**POLÍTICA DE SEGURANÇA INFORMÁTICA**

**INTRODUÇÃO**

O documento possui função da organizacional dentro da empresa MOVITEL, responsável por definir, especificar e destacar as principais questões organizacionais dentro da corporação de funcionários, bem como com o comprometimento da Empresa para com seus colaboradores.

A segurança é a pauta mais importante dentre as funcionalidades da Empresa MOVITEL, serão apresentadas, abaixo, normas, instruções, procedimentos que coincidem a melhor actuação em conjunto da equipe de funcionários e dos indivíduos responsáveis pela gestão da organização. Nós, directores da Empresa MOVITEL tratamos com zelo a sua segurança.

**Politica de segurança de informação**

O documento visa falar das instruções que deverão ser seguidas por todo o conjunto corporativo ou colaboradores e funcionários da equipe da empresa, assim como parceiros e os demais prestadores de serviço para a empresa.

A cópia da Política de Segurança da Empresa **MOVITEL**, (a) SR. (a) Compromete-se a colaborar em conjunto com a gestão de Segurança do Trabalho da empresa, respeitando todas as normas e procedimentos aqui estabelecidos, cliente, ademais, de que poderá ser responsabilizado pelo não cumprimento efectivo das regras dispostas neste documento.

A equipe da Segurança encontra-se à disposição para eventuais dúvidas ou questionamentos em torno das disposições estabelecidas nesta política de Segurança, além disso, qualquer adicional ou auxílio técnico a ser sugerido deverão ser encaminhados directamente à equipe, pessoalmente ou pelo e-mail correio electrónico.

**A Política de Segurança da Informação da empresa devera seguir esses pilares a seguir.**

Independentemente do tipo de companhia, a PSI é um aspecto crítico para qualquer empresa ou instituição, não importando o lugar, em sua essência, ela deve abranger três pilares muito importantes, conhecidos como (**Confidencialidade, integridade, disponibilidade**)

#### 1 – Confidencialidade

A confidencialidade diz respeito ao carácter das informações ao ponto que apenas quem tem o direito de acesso àqueles dados poderá utilizá-lo.

Ela impede que informações não autorizadas sejam vistas ou compartilhadas, minimizando o risco de vazamento de dados e preservando a privacidade dos clientes e dos funcionários da empresa.

#### 2 – Integridade

A integridade representa a veracidade das informações de maneira que todos os dados corporativos possam ser considerados confiáveis e íntegros para cada pessoa.

Esse pilar se concentra na protecção das informações contra alterações não autorizadas ou corrupção de dados. A integridade garante que as informações mantenham a integridade, a autenticidade e a precisão, minimizando o risco de fraudes ou erros.

#### 3 – Disponibilidade

A disponibilidade, por sua vez, diz respeito ao perdimento da informação: ela deverá estar disponível a quem dela precisar (dentro das normas de acesso de cada empresa). Como exemplo se o sistema cair, você ainda terá os dados dos clientes? A resposta deverá sempre ser sim.

Isso inclui a implementação de medidas de alta disponibilidade, como clusters de servidores, redundância de sistemas e backup de energia. Além disso, é importante garantir que esse fluxo seja acessível de forma rápida e eficiente, a fim de suportar as operações da organização.

**Consequência da violação das normas empresariais**

O não cumprimento das normas estabelecidas neste documento poderá acarretar em sanções administrativas, resultando, possivelmente, no desligamento do funcionário perante a Empresa **Movitel,** conforme a gravidade da ocorrência e seus devidos desdobramentos com a legislação vigente.

**Política de uso de equipamentos**

Todos os materiais e equipamentos utilizados conforme a necessidade do funcionário são de prioridade da Empresa **Movitel**, assim deverão ser manejados e ocupados de modo a não causar danos aos materiais e às suas funcionalidades.

Os computadores, bem como as máquinas de uso comum utilizam a autentificação dos funcionários por meio de senhas que deverão conter, no mínimo, oito (8) caracteres para a criação de senha, caracteres alfanuméricos, composto por letras e números, visando maior segurabilidade dos equipamentos. Senhas com combinações simples e óbvias deverão ser evitadas, a criação coerente e segura é um meio seguro de acesso aos sistemas de informação da organização.

Não é permitido o uso de qualquer material ou equipamento para fins ilícitos.

**Política de uso dos sistemas da empresa**

Não deverão ser instalados ou manuseados tipos de software/ hardware sem autorização prévia da equipe de tecnologia e informação ou de segurança, ressalvados os sistemas que já venham instalados nos equipamentos e computadores, bem como o próprio sistema de uso da organização.

Não se deve instalar ou manusear músicas, filmes, fotos, aplicativos, softwares sem qualquer direito autoral. Todos os dados correspondentes à empresa deverão ser mantidos e arquivados no servidor que, por meio de backups diários, disponibiliza as documentações aos demais usuários.

Não é permitindo divulgar, compartilhar ou armazenar em tema próprio nenhuma informação confidencial da Empresa para parceiros, ou até, mesmo, parceiros sem autorização prévia.

**Política de relação**

Não pode mencionar ou revelar nossa política de Segurança com terceiros ou em locais públicos, zelando pela confidencialidade dos assuntos empresariais da organização.

Não compartilhar senhas pessoais com ninguém e deve-se manter todas as documentações que estiverem em posse pessoal em local seguro e adequado.

Não aceitar ajuda técnica de qualquer outro colaborador que não seja da equipe técnica da Empresa.

**Política de internet**

O uso recreativo de internet não deve se dar no horário de expediente.

Acesso a sites com conteúdo pornográfico, jogo, bate-papo, apostas, e assemelhados estará bloqueado e monitorado.

O acesso a Internet é permitido para o uso interno a todos os funcionários da Empresa.

**Políticas de vírus e códigos maliciosos**

Manter o antivírus atualizado. A nossa equipe técnica irá se encarregar disso, mas caso perceba que a actualização não esta funcional, entre em contacto com a mesma para que a situação possa ser corrigida.

Não traga disquetes ou CDs de fora da empresa.

**Técnicas de defesa contra ciberataques**

Para a segurança contra ataques cibernéticos deverão ser feitas cópias de segurança, para garantir a disponibilidade da informação.

Redundância de sistemas, para a alta disponibilidade das informações.

Eficácia no controle de acesso, usando mecanismos físicos ou lógicos.

Deve-se usar um mecanismo de controle de tráfego de dados entre computadores de uma rede interna e destes com as outras rede externas usando Firewall.

**Funcionamento de negócio**

Um dos factores muito importante para a nossa empresa é a disponibilidade, pois de nada adianta uma informação segura se a mesma estiver indisponível para quem necessita dela. Por esse motivo nossas equipes técnicas e de segurança contam com a sua colaboração para manter nossa empresa como líder de mercado. Entre sempre em contacto connosco sempre que julgar necessário.

**Aceitação**

Este documento entra em vigor na data de sua assinatura pelas partes e permanece válido por tempo indeterminado ou ate que advenha outros termos que revoguem por acordo mútuo entre partes.

–––––––––––––––––––––––– **–––––––––––––––––––––**

**Assinatura do Funcionário Director da Empresa**

Nampula, 16 de fevereiro de 2013.