LGPD – CONSTRUTORA SUDOESTE
Inovar para encantar

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Versão: 1.0 – Revisão: 5

1. OBJETIVO

A Política de Segurança da Informação é uma declaração formal da Construtora Sudoeste Ltda e subsidiárias, acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus colaboradores (internos ou externos).

2. ABRANGÊNCIA

Todos os funcionários, estagiários, jovens aprendizes, diretores, executivos, acionistas, prestadores de serviços, consultores, auditores, temporários, fornecedores, parceiros diversos e demais contratados que estejam a serviço e disponibilizam de ativos corporativos da Construtora Sudoeste Ltda, suas Unidades, subsidiárias e/ou coligadas.

3. MISSÃO

Garantir a disponibilidade, integridade, confidencialidade, legalidade e autenticidade da informação necessária para a realização dos negócios da Construtora Sudoeste Ltda e subsidiárias.

4. DOCUMENTOS DE REFERÊNCIA

NBR ISO/IEC 17799:2005 - Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação; ABNT ISO/IEC 27000:2018 – Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary; ABNT ISO/IEC 27001:2013 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos; ABNT ISO/IEC 27002:2013 – Tecnologia da informação — Técnicas de segurança — Código de práticas para controles de segurança da informação.

5. TERMOS E DEFINIÇÕES

5.1. TI - Tecnologia da Informação

- Software: É a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores. Toda interação dos usuários de computadores é realizada através de softwares.

DATA CRIAÇÃO	
DATA ATUALIZAÇÃO	
APROVADO POR	

- Backup: É a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.
- Mídias Removíveis: Dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Disquete, Pen Drive, cartão de memória entre outros.
- USB: É um tipo de conexão "ligar e usar" que permite a conexão de periféricos sem a necessidade de desligar o computador.
- VPN (Virtual Private Network): Modalidade de acesso à rede corporativa, que possibilita a conectividade, via internet, de um equipamento externo à rede interna da corporação, provendo funcionalidades e privilégios como se ele estivesse conectado física e diretamente à rede interna. Comumente é utilizado por funcionários em trânsito.
- Softwares de Mensageria: São programas que permitem a usuários se comunicarem remotamente (à distância), através de conexão com a Internet. Por meio destes programas, é possível enviar mensagens de texto entre equipamentos fisicamente distantes. Também é possível enviar arquivos ou iniciar sessões de conversação com áudio e/ou com vídeo, em tempo real.
- Firewall: É um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.
- Modem 3G/4G: É um dispositivo sem fio, com saída USB para conexão em outro dispositivo tais como Tablets (com suporte 3G/4G), notebooks, netbooks, desktops, etc. objetivando conexão com a internet. O modem 3G/4G recebe e decodifica o sinal digital de alta velocidade transmitido pelas operadoras de celulares para aparelhos portáteis (celulares, smartphones e notebooks) compatíveis com a tecnologia 3G/4G.

6. DIRETRIZES

6.1. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

Conforme definição da norma NBR ISO/IEC 17799: 2005, a informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e, consequentemente, necessita ser adequadamente protegida. A Política de Segurança da Informação objetiva proteger a informação de diversos tipos de ameaça, para garantir a continuidade dos negócios minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócio.

A segurança da informação é aqui caracterizada pela preservação da:

a) Confidencialidade, que é a garantia de que a informação é acessível somente a pessoas com acesso autorizado;

b) Integridade, que é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

c) Disponibilidade, a Política de Segurança da Informação deve ser divulgada a todos os funcionários e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento.

Para assegurar esses três itens mencionados, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não-intencional, acidentes e outras ameaças.

É fundamental para a proteção e salvaguarda das informações que os usuários adotem a ação de Comportamento Seguro e consistente com o objetivo de proteção das informações, devendo assumir atitudes proativas e engajadas no que diz respeito à proteção das informações. Campanhas contínuas de conscientização de Segurança da Informação serão utilizadas para monitoração e controle destas diretrizes.

A Política de Segurança da Informação da Construtora Sudoeste Ltda e subsidiárias é aprovada e revisada anualmente pela Diretoria Executiva.

6.2. ATRIBUIÇÕES E RESPONSABILIDADES NA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

6.2.1. Definição

Cabe a todos os colaboradores (funcionários, estagiários, jovens aprendizes e prestadores de serviços) cumprir fielmente a Política de Segurança da Informação; buscar orientação do gestor imediato em caso de dúvidas relacionadas à segurança da informação; proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados; assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela Construtora Sudoeste Ltda; cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual; e comunicar imediatamente a empresa quando do descumprimento ou violação desta política, através do canal de ética.

6.2.2. Diretorias, Gerências e Coordenações

Cabe às Diretorias, Gerências e Coordenações cumprir e fazer cumprir esta Política; assegurar que suas equipes possuam acesso e conhecimento desta Política de Segurança da Informação; e comunicar imediatamente eventuais casos de violação de segurança da informação.

6.2.3. Área de Governança de TI, Governança Corporativa e Governança Jurídica.

Cabe às três áreas propor ajustes, melhorias, aprimoramentos e modificações desta Política; convocar, coordenar, lavrar atas e prover apoio às reuniões que discutam a respeito desta Política; prover todas as informações de gestão de segurança da informação solicitadas por Gestores.

6.3. PROPRIEDADE INTELECTUAL

6.3.1. É de propriedade da Construtora Sudoeste Ltda e subsidiárias, todos os “designs”, criações, procedimentos, documentos, modelos, sistemas, soluções, modelos de negócios, metodologias e pesquisas desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício com a Construtora Sudoeste Ltda.

6.4. ENGENHARIA SOCIAL

6.4.1. Engenharia social é um termo utilizado para representar a habilidade de enganar pessoas, visando obter informações sigilosas.

6.4.2. A Engenharia Social manifesta-se de diversas formas, e podemos dividi-las em dois grupos. No entanto, o grande ponto onde engenheiros sociais se baseiam é na falta de conscientização do usuário com relação à Segurança da Informação e na exploração da confiança das pessoas para a obtenção de informações sigilosas e importantes, e como uma simples informação poderia trazer prejuízos à empresa:

6.4.2.1. Diretos: São aqueles caracterizados pelo contato direto entre o engenheiro social e a vítima através de telefonemas e até mesmo pessoalmente, pois engenheiro social nem sempre é alguém desconhecido.

6.4.2.2. Indiretos: Caracterizam-se pela utilização de softwares ou ferramentas para invadir, como, por exemplo, vírus, cavalos de Tróia ou através de sites e e-mails falsos para assim obter informações desejadas. Podem ser mensagens que contenham avisos de premiações milionárias em loterias, ofertas de sociedade em grandes somas de dinheiro, heranças e negócios em outros países etc. O melhor a fazer é ignorar a oferta tentadora e encaminhar o e-mail imediatamente para emailsuspeito@sudoeste.com.br.

6.5. CLASSIFICAÇÃO DA INFORMAÇÃO

6.5.1. É de responsabilidade do Gerente/Supervisor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com os critérios a seguir:

DATA CRIAÇÃO	
DATA ATUALIZAÇÃO	
APROVADO POR	

6.5.1.1. Pública: É uma informação da Construtora Sudoeste Ltda ou de seus clientes com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade dela.

6.5.1.2. Interna: É uma informação da Construtora Sudoeste Ltda que ela não tem interesse em divulgar, onde o acesso por parte de indivíduos externos à empresa deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem da Organização, porém, não com a mesma magnitude de uma informação confidencial. Pode ser acessada sem restrições por todos os empregados e prestadores de serviços da Construtora Sudoeste Ltda.

6.5.1.3. Confidencial: É uma informação crítica para os negócios da Construtora Sudoeste Ltda ou de seus clientes. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais à Construtora Sudoeste Ltda ou aos seus clientes. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por empregados, clientes e/ou fornecedores.

6.5.1.4. Restrita: É toda informação que pode ser acessada somente por usuários da Construtora Sudoeste Ltda explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

6.6. REQUISITOS DE SEGURANÇA DO AMBIENTE FÍSICO

6.6.1. As máquinas (servidores) que armazenam sistemas da Construtora Sudoeste Ltda estão em área protegida.

6.6.2. Os servidores têm acesso devidamente controlado e monitorado.

6.6.3. A entrada nestas áreas ou partes dedicadas, por pessoas não autorizadas (visitantes, prestadores de serviço, terceiros e até mesmo funcionários, sem acesso liberado), que necessitarem ter acesso físico ao local, sempre o farão acompanhados de pessoas autorizadas.

6.6.4. O acesso às dependências da empresa com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só pode ser feito a partir de autorização da Diretoria e mediante supervisão. Exceto para eventos e treinamentos organizados pela própria empresa.

6.6.5. Respeitar áreas de acesso restrito, não executando tentativas de acesso às mesmas, ou utilizando máquinas alheias às permissões de acesso delimitadas a cada categoria de colaboradores.

6.7. BOAS PRÁTICAS DE COMUNICAÇÃO VERBAL DENTRO E FORA DA EMPRESA

DATA CRIAÇÃO	
DATA ATUALIZAÇÃO	
APROVADO POR	

6.7.1. Cuidado ao tratar de assuntos da empresa dentro e fora do ambiente de trabalho, em locais públicos, ou próximos a visitantes, seja ao telefone ou com algum colega, ou mesmo fornecedor.

6.7.2. Evite nomes e tratativas de assuntos confidenciais, nestas situações, fora da empresa ou próximos a pessoas desconhecidas.

6.7.3. Caso seja extremamente necessária a comunicação de assuntos sigilosos em ambientes públicos, ficar atento as pessoas à sua volta que poderão usar as informações com o intuito de prejudicar a imagem da empresa.

6.8. REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO

6.8.1. Diretrizes Gerais

6.8.1.1. Todo acesso às informações e aos ambientes lógicos deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas. As autorizações devem ser revistas, confirmadas e registradas continuadamente. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado. Os dados, as informações e os sistemas de informação das entidades devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses bens.

6.8.2. Diretrizes Específicas

6.8.2.1. Sistemas

6.8.2.1.1. Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas por usuários autorizados. O responsável pela autorização deve ser claramente definido e ter registrado a aprovação concedida.

6.8.2.1.2. Cópia de segurança (Backup) deve ser testada e mantida atualizada para fins de recuperação em caso de desastres.

6.8.2.1.3. Não executar programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilidade de serviços.

6.8.2.1.4. Não executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da empresa.

6.8.2.1.5. Não enviar informações confidenciais (autorizadas) para e-mails externos sem proteção. No mínimo, o arquivo deve contar com a proteção de uma senha “robusta”.

6.8.2.2. Máquinas – Estação de Trabalho

6.8.2.2.1. As estações de trabalho, incluindo equipamentos portáteis, e informações devem ser protegidos contra danos ou perdas, bem como o acesso, uso ou exposição indevidos.

6.8.2.2.2. As estações de trabalho possuem códigos internos, os quais permitem que seja identificada na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do funcionário.

6.8.2.2.3. O acesso a estação de trabalho deverá ser encerrado no final do expediente, desligando o equipamento.

6.8.2.2.4. A empresa dispõe de softwares e sistemas implantados capazes de monitorarem o uso da Internet, o acesso a redes de acesso, e-mails, aplicativo da Microsoft Teams, vídeos-chamadas, chamadas de voz, chats e demais aplicativos e extensões, através da rede local e das estações de trabalho da empresa.

6.8.2.2.5. A empresa se reserva no direito de inspecionar, sem a necessidade de aviso prévio, as estações de trabalho, bem como a qualquer arquivo armazenado, que estejam no disco local da estação ou nas áreas privadas da rede, assim como monitorar o volume de tráfego na Internet e na Rede juntamente com os endereços web (http://) visitados, visando assegurar o cumprimento desta política.

6.8.2.2.6. Quando se ausentar da mesa, deverá bloquear a estação de trabalho com senha. Esta ação aplica-se a todos os funcionários com estações de trabalho, incluindo equipamentos portáteis.

6.8.2.2.7. Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo às entidades da Construtora Sudoeste Ltda, só devem ser utilizadas em equipamentos com controles adequados.

6.8.2.2.8. Os usuários (colaboradores internos) devem utilizar apenas softwares licenciados pela Construtora Sudoeste Ltda, nos equipamentos da empresa.

6.8.2.2.9. A área de TI deverá estabelecer os aspectos de controle, distribuição e instalação de softwares utilizados.

6.8.2.3. Boas práticas de segurança para seu notebook

6.8.2.3.1. Quando em deslocamentos de carro, coloque o mesmo no porta-malas ou em local não visível.

6.8.2.3.2. Ao movimentar-se com o notebook, se possível, não utilize malas convencionais para notebook e sim mochilas ou malas discretas.

6.8.2.3.3. Não coloque o notebook em carrinhos de aeroportos ou despache junto à bagagem.

6.8.2.3.4. Em locais públicos (recepção de hotéis, restaurantes e aeroportos dentre outros), mantenha o notebook próximo e sempre à vista, não se distanciando do equipamento.

6.8.2.3.5. Evite utilizar o notebook em locais públicos.

6.8.2.3.6. Nos hotéis, preferencialmente, guarde o notebook no cofre do seu apartamento.

6.8.2.3.7. Avalie se em pequenas viagens é realmente necessário levar o notebook.

DATA CRIAÇÃO	
DATA ATUALIZAÇÃO	
APROVADO POR	

6.8.2.4. Utilização de equipamentos particulares / terceiros dentro da empresa

6.8.2.4.1. Notebooks particulares para serem usados dentro da rede das empresas abrangidas neste documento, se sujeitam a uma avaliação pelo pessoal responsável de TI.

6.8.2.4.2. Equipamentos de terceiros devem ser levados ao suporte para serem verificadas atualização do antivírus e existência de vírus.

6.8.2.4.3. É responsabilidade da área contratante encaminhar os terceiros sob sua responsabilidade para esta verificação.

6.8.2.5. Boas práticas de segurança para Impressões.

6.8.2.5.1. Documento enviado para a impressão deverá ser retirado imediatamente.

6.8.2.5.2. A impressão de documentos sigilosos deve ser feita sob supervisão do responsável. Os relatórios impressos devem ser protegidos contra perda, reprodução e uso não-autorizado. Isto é, documentos esquecidos nas impressoras, ou com demora para retirada, ou até mesmo em cima da mesa, podem ser lidos, copiados ou levados por outro funcionário ou por alguém de fora da empresa.

6.8.2.6. A Instalação de Softwares

6.8.2.6.1. Qualquer software que, por necessidade do serviço, necessitar ser instalado deverá ser comunicado a área de Suporte Técnico da TI, para que o mesmo possa ser homologado pelos responsáveis de TI e só assim serem disponibilizados para a área requerente.

6.8.2.6.2. A empresa respeita os direitos autorais dos softwares que usa e reconhece que deve pagar o justo valor por eles, não recomendando o uso de programas não licenciados nos computadores da empresa. É terminantemente proibido o uso de softwares ilegais (sem licenciamento) na Construtora Sudoeste Ltda.

6.8.2.6.3. A TI poderá valer-se deste instrumento para desinstalar, sem aviso prévio, todo e qualquer softwares em licença de uso, em atendimento à Lei 9.609/98 (Lei do Software).

6.8.2.7. Diretrizes quanto à utilização da Rede Corporativa

6.8.2.7.1. É vedada a navegação web em sites pertencentes às categorias abaixo, bem como a exposição, o armazenamento, a distribuição, a edição, a gravação através do uso dos recursos computacionais e de comunicação da empresa:

a) Material sexualmente explícito e ainda material contrário à moral ou aos bons costumes;

b) Material de conteúdo impróprio, ofensivo, preconceituoso ou discriminatório;

c) Apologia à violência ou ao terrorismo;

d) Apologia às drogas;

e) Violação de direito autoral (pirataria);

f) Execução de quaisquer tipos ou formas de fraudes;

6.8.2.7.2. Somente os colaboradores que estão devidamente autorizados a falar em nome da empresa para os meios de comunicação podem escrever em nome da empresa em sites de Bate-Papo (Chat Room) ou Grupos de Discussão (fóruns, newsgroups). Em caso de dúvidas, procurar a Gerência da área.

6.8.2.7.3. Todos os arquivos devem ser gravados na rede, pois arquivos gravados no computador (local) não possuem cópias de segurança (backup) e podem ser perdidos. O espaço em disco é controlado por departamento, por isso, os usuários devem administrar seus arquivos gravados, excluindo os arquivos desnecessários. Importante citar que não é responsabilidade da área de TI a recuperação de arquivos que não respeitem a regra acima citada.

6.8.2.7.4. Arquivos que estão na rede com mais de 12 meses sem acesso serão copiados em mídias removíveis via Backup específico e excluídos após. Para ter acesso a esses arquivos, é necessário solicitar a TI.

6.8.2.7.5. Não é permitida a gravação de arquivos particulares (músicas, filmes, fotos etc.) nos drivers de rede, pois ocupam espaço comum limitado do departamento.

6.8.2.8. Diretrizes quanto ao uso de Mídias Removíveis e da porta USB

6.8.2.8.1. O uso de mídias removíveis na empresa não é estimulado, devendo ser tratado como exceção à regra.

6.8.2.8.2. A porta USB é o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de informações corporativas confidenciais, neste caso, os modens 3G/4G e os “pen drives” merecem a atenção. Tal vulnerabilidade não pode ser contida com firewalls já que os dispositivos são acoplados aos equipamentos pelos próprios funcionários da empresa.

6.8.2.8.3. Para liberação das portas USB dos desktops e notebooks é necessário justificar o uso e a aprovação da chefia do departamento do solicitante. Para notebooks de gerentes e cargos acima esta liberação é efetuada por padrão.

6.8.2.8.4. Dentro da empresa dê preferência à utilização da rede evitando a utilizando de modem 3G/4G conectado à porta USB do computador, pois é considerada uma forma de burlar a segurança de rede, protegida por Firewall e regras de segurança. Assim o funcionário abre a porta para acesso sem qualquer controle.

DATA CRIAÇÃO	
DATA ATUALIZAÇÃO	
APROVADO POR	

6.8.2.8.5. Os usuários de mídias removíveis são diretamente responsáveis pelos riscos e impactos que o uso de tais dispositivos possa vir a causar nos ativos de informação, pois este tipo de mídia pode conter vírus e softwares maliciosos podendo danificar e corromper dados.

6.8.2.8.6. É vedado aos usuários utilizarem as mídias removíveis como meio preferencial de armazenamento de informações corporativas.

6.8.2.9. Diretrizes quanto ao uso da Internet

6.8.2.9.1. A internet deve ser utilizada para fins corporativos, enriquecimento intelectual ou como ferramenta de busca de informações, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas à empresa.

6.8.2.9.2. O acesso às páginas e web sites é de responsabilidade de cada usuário ficando vedado o acesso a sites com conteúdo impróprios e de relacionamentos.

6.8.2.9.3. O uso da internet para assuntos pessoais deve ser restrito, sem comprometer as atividades dos usuários.

6.8.2.9.4. É vedado qualquer tipo de download. Como também o upload de qualquer software licenciado à empresa ou de dados de propriedade da empresa ou de seus clientes, sem expressa autorização do gerente responsável pelo software ou pelos dados.

6.8.2.9.5. Os acessos à internet serão monitorados através de identificação e autenticação do usuário.

6.8.2.9.6. É vedado o uso da rede para promover competições e para participar de jogos e games em geral, como por exemplo, jogos de poker, jogos de azar, apostas, inclusive os disponibilizados pela Internet (onlines).

6.8.2.9.7. É vedado o acesso a programas de TV na Internet ou qualquer conteúdo sob demanda (*streaming*).

6.8.2.9.8. É proibida a transferência de qualquer tipo de programa, jogo e similares para a rede interna da empresa sem autorização específica do superior hierárquico.

6.8.2.9.9. Sendo do interesse da empresa que os seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços de notícias é visado e aceitável, desde que o seu uso não comprometa o uso do pacote de dados da Banda Larga da rede, nem perturbe o bom andamento dos trabalhos, observados em todos os casos os termos desta política de uso.

6.8.2.9.10. A utilização da Internet para atividades não relacionadas com os negócios da empresa é facultada durante o horário de almoço, ou fora do expediente, desde que dentro das regras de uso definidas nesta política.

6.8.2.10. Recomendações sobre o uso do Correio Eletrônico (E-Mail)

6.8.2.10.1. É vedado o uso de sistemas webmail externo. O uso do correio eletrônico para envio e recepção de e-mail deverá ocorrer apenas através do correio eletrônico da Construtora Sudoeste Ltda.

6.8.2.10.2. É proibido o uso do Correio Eletrônico para envio de mensagens que possam comprometer a imagem da empresa perante seus clientes e a comunidade em geral e que possam causar prejuízo moral e financeiro.

6.8.2.10.3. Evitar utilizar o e-mail da empresa para assuntos pessoais.

6.8.2.10.4. Assegurar a propriedade de todas as mensagens geradas internamente e/ou por meio de recursos de comunicação e definir o uso desses recursos como ferramenta de comunicação e aumento de produtividade, devendo ser usado prioritariamente para atividades de negócio e podendo ser monitorado a qualquer momento por ser propriedade da empresa e até mesmo vistoriado por direitos de verificação e auditoria.

6.8.2.10.5. Não executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Exemplo de extensões que não devem ser abertas: .bat, .exe, .src, .lnk, .mp3, .wav, .com, .sys, .ppt, .mpeg, .avi, .rmvb, .dll e .com, ou de quaisquer outros formatos alertados pela área de TI.

6.8.2.10.6. Não utilizar o e-mail para enviar grande quantidade de mensagens (spam) que possam comprometer a capacidade da rede, não reenviando e-mails do tipo corrente, aviso de vírus, avisos de criança desaparecida, criança doente, materiais preconceituosos ou discriminatórios e os do tipo boatos virtuais etc.

6.8.2.10.7. Utilizar o e-mail para comunicações oficiais internas, as quais não necessitem obrigatoriamente do meio físico escrito. Isto diminui custo com impressão e aumenta a agilidade na entrega e leitura do documento.

6.8.2.10.8. A utilização do e-mail/webmail da empresa fora do horário de trabalho para posições que possuam controle/reporte de jornada deve ser aprovado pelo Diretor da área.

6.8.2.11. Antivírus

6.8.2.11.1. Antivírus dos servidores e estações são atualizados automaticamente.

6.8.2.11.2. A varredura por vírus é feita diariamente nas estações e nos servidores.

6.8.2.12. Uso de Softwares de Mensageria

6.8.2.12.1. Recomenda-se a utilização do Software mensageria como ferramenta de comunicação e aumento de produtividade, devendo ser usado prioritariamente para atividades de negócio e podendo ser monitorado por ser propriedade da empresa e até mesmo vistoriado por direitos de verificação e auditoria.

6.8.2.12.2. A instalação de software de mensageria e a liberação do acesso são restritas e sua utilização deve ser justificada à Gerência e a TI.

6.8.2.12.3. O uso de sistemas de mensageria é aceitável apenas quando for utilizado como ferramenta de produtividade para comunicação online, no exercício de sua função. Enquanto o uso responsável dos sistemas de mensageria é estimulado, o seu abuso deve ser evitado.

6.8.2.12.4. Sistemas de mensageria possuem histórico de riscos associados à malwares (p.ex. vírus, worms, etc), de forma que deve ser utilizado com zelo e cuidado.

6.8.2.12.5. O uso de sistemas de mensageria em redes de relacionamento pessoais deve ser evitado no ambiente corporativo, por conta da natural assincronia das mensagens instantâneas oriundas de terceiros sem finalidades laborais, o que usualmente torna-se contraproducente.

6.8.2.12.6. O grande problema de se utilizar este tipo de software é que, uma vez conectado, o computador fica altamente vulnerável. As portas de entrada/saída ficam abertas, sem qualquer restrição de leitura ou gravação. Desta forma, vírus que exploram esse tipo de vulnerabilidade não encontram empecilhos para se instalarem e iniciarem os processos danosos, não só para aquele dispositivo, mas para todos os que a ele estiverem conectados ou que estiverem em rede.

6.8.2.12.7. Exemplos de softwares de Mensageria: mIRC, Scoop Script, Avalanche, Full Throttle, MSN Messenger, Yahoo Messenger, Skype, Whatsapp, etc.

6.8.2.13. Controle de Acesso a VPN

6.8.2.13.1. O usuário deve restringir o uso do acesso via VPN para as finalidades relacionadas com os negócios devendo abster-se de usar a funcionalidade para quaisquer outras atividades.

6.8.2.13.2. É vetado aos usuários do serviço compartilhar credenciais de acesso via VPN com quem quer que seja, ou de acessar ele próprio o recurso VPN e conceder o uso da sessão a quaisquer outros funcionários.

6.8.2.13.3. O acesso VPN implica em riscos para a rede corporativa, uma vez que com ele é possível acessar à mesma, de forma privilegiada, a partir de qualquer ponto da internet, como se o usuário estivesse fisicamente nas instalações das empresas abrangidas neste procedimento.

6.8.2.13.4. Nunca deixar sessões VPN abertas. Cada vez que o usuário deixar o seu equipamento conectado via VPN, deve executar log-off ou bloquear seu equipamento.

6.8.2.13.5. Manter-se conectado à rede via acesso VPN apenas pelo tempo necessário à execução da tarefa que requereu o uso do serviço.

6.8.2.14. Controle de Acesso Lógico (Baseado em Senhas)

6.8.2.14.1. Todo usuário deve ter uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação. O titular assume a responsabilidade quanto ao sigilo da sua senha pessoal.

6.8.2.14.2. Utilizar senha de qualidade, seguindo os requisitos de complexidade, com pelo menos (8) oito caracteres contendo números, letras (maiúsculas e minúsculas) e caracteres especiais (símbolos), e não deverá utilizar informações pessoais fáceis de serem obtidas como, o nome, o número de telefone ou data de nascimento como senha.

6.8.2.14.3. Utilizar um método próprio para lembrar-se da senha, de modo que ela não precise ser anotada em nenhum local, em hipótese alguma.

6.8.2.14.4. Não incluir senhas em processos automáticos de acesso ao sistema, por exemplo, armazenadas em macros ou teclas de função.

6.8.2.14.5. A distribuição de senhas aos colaboradores (inicial ou não) deve ser feita de forma segura. A senha inicial, quando gerada pelo sistema, deve ser trocada, pelo colaborador no primeiro acesso.

6.8.2.14.6. A troca de uma senha bloqueada só deve ser liberada por solicitação do próprio usuário.

6.9. VIOLAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SANÇÕES

6.9.1. Nos casos em que houver violação desta política, sanções administrativas e/ou legais poderão ser adotadas, sem prévio aviso, podendo culminar com o desligamento e eventuais processos, se aplicáveis.

6.9.2. O funcionário infrator poderá ser notificado e a ocorrência da transgressão imediatamente comunicada ao seu gestor imediato, e à diretoria.

6.10. VIGÊNCIA E VALIDADE

A presente política passa a vigorar a partir da data de sua homologação e publicação, sendo válida por tempo indeterminado.

DATA CRIAÇÃO	
DATA ATUALIZAÇÃO	
APROVADO POR	

Anexo 1

Termo de Responsabilidade

Pelo presente instrumento, eu,_____, matrícula/identidade no _____, perante a CONSTRUTORA SUDOESTE LTDA, na qualidade de usuário dos recursos de processamento da informação da CONSTRUTORA SUDOESTE LTDA, declaro estar ciente e comprometo-me a executar minhas tarefas de forma a cumprir com as orientações da Política de Segurança da Informação composta por suas Diretrizes Gerais, Normas, Procedimentos e Padrões vigentes.

Declaro, também, estar ciente de que os acessos por mim realizados à Internet, bem como o conteúdo das mensagens enviadas através do Correio Eletrônico ou Comunicadores Instantâneos do tipo “InstantMenssagers” corporativo são monitorados automaticamente e podem ser acessados e visualizados a qualquer tempo pela alta direção da CONSTRUTORA SUDOESTE LTDA.

Declaro, ainda, estar ciente das minhas responsabilidades descritas nas normas da Política de Segurança da Informação e que, a não observância desses preceitos, implicará na aplicação das sanções previstas nas Diretrizes desta Política.

Belo Horizonte, _____ de _____de _____.

_____

(Assinatura)

(1a Via com Funcionário) (2a via Departamento Pessoal)

DATA CRIAÇÃO	
DATA ATUALIZAÇÃO	
APROVADO POR	