OBJETIVOS

Definir as Políticas, Diretrizes, Critérios e Responsabilidades pela Utilização dos Recursos de Tecnologia da Informação e de Comunicação da Companhia.

Designar todos os Diretores e Assessores, como responsáveis pelo cumprimento das orientações desta Instrução no âmbito de suas equipes.

Designar o Assessor de Planejamento e Organização como responsável por garantir o fiel cumprimento desta Instrução, pela sua divulgação a todos os Colaboradores e pela proposição de documentos normativos complementares que se fizerem necessários.

ANEXOS

1. **TECNOLOGIA DA INFORMAÇÃO**
2. **TELEFONIA FIXA E MÓVEL**
3. **RÁDIOS MÓVEIS**
4. **RESPONSABILIDADES**

São Paulo, 30 de dezembro de 2009

Roberto Lopes Pontes Simões
Diretor Presidente

Distribuição:
Diretores
Assessores
Gerentes
Demais Colaboradores através de seus Líderes

Nota:

Este documento pode ser acessado na Rede Interna de Computadores da Companhia, através do seguinte endereço eletrônico:

G:\Geral\Instruções do DP\IN-DP-007-09

1 – Propriedade das Informações e dos Softwares

1.1 – Todos os dados e informações, gerados e manipulados durante a execução dos sistemas e processos da Companhia, são considerados como seu Ativo Intangível. Portanto devem ser protegidos de acordo com as Políticas de Segurança estabelecidas nesta Instrução.

1.2 – Os dados e informações criados nos recursos computacionais da Companhia são de sua propriedade e devem ser utilizados pelos Colaboradores, Prestadores de Serviços e Consultores, exclusivamente no exercício de suas atividades.

1.3 – Os softwares adquiridos no mercado ou desenvolvidos internamente pertencem exclusivamente à Companhia, inclusive os direitos relativos a todas as invenções, inovações tecnológicas e criações intelectuais elaboradas e desenvolvidas pelos Colaboradores, Prestadores de Serviços e Consultores, durante a vigência da relação de emprego / contratual, ou quando forem utilizados recursos, dados, meios, materiais, instalações, equipamentos, informações tecnológicas e segredos comerciais pertencentes à Companhia.

2 – Segurança das Informações

2.1 – Os Colaboradores devem zelar para que as informações contidas nos sistemas sejam mantidas dentro de seu ambiente de trabalho, evitando o seu compartilhamento e a sua divulgação com pessoas estranhas e/ou não pertencentes ao quadro de Colaboradores da Companhia, principalmente quando estiver utilizando computadores portáteis fora das instalações da Companhia.

2.2 – As informações contidas nos sistemas ou em documentos armazenados em rede ou em computadores locais (desktops ou notebooks), nas contas de correio, sejam elas de responsabilidade do Colaborador ou de terceiros, devem ser consideradas de absoluto sigilo comercial, não podendo ser divulgadas sem autorização do Responsável pela Área solicitante, ou retiradas das dependências da Companhia por qualquer meio físico ou eletrônico, evitando a sua perda, furto, cópia, utilização indevida e divulgação não autorizada.

2.3 – Todos os computadores conectados às redes internas devem possuir softwares antivírus padronizados pela Companhia, permanentemente ativados e atualizados, bem como "descansos de tela" protegidos com senha.

2.4 – Os acessos feitos pelos prestadores de serviços e/ou consultores à rede interna não devem ser permitidos, exceto quando se utilizarem de computadores fornecidos pela Companhia, devidamente configurados dentro dos padrões adotados e com a prévia autorização do Responsável pela Área gestora dos serviços prestados.

2.5 – Os acessos à Internet aos prestadores de serviço e/ou consultores, devem ser permitidos somente via "wireless" e com prévia aprovação do Responsável pela Área gestora dos serviços prestados.

2.6 – Os usuários de computadores com acesso à Internet devem ser extremamente cautelosos e **não devem abrir e-mails com arquivos anexados**, recebidos de endereços desconhecidos, a fim de evitar a recepção de vírus.

2.7 – As publicações feitas por Colaboradores em grupos de discussão, não devem ser feitas com a utilização de endereços de e-mails da Companhia.

2.8 – A Companhia reserva o direito de realizar auditorias nas redes e nos sistemas, periodicamente, para garantir que esta Instrução esteja sendo seguida, podendo autorizar o monitoramento dos equipamentos, sistemas e redes, quando julgar necessário, **sem violar informações particulares dos Colaboradores**.

2.9 – Utilizações e proteções de senhas:

2.9.1 – As senhas são pessoais e intransferíveis. Devem estar sob a custódia e responsabilidade de cada Colaborador. O seu uso não deve ser compartilhado. Trata-se de um instrumento importante de segurança das informações, pois são utilizadas para validação dos usuários ao acessar os diversos sistemas da Companhia, a Internet, o correio de voz, as proteções de telas de computadores e os elementos ativos de redes (*routers, switches*, etc.).

2.9.2 – As senhas devem ser escolhidas e criadas pelos próprios Colaboradores usuários dos sistemas. A seguir, alguns cuidados que devem ser tomados pelos Colaboradores na construção e proteção de suas senhas:

a) As senhas devem conter pelo menos 8 (oito) caracteres, composto de 1 (um) caracter especial, 1 (um) número e 6 (seis) caracteres alfabéticos intercalados. Não devem ser repetidas as 10 (dez) últimas senhas utilizadas.

b) Não utilizar palavras comuns como: nome de familiares, de colegas, de Empresas ou de personagens conhecidas, bichos de estimação, terminologias de informática, comandos de sistemas, nomes de sites, hardwares, softwares, etc..

c) Evitar datas de aniversários, endereços, números de telefones, palavras ou seqüências de números e/ou letras, como: 12345678, 87654321, abcdef, qwertyu, aaabbb, carro1, 1carro, etc..

d) Não utilizar os recursos de "lembrar senha", constantes de aplicativos como: *Internet Explorer, Outlook, Dial-up* e outros.

e) Devem ser alteradas pelo próprio Colaborador, a cada período de 90 (noventa) dias, no mínimo, sem reutilizar as senhas anteriores.

f) As senhas com privilégios de Administradores de Sistemas, de Aplicações e de Equipamentos (*ROOT, NT, ADMIN* e outras) devem ser alteradas a cada período de 45 (quarenta e cinco) dias, no mínimo, sem reutilizar as senhas anteriores.

2.9.3 – Uma senha segura deve ser construída com letras maiúsculas e minúsculas, intercaladas com números e caracteres (8 no mínimo), como exemplos: a78BG(*), #$%67hly+*, etc., e não devem ser armazenadas ou anotadas em locais de fácil acesso por terceiros. Devem ser fáceis de serem lembradas e difíceis de serem descobertas.

2.10 – Acessos remotos aos dados e informações da Companhia:

2.10.1 – Permitem aos Colaboradores usuários dos Recursos de T.I., devidamente autorizados pela Diretoria, acessar as suas bases de dados e informações fora de seu local de trabalho habitual, para atender as necessidades da Companhia.

2.10.2 – Os fornecedores e prestadores de serviços, quando autorizados a acessar remotamente dados e informações da Companhia, devem ter em seus Contratos de Prestação de Serviços, cláusulas específicas de "confidencialidade".

2.10.3 – Esses acessos devem ser feitos com cuidados especiais por parte dos Colaboradores e conter mecanismos especiais de proteção, para evitar exposição indevida das informações e danos causados por acessos não autorizados.

2.10.4 – Os acessos remotos devem ser feitos via *Internet,* através de *ISP* (*Internet Service Provider*), contratado pelo Colaborador usuário, desde que possua uma *VPN* (*Virtual Private Network*) para acesso externo à rede interna da Companhia, instalada em seu computador e fornecida pelo Responsável pelo Suporte de T.I., juntamente com o software "antivírus" padronizado pela Companhia.

2.10.5 – Os acessos discados através de *callback* ficam restritos aos técnicos de suporte e administradores de redes, previamente cadastrados e autorizados.

2.10.6 – Os acessos remotos às redes internas devem ser protegidos por *firewall* homologado e padronizado pela Companhia.

2.10.7 – Os "privilégios" de acesso pelos Colaboradores devem ser os mesmos, tanto para os acessos locais como para os remotos. Esses acessos estão limitados ao *datacenter*, sem acesso aos computadores pessoais da Companhia.

3 – Internet

3.1 – Os acessos à Internet devem ser feitos com o objetivo de obter informações essenciais aos negócios da Companhia, ou para a execução de serviços *on-line* que possam trazer maior produtividade às funções de cada Colaborador.

3.2 – Os serviços de acesso à *Internet*, disponíveis e permitidos, são os seguintes:

a) *www* (*world wide web*), para acessar os diversos endereços (*sites*) de interesse profissional do Colaborador.

b) *newsgroups*: seções especiais para tratar de assuntos de interesse comum entre os participantes.

c) *FTP* e *downloads* (transferências de arquivos até 50 MB): ferramentas específicas para a transferência de arquivos magnéticos de grandes volumes.

d) Videoconferências: ferramenta específica para a participação de fóruns, debates e seminários à distância.

e) Correio eletrônico: para a troca de correspondência de forma rápida entre várias pessoas de relacionamento do Colaborador.

f) Comunicação entre duas ou mais pessoas (*chat*, tipo *MSN* e assemelhados).

g) Os Recursos de T.I. podem ser utilizados pelos Colaboradores para a solução de assuntos particulares (movimentações bancárias, correio eletrônico, etc.) dentro dos limites do bom senso.

3.3 – Os acessos a videoconferências, transferências de arquivos (acima de 10 Mb) e outros serviços que impliquem na utilização extensiva dos meios de acesso à *Internet* devem ser feitos em horários pré-definidos, de comum acordo com o Responsável pelos Recursos de T.I. da Companhia.

3.4 – Os Colaboradores participantes de *chats, newsgroups* e videoconferências, não devem tratar de assuntos confidenciais da Companhia.

3.5 – O acesso e a navegação pela Internet devem ser protegidos por recursos de controle de monitoramento de acesso, por *softwares antivírus* nas estações e servidores e por *firewall* de proteção contra tentativas de danificação da infra-estrutura e das informações existentes nas redes da Companhia.

3.6 – Os acessos a *sites* que contenham conteúdos proibidos devem ser bloqueados de forma automática pelos servidores de acesso.

3.7 – As necessidades de softwares e aplicativos disponíveis na Internet devem ser encaminhadas para análise, aprovação e homologação, pelo Responsável pelos Recursos de T.I. da Companhia.

3.8 – Os recursos de Correio Eletrônico destinam-se a otimizar as comunicações entre os Colaboradores, para tratar de assuntos profissionais. Destinam-se também a estabelecer comunicações com terceiros.

3.9 – Ficam definidos os softwares "*Microsoft Exchange*" e "*Microsoft Outlook*", para serem utilizados como recursos de Correio Eletrônico, em todas as Áreas da Companhia.

3.10 – O formato de endereço de correio eletrônico, preferencialmente, deve ser o seguinte: "nomedousuário@santoantonioenergia.com.br".

3.11 – Fica definido o limite de *500 MB* por caixa postal que deve estar localizada no servidor *Exchange*. Ao ultrapassar esse limite, o Colaborador fica impedido de enviar e receber novas mensagens. Quando atingir cerca de 90% desse limite, o Colaborador deve ser avisado para que tome as devidas providências.

3.12 – Devem ser providenciados arquivos de segurança (*backups*) das caixas postais armazenadas no servidor *Exchange*, 5 (cinco) vezes por semana, pela Equipe de Correio do Suporte Corporativo.

3.13 – Podem utilizar-se dos recursos de Correio Eletrônico, todos os Colaboradores que exerçam funções que requeiram a sua utilização, a critério de sua respectiva Diretoria, Assessoria ou Gerência.

3.14 – Os acessos às caixas postais podem ser feitas através da utilização dos recursos de *webmail*.

4 – Padrões para Desenvolvimento de Aplicativos

4.1 – Os sistemas desenvolvidos internamente, ou adquiridos de terceiros, devem garantir os seguintes padrões de segurança:

a) Autenticação de usuários individuais e nunca de grupos.

b) Armazenagem de senhas criptografadas e nunca em texto.

c) Permissão e administração de perfis de acesso pelo Administrador do sistema, sem que este tenha acesso ao conteúdo das senhas dos usuários.

5 – Armazenamento de Arquivos (Servidores)

5.1 – Os arquivos eletrônicos da Companhia devem ser armazenados de forma segura, com as seguintes definições e características:

a) Devem ser utilizados Servidores de padrão *Windows* (última versão).

b) Os nomes dos servidores devem ser padronizados, como segue: Inicial do sistema operacional (W = Windows, U = Unix e L = Linux), inicial distintiva (S = Servidor), inicial da localidade (SP = São Paulo, PV = Porto Velho), número seqüencial, empresa (escritos em letras minúsculas, com, no máximo, 15 dígitos).

Exemplo: wssp01-saesa

c) Os modos de acesso devem ser por compartilhamentos de diretórios no servidor, organizados por: Dados Corporativos, Dados de Usuários e Aplicativos. O diretório de Dados Corporativos deve ser subdividido por Setores. Os diretórios Setores devem ser subdivididos em Processos. O diretório de Dados de Usuários deve ser subdividido por *login* do Usuário. O diretório de Aplicativos deve ser subdividido por Aplicativo existente.

d) Os acessos aos diretórios dos Setores e Aplicativos são definidos de acordo com as necessidades de cada Usuário. Cabe ao Responsável pelos Recursos de T.I. da Companhia definir os meios de segurança necessários.

e) Deve ser utilizado um Diretório Geral, de uso compartilhado e localizado no Servidor, com acesso a todos os Usuários, com Área de Transferência e Armazenamento Temporário, cujo conteúdo deve ser deletado semanalmente.

f) Os arquivos relacionados aos negócios da Companhia devem ser armazenados nos Servidores e não nos *hard disks* dos *PCs* e/ou *laptops* dos Colaboradores.

5.2 – Os servidores devem dispor de espaço suficiente para o armazenamento seguro dos arquivos que contenham informações referentes aos processos e atividades da Companhia, cabendo ao Responsável pelos Recursos de T.I. administrar e atualizar as suas capacidades.

5.3 – Devem ser feitas cópias de segurança (*backups*) dos servidores, diariamente, no modo "completo".

6 – Padrões de Equipamentos e Softwares

6.1 – Os *hardwares* básicos (*PCs e laptops*) para uso dos Colaboradores devem ter configuração definida pelo Responsável por T.I. da Companhia, e, periodicamente, em função da evolução tecnológica do mercado fornecedor de equipamentos, devem ser atualizados considerando também as necessidades dos usuários.

6.2 – A aquisição de equipamentos fora dos padrões estabelecidos deve ser precedida de justificativa formal, com aprovação do Assessor de Planejamento e Organização.

6.3 – Essas aquisições devem ser coordenadas pelo Responsável por T.I. da Companhia, visando padronização, atualização tecnológica, assistência técnica de manutenção, capacidade de atendimento e redução de custos, através da negociação com parceiros estratégicos.

6.4 – Anualmente, o Responsável pelos Recursos de T.I. deve analisar o inventário de equipamentos disponíveis que necessitam de alteração e/ou substituição no ano seguinte. Cabe a cada Diretoria ou Assessoria incluir em seus orçamentos as necessidades de alteração e/ou substituição.

6.5 – As impressoras devem ser instaladas em "pools" e ser compartilhadas por vários Colaboradores, preferencialmente.

6.6 – Os softwares básicos devem ser da linha *Microsoft* em suas últimas versões (*Windows XP, VISTA, Windows 7, MS Office) e Antivírus Trend.*

6.7 – O software utilizado como "plataforma de colaboração" para aplicações "*intranet*", deve ser o "*Sharepoint*" da linha *Microsoft,* em sua última versão.

7 – Aquisição de Soluções de Tecnologia da Informação

7.1 – Todas as aquisições de soluções de T.I. (softwares, aplicativos, equipamentos, telemática, etc.) e serviços (desenvolvimento de softwares, aplicativos e consultorias) devem ser submetidos à prévia aprovação do Responsável por T.I., com o objetivo de padronização e racionalização desses recursos.

7.2 – As aquisições / contratações de serviços de desenvolvimento de softwares específicos para a Companhia, devem incluir os fornecimentos dos respectivos códigos-fonte e demais documentações, necessárias para a realização de eventuais adaptações e/ou manutenções, de forma independente do Fornecedor, sempre que possível.

8 – Bancos de Dados

8.1 – Fica definido como padrão, para suportar a gestão dos bancos de dados da Companhia, o software *ORACLE*; e para a *Intranet*, o software *MS-SQL Server.*

9 – Plano de Contingência

9.1 – Deve ser desenvolvido, publicado e revisado anualmente, um Plano de Contingência, a ser implementado em caso de acidentes graves que possam afetar as operações da Companhia, quanto à utilização dos recursos de T.I..

9.2 – O Plano de Contingência deve conter meios para identificar e reduzir riscos em casos de acidentes graves, bem como de garantir que os serviços essenciais de T.I. sejam normalizados dentro dos prazos requeridos.

9.3 – O Plano de Contingência deve prever:

a) Os recursos e serviços críticos para a operação da Companhia.

b) As soluções propostas para cada tipo de serviço.

c) A freqüência e planejamento dos testes dos procedimentos de "Contingência".

d) Os resultados esperados e históricos.

e) Os Fornecedores com os respectivos endereços e contatos.

f) Os *backups*, os Responsáveis e respectivos endereços / contatos.

10 – Utilizações não permitidas

10.1 – Os Recursos de T.I. (computadores, *softwares*, redes, *Internet*, *e-mails*, etc.) não devem ser utilizados pelos Colaboradores em atividades consideradas ilegais ou antiéticas, como exemplos:

a) Obter ou distribuir softwares ou arquivos que impliquem em "quebra de direitos autorais" ou "de propriedade intelectual do Autor", devendo seguir, rigorosamente, a Legislação em vigor sobre licença e *copyright* (Leis Federais 9609 e 9610).

b) Disseminar / distribuir softwares ou produtos que atuem em forma de "vírus" e/ou que possam prejudicar a Companhia ou causar danos aos destinatários / terceiros.

c) Instalar, distribuir, reproduzir e utilizar quaisquer softwares não licenciados pela Companhia.

d) Obter ou tentar obter acessos não autorizados a outros sistemas ou redes de computadores da Companhia.

e) Interferir ou interromper serviços, servidores ou redes conectados aos sistemas da Companhia.

f) Divulgar informações ou listas de Colaboradores da Companhia para terceiros, sem prévia autorização da Diretoria.

g) Enviar *e-mails* não solicitados (*spam*) ou dos tipos de pirâmide ou cadeia.

h) Transmitir / divulgar material com conteúdo ilegal, difamatório, que possa violar a privacidade de terceiros, ou que seja abusivo, discriminatório, preconceituoso, ameaçador, obsceno, prejudicial, injurioso ou de qualquer outra forma censurável.

i) Transmitir material de divulgação política, religiosa e afins.

j) Acessar endereços (*sites*), que tratam de assuntos que estimulem a violência, corrupção, pornografia, discriminação social, racial, religiosa, política ou quaisquer outras que estimulem a ofensa e atentem contra os bons costumes.

k) Quaisquer outras utilizações para fins ilegais, ou que violem qualquer Lei ou Regulamento das esferas Municipais, Estaduais ou Federais, ou que não estejam de acordo com as Políticas e Diretrizes da Companhia.

10.2 – Os sistemas de proteção da Companhia (*firewall*) devem controlar os *logs* de acesso à *Internet*, como medida de segurança, e para identificar as utilizações indevidas.

1 – Gerais

1.1 – Os telefones fixos e móveis pertencentes à Companhia e colocados à disposição de seus Colaboradores, são considerados como instrumentos de apoio nas comunicações internas e externas, necessárias para o desempenho de suas atividades.

2 – Telefones Fixos (Linhas Diretas Normais ou através de VOIP)

2.1 – Os telefones fixos tradicionais ou *VOIP (voz sob IP)* devem ser utilizados nas comunicações internas e externas, preferencialmente, em relação aos telefones móveis (celulares), em função de seus custos de utilização.

2.2 – As ligações interurbanas e internacionais devem ser efetuadas com parcimônia pelos Colaboradores, restritas às suas reais necessidades profissionais.

2.3 – As centrais telefônicas, tipo PABX ou similares, devem dispor de recursos de controle das ligações efetuadas, para efeito de contabilização das despesas por Unidade de Acompanhamento (U.A.) bem como para identificar as ligações particulares, cujos custos devem ser ressarcidos à Companhia pelos respectivos Colaboradores.

3 – Ramais Telefônicos

3.1 – Os ramais telefônicos devem ser classificados em 3 (três) categorias básicas, como segue:

a) Categoria A: sem restrição, podendo fazer ligações DDI e DDD.

b) Categoria B: com restrição somente para DDI.

c) Categoria C: com permissão somente para fazer ligações internas e receber chamadas externas.

4 – Telefones Móveis (Celulares)

4.1 – Os telefones móveis (celulares) à disposição de seus Colaboradores são considerados como instrumentos de apoio nas comunicações internas e externas, necessárias para o desempenho de suas atividades.

4.2 – Os telefones móveis não devem ser considerados como benefício ou complemento salarial, em nenhuma hipótese.

4.3 – Os tipos de telefones móveis são os seguintes: *"Blackberry" e Celular Corporativo.*

4.4 – Os tipos e suas destinações devem ser precedidos de rigorosa avaliação de suas necessidades e aprovadas pelo respectivo Diretor ou Assessor.

4.5 – Os telefones móveis por terem os seus custos superiores aos dos telefones fixos e *VOIP* devem ser utilizados com parcimônia e racionalidade pelos respectivos usuários.

4.6 – Os custos com a aquisição de aparelhos móveis, bem como de suas faturas mensais, devem ser assumidos pela Companhia e apropriados nas U.A.s dos Colaboradores usuários.

4.7 – Os custos com as ligações particulares devem ser ressarcidos à Companhia pelos respectivos Colaboradores.

1 – Os rádios móveis colocados à disposição de seus Colaboradores pela Companhia destinam-se a estabelecer uma comunicação eficaz e eficiente entre eles, quando de suas atividades externas, principalmente nas áreas adjacentes à U.H.E. Santo Antônio.

2 – Eles permitem uma comunicação dentro de uma área restrita, com utilização de freqüências específicas autorizadas pela ANATEL – Agência Nacional de Telecomunicações.

3 – Esses recursos devem ficar restritos às comunicações internas, entre os próprios Colaboradores da Companhia, podendo, eventualmente, serem estendidos aos Colaboradores de outras Empresas prestadoras de serviços, quando necessário.

4 – A utilização desse meio de comunicação deve se destinar exclusivamente ao atendimento das necessidades profissionais dos Colaboradores.

5 – A forma de comunicação através desse sistema deve ser a mais direta e objetiva possível, a fim de evitar o congestionamento dos recursos disponíveis (equipamentos, antenas, repetidoras, bandas etc.). Devem ser utilizados para tratar de assuntos pontuais e inadiáveis.

6 – Esse sistema não permite a integração ou interface com os outros meios tradicionais de comunicação, como: serviços de telefonia fixa, móvel ou internet. Ele funciona dentro de uma rede própria e limitada geograficamente.

7 – Cada Colaborador é diretamente responsável pelo uso que fizer do equipamento de rádio colocado à sua disposição, pela sua guarda e pela sua devolução quando se tornar desnecessário.

8 – A sua operação e manutenção básica (carga de bateria, proteção contra umidade e calor excessivo etc.), devem ser feitas de acordo com o Manual do Fabricante colocado à disposição de cada Colaborador usuário.

9 – Existem 2 tipos de radiocomunicador:

a) Afixado em um veículo motorizado.

b) Portátil.

10 – O equipamento afixado em um veículo motorizado, tem a sua alimentação elétrica oriunda da bateria do veículo onde a sua antena é instalada. Esse tipo de equipamento possui, normalmente, uma maior cobertura para a transmissão e recepção de comunicação.

11 – O equipamento portátil tem a sua alimentação elétrica oriunda de bateria própria, a ser carregada pelo próprio Colaborador, com a utilização de carregador (conversor de CA para CC), semelhante aos que são utilizados pelos celulares. Esse tipo de equipamento possui, normalmente, uma menor cobertura para a transmissão e recepção de comunicação, uma vez que a sua antena é acoplada ao próprio equipamento.

1 – Da Assessoria de Planejamento e Organização

1.1 – Liderar a especificação e a revisão das estratégias de Tecnologia da Informação e Comunicação, baseadas nas necessidades dos negócios da Companhia.

1.2 – Zelar pelo cumprimento das Políticas e Diretrizes desta Instrução, principalmente quanto à disponibilidade e qualidade de sistemas, serviços, segurança e contratos de prestação de serviços por terceiros.

1.3 – Disponibilizar e manter uma infra-estrutura adequada às necessidades atuais, bem como coordenar a definição da arquitetura futura da Companhia, em termos de Tecnologia da Informação e Comunicação.

1.4 – Promover o treinamento e a capacitação dos Colaboradores na utilização dos recursos de Tecnologia da Informação e de Comunicação, assim como dos Sistemas de Gestão adotados pela Companhia, inclusive *help-desk*.

1.5 – Coordenar os orçamentos sobre os recursos de Tecnologia da Informação e de Comunicação.

1.6 – Administrar os serviços de telefonia da Companhia, como segue:

a) Classificar os ramais da central de PABX por categoria.

b) Providenciar a aquisição de equipamentos fixos e móveis, quando necessário.

c) Controlar os equipamentos móveis, conforme Instrução IN-DP-012-09 – Bens Patrimoniais.

d) Zelar pela operacionalidade dos sistemas de comunicação da Companhia, providenciando as manutenções que se fizerem necessárias.

e) Receber, conferir e encaminhar as contas telefônicas para pagamento, indicando as respectivas UAs.

f) Controlar e avaliar a evolução dos custos com os serviços de telefonia móvel, e oportunamente propor a definição de limites mensais a serem adotados pelos Colaboradores usuários.

g) Identificar as ligações particulares efetuadas pelos Colaboradores e providenciar o ressarcimento de seus custos à Companhia.

2 – Dos Colaboradores

2.1 – Utilizar os sistemas e os recursos de Tecnologia da Informação e de Comunicação, de acordo com as Políticas e Diretrizes desta Instrução.

2.2 – Reportar ao Assessor de Planejamento e Organização, quaisquer anomalias verificadas na utilização dos recursos de e dos sistemas adotados pela Companhia, para que sejam tomadas as medidas corretivas e preventivas necessárias.

2.3 – Identificar as ligações particulares de sua responsabilidade, informando-as à Assessoria de Planejamento e Organização, para efeito de ressarcimento de seus custos à Companhia.

3 – Dos Diretores e Assessores

3.1 – Definir os Colaboradores que tenham necessidade de dispor de:

a) Telefones móveis (celulares, por tipo).

b) Categoria de ramal telefônico.

c) Radiocomunicadores (fixos ou móveis).

d) Computadores pessoais (de mesa ou portáteis).