qualquer tempo, desde que solicitado pela chefia imediata de cada setor;

f.2.) O setor de Tecnologia da Informação manterá o controle das informações referentes ao perfil de bloqueio definido conforme os procedimentos acima citados.

## **7. DO ACESSO A REDE CORPORATIVA, INTRANET E BANCO DE DADOS**

a) O acesso a informações e recursos da rede corporativa de computadores, bem como Aplicações Corporativas em Banco de Dados e Intranet, só é permitido aos usuários que possuem contas de acesso nomeadas ou setoriais, com suas respectivas senhas, as quais possuem diferentes níveis de acesso;

a.1) Para o caso de visitantes, palestrantes, parceiros, fornecedores e pessoal terceirizado, que façam uso de equipamento próprio, os mesmos só poderão dispor de acesso à rede local mediante solicitação aprovada pelo setor ou UER ao qual estejam vinculados, e após a verificação dos critérios de segurança por parte do setor de TI (instalação de antivírus, Firewall ativado);

a.2) Para estes, o acesso exclusivo a Internet através da rede Wireless pode ser disponibilizado mediante fornecimento de senha apropriadas para conexão a esta, configurada para o evento específico, fornecida pelo Setor de TI mediante solicitação aprovada pelo setor ou UER ao qual estejam vinculados;

b) O acesso às Aplicações Corporativas em Banco de Dados do SESI-RR, se dá unicamente através de conta setorial / nomeada, devendo os usuários restringir o seu uso para fins unicamente profissionais, respeitando os perfis de acesso, o sigilo das senhas e informações, bem como o correto uso dos sistemas;

c) É de responsabilidade do Setor de TI o cadastramento de senhas de acesso setoriais, bem como a alteração ou cancelamento das mesmas, quando solicitado pelas chefias imediatas ou nos casos de desligamento dos colaboradores. É vedado ao usuário de qualquer senha de acesso setorial efetuar sua alteração. Toda e qualquer alteração deve ser efetuada somente pela coordenação ou gestores responsáveis pela manutenção da conta nomeada, ou pelo Setor de TI.



## **7.1 DA UTILIZAÇÃO DA INTRANET E INTERNET**

a) Os serviços de acesso à Internet e Intranet do SESI-RR (WWW, FTP, Correio Eletrônico, entre outros) estão disponíveis para os usuários como ferramenta de trabalho, devendo sua utilização guardar estrita relação com as atividades desenvolvidas no DR, bem como estar em pleno acordo com as práticas profissionais adequadas ao Regional;

b) Não serão aceitos atos de hostilidade ou pirataria eletrônica, que venham ou não a alterar, destruir ou violar informações e recursos da Intranet / Internet;

c) Configuram uso indevido da internet o acesso a sites que contenham material pornográfico e assemelhados; jogos de azar; programas de busca e download de músicas, vídeos e softwares, exceto aqueles destinados a trabalhos específicos da área; sites de relacionamento virtual (tais como Orkut, Facebook, Twitter, entre outros), exceto para fins específicos definidos por projeto em desenvolvimento aprovado pela Alta Direção (o mesmo se aplica aos sites de compra); sites de conteúdo ilegal ou não ético; sites com conteúdo que seja ofensivo ou cause molestamento ou tormento; sites com conteúdo racista ou preconceituoso; sites de entretenimento e os que contenham outras atividades que possam afetar de forma negativa o DR/RR, seus clientes, colaboradores, fornecedores e parceiros;

d) Para fins de controle e segurança, todo acesso a Internet é monitorado via sistema denominado BRMA, sendo que um registro das atividades do usuário é mantido, podendo ser consultado e as devidas medidas administrativas tomadas, em caso do não cumprimento das normas aqui descritas, tendo como referência o Regulamento de Pessoal do SESI-RR;

e) A realização de baixa/installação (downloads) de programas (softwares) deverá ser feita conforme a política de software definida pelo SESI-RR no item 5. *DO HARDWARE E DOS SOFTWARES*, conforme citado nesta Instrução Normativa;

f) As informações corporativas, que se referem a clientes, colaboradores, fornecedores, parceiros, serviços, projetos, atividades ou ações de qualquer natureza ou formato no âmbito institucional, não devem ser disponibilizadas na Intranet, internet ou enviadas por qualquer ferramenta de comunicação ou sistemas de compartilhamento e envio de arquivos, sem a expressa autorização da chefia imediata ou Alta Direção.

## **7.2 DA UTILIZAÇÃO DO CORREIO ELETRÔNICO**



- a) O uso de correio eletrônico, correio de voz ou qualquer outra forma corporativa de comunicação eletrônica de mensagens deve ser voltado para a condução dos negócios do SESI-RR, e é restrito aos usuários cadastrados. O conteúdo das caixas postais dos usuários, por se tratar de ferramenta de comunicação institucional, são consideradas de propriedade do SESI-RR;
- b) O SESI-RR respeita a privacidade e os direitos dos colaboradores na utilização do correio eletrônico, porém se reserva o direito de preservar o uso adequado do sistema, a fim de resguardar a integridade das informações e manter o seu gerenciamento, podendo exercer fiscalização com fins de auditoria, inclusive para efeito de apuração de eventual uso indevido;
- c) O usuário fica ciente de que a senha de acesso ao correio eletrônico é pessoal e intransferível, devendo zelar pela mesma de forma responsável, garantindo o sigilo de sua senha de acesso, trocando-a obrigatoriamente por ocasião da primeira utilização, e após, periodicamente, a cada 3 (três) meses. O usuário é responsável por qualquer uso indevido de sua conta e senha, mesmo que por terceiros, quando do não cumprimento das orientações de segurança estabelecidas neste documento;
- d) Configura uso indevido do correio eletrônico a tentativa de acesso não autorizado às caixas postais de terceiros; o envio de informações corporativas e institucionais, inclusive senhas, para pessoas ou organizações não autorizadas; a remessa de material obsceno, pornográfico ou de pedofilia, ilegal ou não ético; materiais que sejam ofensivos ou causem moléstia, comerciais, pessoais, de propaganda, mensagens do tipo corrente e de entretenimento, e outras atividades que possam afetar de forma negativa a imagem do SESI-RR ou de seus clientes, colaboradores, fornecedores e parceiros;
- e) O uso do correio eletrônico corporativo, em qualquer de suas formas, deve ser orientado para as atividades do SESI-RR ou para atividades que promovam o desenvolvimento profissional de seus colaboradores, devendo ser usado de forma eficiente, eficaz, obedecidos os critérios éticos e legais, bem como a observância dos itens descritos esta norma;
- f) Nenhum anexo de mensagem de correio eletrônico deve ser aberto caso a origem desta mensagem seja desconhecida, o mesmo ocorrendo com os *link's* apresentados nas mensagens, a fim de preservar a integridade da rede corporativa de computadores, já que elas podem conter código malicioso e não seguro;
- g) Para o caso de mensagens recebidas de origem conhecida, não devem ser abertos anexos de origem duvidosa, que possam trazer códigos maliciosos, vírus, *spywares* (softwares espiões), *trojans* (cavalo de tróia) ou *link's* apresentados nas mensagens. Para tal efeito, consideram-se anexos seguros

somente os arquivos originados por processadores de texto, planilha eletrônica, apresentações e arquivos de imagens devidamente anexados, não devendo ser acessados *link's* que direcionem para tais arquivos. Qualquer outro tipo de arquivo deve ser submetido ao Setor de TI para análise de seu risco potencial.

## 8. DA DEFINIÇÃO DE DOCUMENTOS CRÍTICOS PROTEGIDOS

São considerados documentos críticos ao desenvolvimento das atividades do setor, e dessa forma, protegidos pela política de backup:

- Atas;
- Relatórios;
- Planilhas de cálculo;
- Ofícios / Cartas;
- Memorandos;
- Editais;
- Documentos Normativos;
- Quaisquer documentos referentes a processos de prestação de contas;
- Apresentações;
- Laudos;
- Parecer Técnico;
- Projetos;
- Minutas;
- Contratos;
- Requerimentos;
- Documentos que contenham informações referentes a clientes e/ou serviços prestados pela instituição;
- Demais documentos cujas informações sejam consideradas críticas para os setores.

Somente os arquivos de fotos e vídeos referentes ao acervo institucional sob responsabilidade da ASCOM serão protegidos pelas rotinas de backup, não sendo considerados críticos para os processos os arquivos desta natureza armazenados nas estações de trabalho dos setores.

Não devem ser armazenados nos microcomputadores do SESI-RR, de nenhuma forma, arquivos de uso pessoal, sem relação com a atividade ou função desempenhada pelo colaborador, seja na estação de trabalho, ou na pasta Setores.

## 9. DA UTILIZAÇÃO DO SERVIDOR DE ARQUIVOS, E DA SEGURANÇA DA INFORMAÇÃO

a) sistema de compartilhamento de arquivos foi estruturado no servidor local de nome “Sesi\_Master”, em pasta compartilhada denominada “Setores”. Esta pasta compartilhada está disponível para acesso a instituição, e sua estrutura interna foi elaborada através da criação de pastas denominadas “setoriais”, cuja nomenclatura coincide com a área a qual atendem, e outras pastas de uso específico para realização de determinados processos;

b) As pastas setoriais são de uso exclusivo a área a qual se destinam, ficando o acesso às informações restrito e protegido de uso indevido por colaboradores de outras áreas. Apenas as coordenações de área e a Alta Direção tem acesso a conteúdo a pastas das demais áreas;

c) A estrutura interna de cada pasta setorial deve refletir, na medida do possível e de acordo com as necessidades da área, a estrutura organizacional da mesma, separando projetos e setores em pastas específicas, e aplicadas às devidas políticas de restrição de acesso, podendo negar acesso a pasta, liberar acesso para somente leitura (consulta), ou acesso para leitura e alteração dos arquivos ali existentes;

c.1 Cabe a Coordenação de Área definir as necessidades e a política de acesso às pastas, sua criação, exclusão ou alteração, podendo essa ser personalizada conforme a necessidade de cada setor;

c.2 Cabe ao Setor de TI aplicar as políticas de acesso definidas pela Coordenação de Área;

c.3 A restrição de acesso às pastas setoriais se dá através da conta nomeada / setorial utilizada pelo colaborador;

d) A transferência de arquivos entre áreas deve ser feita através da pasta de acesso livre chamada “Temporária”. Os arquivos armazenados nesta pasta somente serão mantidos por 7 (sete) dias, sendo automaticamente deletados após este período;

e) Somente devem ser armazenados no servidor de arquivos, nas pastas referentes a cada área, os arquivos considerados “Importantes”, conforme listado no item 8 desta normativa;

e.1) Documentos considerados de “Baixa Criticidade” podem ser armazenados no servidor de arquivos, se necessários ao desenvolvimento de atividades, projetos ou registro, desde que seja feito nas pastas especificamente criadas para esta finalidade;

f) Quanto às demais pastas localizadas no compartilhamento ‘Setores’, foram disponibilizadas com a seguinte estrutura:

f.1) A pasta “Músicas e Vídeos” foi disponibilizada para que sejam armazenados os respectivos arquivos, desde que os mesmos tenham relação com desenvolvimento de atividades ou projetos. Não devem ser gravados nesta pasta arquivos pessoais ou protegidos por direitos autorais. Esta pasta não está contemplada pela política de Backup;

f.2) A pasta “Fóruns” armazena os arquivos referentes aos fóruns realizados pelo Sesi, sendo PDL1, PDL2, Relise1, Relise2, Somar e Repensar. O acesso ao conteúdo das pastas é restrito aos participantes de cada fórum;

f.3) A pasta “Avisos” está acessível a todos os usuários, mas seu uso é restrito ao Setor de TI, para disponibilizar avisos institucionais;

f.4) A pasta “Fotos” armazena o acervo institucional, conforme capítulo 8, item ‘b’ desde manual. Esta pasta está disponível às áreas apenas para consulta, sendo que a manutenção dos arquivos ali armazenados é de responsabilidade da ASCOM;

f.5) A pasta “Gfip’s” está disponível somente para consulta por parte dos usuários, e é gerenciada pela Relcom;

f.6) A pasta “SGQ’s” está disponível somente para consulta por parte dos usuários, e é gerenciada pela Adest;

g) Somente o servidor de arquivos é contemplado na política de backup. Arquivos armazenados localmente nas estações de trabalho, não estão contemplados na política de backup e, portanto, não podem ser recuperados em caso de perda devido a defeito no equipamento ou exclusão. Todos os arquivos que necessitam de proteção devem ser armazenados no servidor de arquivos, de acordo com os critérios deste manual, salientando o item ‘e’ deste capítulo;

g.1) O SESI-RR não se responsabiliza por arquivos pessoais armazenados nas estações, nem mantém uma política para backup dos mesmos, ficando sob responsabilidade da Instituição tão e somente os arquivos de uso no desenvolvimento das atividades profissionais, armazenados no Servidor de Arquivos conforme as normas já mencionadas;

h) O backup do sistema de arquivos é realizado de forma incremental – ou seja, é efetuada uma cópia apenas dos arquivos alterados desde o último backup – de forma diária, e um backup completo é realizado toda sexta-feira. Os arquivos são preservados pelo período de 30 dias. Esta estrutura se faz necessária devido a grande quantidade de arquivos a serem armazenados, tornando dessa forma possível se manter o armazenamento do backup pelo período especificado.

i) O backup dos sistemas de banco de dados é realizado diariamente, e os arquivos de backup são preservados por período de 30 dias.

j) A guarda e preservação dos arquivos de backup é de responsabilidade do Setor de TI, devendo os mesmos serem mantidos em ao menos 2 (dois) locais distintos, de forma a garantir a integridade e preservação dos mesmos;

k) Toda requisição de restauração de backup deve ser feita pela área ao Setor de TI, ficando sob responsabilidade do Setor de TI disponibilizar os arquivos resgatados;

l) O SESI-RR reserva o direito de preservar as informações que trafegam em sua Intranet e conexão com a Internet, a fim de manter a integridade das informações, identificar situações de falha, tentativas de invasão, auditar o uso e adotar padrões, mantendo o sigilo e evitando violações de privacidade;

m) O Setor de TI deve preservar os arquivos que trafegam na Intranet, com vistas a garantir a integridade dos recursos do SESI-RR frente à entrada de vírus de computador e invasão por agentes não autorizados, falhas de sistema e equipamento, e para fins de segurança e auditoria.

n) A preservação de que trata esse item limita-se, obrigatoriamente, as questões relativas à segurança de equipamentos de informática e sistemas informatizados;

## 10. PROCEDIMENTO PARA ABERTURA DE CHAMADOS SOLICITAÇÕES DE MANUTENÇÃO E EVENTOS

### OBJETIVO:

Padronizar o procedimento de abertura de chamados, definindo as responsabilidades das partes envolvidas e criando critérios e normas para que todos os chamados sejam atendidos e classificados em tempo hábil pelo Setor de TI, maior qualidade e desempenho das funções necessárias para um atendimento com agilidade e qualidade.

### NOMENCLATURA:

**Chamado:** Toda solicitação efetuada via Ocomon, memorando ou email ao Setor de TI.

**Chamado de Manutenção:** São os chamados relativos à manutenção – preventiva ou corretiva – de equipamentos, rede e outros elementos.

**Chamado de Evento:** são todos os chamados relativos à solicitação de eventos, montagem de equipamento, vídeo conferencia, apoio técnico para eventos, etc.



## 10.1 SOBRE O USO DA FERRAMENTA, E ABERTURA DE CHAMADOS

a) Toda solicitação de manutenção e evento deve ser efetuada via Ocomon, Em caso de impossibilidade de acessar o sistema, o usuário poderá realizar a solicitação via telefone, pessoalmente, e-mail ou memorando. No caso de solicitações via telefone ou pessoalmente, fica sob a responsabilidade do usuário o posterior registro para controle;

b) Chamados de Evento devem ser abertos com uma antecedência mínima de 24 (vinte e quatro) horas do referido evento;

b.1) Em caso de eventos informados sem a devida antecedência, o Setor de TI somente efetuará o atendimento caso haja disponibilidade de recursos, desde que não cause impacto na agenda de atendimentos previamente estabelecida;

b.2) Cada chamado de evento deve ser relacionado a 1 (um) único evento;

b.3) Mesmo para o caso de um evento que se repita em datas ou horários diferentes, deve ser aberto um chamado específico para cada evento;

c) As seguintes informações devem ser necessariamente informadas para que os chamados sejam corretamente atendidos e com maior agilidade:

**Área Responsável:** Chamados de manutenção e evento devem ter área TI selecionada;

**Problema:** Deve ser selecionada a opção que melhor se encaixa a descrição do chamado;

**Descrição do problema:** Deve ser informada uma breve descrição da solicitação do chamado, sendo:

- Em caso de chamado técnico, informar descrição do problema apresentado;
- Em caso de chamado de evento, informar corretamente os dados do evento, constando hora, local, serviços e equipamentos necessários, bem como citar a origem destes equipamentos;
- Informar se houver necessidade de acompanhamento técnico durante o evento;

**Unidade:** Identificar corretamente a unidade responsável pelo pedido de atendimento;



**Etiqueta do Equipamento:** Para caso de chamado de manutenção, informar nº patrimônio;

**Contato:** Informar o nome do solicitante ou do contato responsável pelo chamado;

**Ramal:** Informar ramal ou telefone para contato;

**Local:** Informar o local onde deve ser realizada manutenção / evento;

**Enviar e-mail para:** Devem ser desmarcadas todas as opções.

d) Após este procedimento, o chamado se encontrará em aberto, aguardando o atendimento por parte do Setor de TI. O chamado pode ser agendado para atendimento futuro, para os casos de chamado de evento, ou para chamados de manutenção que dependam da compra de peças, acordo entre setores, dependências de outros projetos, ou quaisquer motivos que impeçam o atendimento imediato da solicitação.

e) Cabe ao usuário o acompanhamento do Status de seu chamado através da ferramenta Ocomon.

## 11. PROCEDIMENTO PARA ENCERRAMENTO DE CHAMADO (TI)

### OBJETIVO:

Padronizar o processo de fechamento de chamados, tornando este processo mais ágil, e passando a maior informação possível a respeito do atendimento para o usuário solicitante, diminuindo a fila de chamados pendentes e evitando o processo de reabertura de chamado.

a) Todos os chamados devem ser fechados pelo técnico da T.I. responsável pelo atendimento, tão logo sejam concluídos, a fim de evitar o acúmulo de chamados já solucionados na fila de atendimento;

b) Os chamados que não são possíveis de serem atendidos, devido a demanda, ou inviabilidade técnica, devem ser agendados, e informado o motivo do não atendimento imediato da solicitação;

c) Ao atender um chamado, informar corretamente a descrição do problema e a solução tomada, deixando bem claro ao solicitante todas as ações tomadas para o bom atendimento do chamado.

### 11.1 SUPORTE REMOTO



Para os casos de chamado de manutenção, a mesma poder ser efetuada via ferramenta de suporte remoto. Para tal, será feito contato prévio com o solicitante informando do acesso a sua estação.

a) Quando em uso da ferramenta de suporte remoto, ficará visível durante todo o período de acesso, um Banner indicativo no canto inferior direito da tela, indicando o login de usuário que está efetuando acesso, e o nome da estação que originou este acesso. Esta tela não pode ser removida, até que seja feita a desconexão da ferramenta de suporte remoto;

b) Quando do término do atendimento, o chamado será fechado pelo Setor de TI, registrando, em campo específico, os procedimentos e medidas tomadas para sua conclusão, ficando estas informações disponíveis para acesso do usuário, podendo inclusive o fechamento do chamado ser recusado, caso o problema persista ou o usuário não concorde com a solução tomada;

c) Para os chamados que tem seu fechamento recusado, será tomada nova atitude corretiva pelo Setor de TI, para que seja tomada uma solução adequada a solicitação, procedendo com um novo fechamento após a tomada destas medidas;

d) Em caso de não haver uma solução a ser tomada, devido a inviabilidade técnica, falta de recursos ou outros, deve ser lavrado um termo de não conformidade, detalhando a situação e as providencias tomadas;

e) No caso de equipamentos que necessitem de compra de peças, o mesmo será devolvido ao setor juntamente com relatório informando os procedimentos tomados, o diagnostico e a necessidade a ser atendida, o chamado será atualizado com o número do relatório emitido e ficará pendente, aguardando o processo de compra;


f) No caso de equipamentos que necessitem de manutenção externa, o mesmo será devolvido ao setor juntamente com relatório informando os procedimentos tomados, o diagnostico e a necessidade a ser atendida, e o chamado será fechado, indicando o número do relatório emitido;



## DAS DISPOSIÇÕES FINAIS

- a) Esta Política entra em vigor nesta data;
- b) itens alterados: 6.d; 6.d.1. (desligamento dos colaboradores);
- b) Ficam revogadas as disposições em contrário, especialmente a Instrução Normativa 004/2006, de 12 de julho de 2006 e Instrução Normativa 001/2011, de 15 de abril de 2011.

Dê ciência e cumpra-se.  
Boa Vista – RR, 11 de maio de 2014.



**Rivaldo Fernandes Neves**  
Diretor Regional do Sesi