**Políticas de segurança da informação**

1. **Introdução:**

Estabelecer as diretrizes, princípios e responsabilidades além de orientar na execução das ações relacionadas ao tratamento das informações e o uso adequado de ativos pelos colaboradores, estagiários, terceiros, fornecedores, parceiros e partes interessadas nos negócios das empresas do grupo SOS Logística e Alugueis. Tal política está baseada em confiabilidade, integridade e disponibilidade, pois tais informações devem sempre estar disponíveis para que for autorizado.

1. **A Empresa e a Política de Segurança:**

A Tecnologia da Informação, TI, está cada dia mais presente nas empresas, mudando radicalmente os hábitos e a maneira de comunicação, sendo de vital importância a definição de normas de segurança que visem disciplinar o uso da tecnologia da informação.

A Política de Segurança da Informação – PSI, conscientizando e definindo as normas e procedimentos necessários para proteger a confidencialidade das informações e a continuidade dos negócios.

A Política de segurança da Informação tem como principal objetivo documentar e proteger as informações consideradas importantes para a continuidade e manutenção dos objetivos de negócio de uma organização, padronizando e estabelecendo requisitos mínimos de segurança.

A **Elaboração de Política de Segurança da Informação** trabalha com um conjunto de controles e mecanismos que garantem a integridade e segurança de uma estrutura de rede na qual exista o trafego de informações e dados comuns e/ou restritos, e nela incluídos os equipamentos que armazenam tais informações.

Garante a proteção das informações entre clientes e empresa nos aspectos de confidencialidade, integridade e disponibilidade.

1. **O Não Comprimento Dessa Política:**

O descumprimento das Normas Regulamentadoras da empresa pode ocasionar inúmeros problemas para empregador e empregado. Poderá ocasionar o desligamento do funcionário da empresa dependendo da gravidade do erro.

**Penalidades**

O descumprimento ou violação, pelo usuário, das regras previstas na Política de Segurança da Informação e Comunicações (PoSIC) poderá resultar na aplicação das sanções previstas em regulamentações internas e legislação em vigor.

O usuário responderá disciplinarmente e/ou civilmente pelo prejuízo que vier a ocasionar a empresa, podendo culminar com o seu desligamento e eventuais processos criminais, se aplicáveis.

1. **Autenticação:**

Em segurança da informação, a autenticação é um processo que busca verificar a Identidade digital do usuário de um sistema, normalmente, no momento em que ele requisita um *log in* (acesso) em um programa ou computador. A autenticação normalmente depende de um ou mais "fatores de autenticação".

**Controle de acesso:**

### **1. Cartões de proximidade**

Os cartões de proximidade são amplamente utilizados em vários estabelecimentos em nosso país. Geralmente, eles possuem as seguintes informações:

* Nome;
* Número de algum documento de identificação único, como o RG;
* Nível do acesso.

Assim, é possível controlar quem entra e quem sai de um local, sempre limitando o acesso de acordo com as funções e as necessidades de seus usuários.

### **2. Biometria**

A biometria é um sistema que utiliza a impressão digital das pessoas para [monitorar a movimentação](http://blog.condlink.com.br/2017/04/02/como-escolher-o-melhor-sistema-de-monitoramento-para-o-condominio/?utm_source=blog&utm_campaign=rc_blogpost) em um estabelecimento ou residência. Em alguns casos, também podem ser utilizados o reconhecimento facial e, até mesmo, de voz.

Além de ter uma fácil instalação, esse tipo de controle de acesso é extremamente seguro, já que os casos de falsificações são raros.

### **3. Portaria remota**

A [portaria remota](http://blog.condlink.com.br/2016/08/22/entenda-como-funciona-a-portaria-remota-e-quais-seus-beneficios/?utm_source=blog&utm_campaign=rc_blogpost) é um tipo de controle de acesso que está revolucionando o mercado. Ela reduz os custos de uma gestão, ao substituir os porteiros de verdade por tecnologias avançadas e inovadoras.

Então, são instaladas câmaras de segurança que enviam suas imagens para uma central de segurança. Com isso, profissionais especializados acompanham a movimentação de pessoas e a sua liberação é dada por dispositivos próprios, radiofrequência ou biometria.

Ao conhecer os tipos de controle de acesso, você pode tomar medidas mais eficientes e assertivas em sua rotina de trabalho, sem se esquecer da segurança e da qualidade em sua prestação de serviço.

1. **Políticas de senhas:**

A senha é a forma mais convencional de identificação e acesso do usuário. Se um terceiro tem acesso a sua senha, ele poderá utilizá-la ilegalmente ou para se passar por você.

Em determinadas corporações, pode existir a chamada 'política de senhas', que tem como regras as seguintes observações:

* Adotamos um padrão de prazo de validade das senhas (60 dias, por exemplo), que obriga o usuário a renovar as suas senhas nesse período;
* Proibindo a repetição de caracteres. Por exemplo, se a senha era '123hut', a próxima senha tem que ter caracteres diferentes, ou pelo menos 60%;
* Obrigar a inserção de quantidade de letras e números. Por exemplo, a senha deve ter 4 números e 4 letras;
* Criar uma lista de senhas que não podem ser utilizadas.

**O que não usar na elaboração de uma senha:**

Nomes, sobrenomes, números de documentos, telefones, placas de carro e datas não devem ser utilizados em senhas, pois são dados que podem ser obtidos com uma certa facilidade e que possivelmente vão ser alvos de tentativa para descobrir a senha do usuário.

Entre as regras de criação de senhas, existe uma regra muito importante que é NÃO utilizar palavras do dicionário como código ('geladeira', por exemplo), pois existem softwares capazes de descobri-las, fazendo combinação e teste de palavras em diversos idiomas.

* Uma boa senha deve ter pelo menos 10 caracteres e deve conter letras, números e símbolos misturados;
* Quanto mais 'diversificada' for a senha, melhor. Misturar letras maiúsculas e minúsculas pode ser uma boa alternativa;
* Conseguir memorizar a senha também é importante;
* Utilizar senhas diferentes para cada local de acesso.
* Certificar-se de que não está sendo observado enquanto utiliza suas senhas;
* Não fornecer a senha a terceiros;
* Não utilizar a senha em computadores de terceiros (Ex.: lan houses, cybercafés, etc.);
* Certificar que o provedor utilizado tem serviços criptografados.

1. **Políticas de e-mail:**

**O propósito dessa política é assegurar o uso apropriado do Sistema de Mensagens Eletrônicas da [Empresa].**

* Todas as mensagens distribuídas pelo sistema da empresa, até e-mails pessoais, são de propriedade da [Empresa].
* Você não deve manter quaisquer expectativas de privacidade sobre quaisquer mensagens que você crie, armazene, envie ou receba através do sistema de e-mail da Empresa.
* Seus e-mails podem ser monitorados sem prévia notificação se [Empresa] assim achar necessário.
* Se existir quaisquer evidências que você não está aderindo às regras citadas nessa política, a empresa se reserva ao direito de tomar medidas disciplinares, incluindo demissão e/ou ação judicial.
* Se você tem alguma dúvida ou comentários sobre essa Política de uso de E-mail, por favor entre em contato com seu supervisor.

**É estritamente proibido:**

* Enviar ou encaminhar e-mails contendo comentários difamatórios, ofensivos, racistas ou obscenos. Se você receber algum e-mail dessa natureza, o envie no mesmo instante para seu supervisor.

* Encaminhar mensagens ou copiar uma mensagem ou anexo pertencente a outro funcionário sem obter primeiro a permissão desta pessoa.
* Enviar Spam ou “correntes”.
* Forjar ou tentar forjar mensagens de e-mail, ou disfarçar ou tentar disfarçar sua identidade quando enviando um e-mail.

**Cuidados necessários**

Os usuários devem ter os mesmos cuidados em escrever um e-mail quanto na escrita de qualquer outro instrumento de comunicação. Informações confidenciais não devem ser enviadas via e-mail, pois eventualmente serão interceptadas.

Para evitar fraudes, recomendamos fortemente que seja utilizada uma identificação digital de segurança ou pelo menos uma assinatura padrão de conhecimento prévio por seus colegas de trabalho, citando seu nome completo e função.

**Uso Pessoal**

* Apesar do sistema de e-mail de e-mail da Empresa ser para assuntos do Negócio, a [Empresa] permite o uso pessoal se isto for necessário e isto não interferir com o trabalho a ser executado.

**Isenção de Responsabilidade (Discai-me)**

Todas as mensagens devem finalizar com a seguinte comunicação de isenção:

**Aviso 1**: *‘Esta mensagem é direcionada apenas para os endereços constantes no cabeçalho inicial. Se você não está listado nos endereços constantes no cabeçalho, pedimos-lhe que desconsidere completamente o conteúdo dessa mensagem e cuja cópia, encaminhamento e/ou execução das ações citadas estão imediatamente anuladas e proibidas’.*

**Aviso 2**: *‘Apesar da [Empresa] tomar todas as precauções razoáveis para assegurar que nenhuma virose esteja presente nesse e-mail, a empresa não poderá aceitar a responsabilidade por quaisquer perdas ou danos causados por esse e-mail ou por seus anexos’.*

1. **Políticas de acesso à Internet:**

**Objetivo da Política:** Deixe claro que a sua intenção é assegurar que a internet seja usada de forma apropriada dentro da empresa, sem oferecer prejuízos à organização e aos seus colaboradores.

**Deveres dos Funcionários:**  
   
• Não utilizar a rede da empresa para quaisquer atividades ilegais, como pirataria, injúrias, pedofilia, etc.  
   
• Não criar nenhum tipo de risco para a empresa, como: acessar sites desconhecidos, baixar e instalar programas de fontes de procedência duvidosa, utilizar dispositivos, como dendrites, para fins que não tenham relação com a empresa, etc.  
   
É terminantemente proibido:  
   
• Acessar páginas de conteúdo pornográfico.  
   
• Utilizar a rede para difamar ou constranger terceiros, sejam eles funcionários ou não da empresa.  
   
• Fazer atividades que permitam a entrada de vírus nos computadores.  
   
• Invadir sites de terceiros.  
   
• Instalar softwares piratas.  
   
• Compartilhar informações confidenciais da empresa com outras pessoas.

**Monitoramento:** Além de criar essa política de controle de acesso à internet, o monitoramento é uma ferramenta que pode garantir que as regras estão sendo seguidas por todos. Entretanto, é fundamental que seja um processo transparente e que todos sejam informados que os acessos feitos pela rede corporativa são monitorados.

Deixe claro para os funcionários que não se trata de uma forma de vigiá-los a todo o momento, mas sim um meio de a empresa se resguardar em casos que possam ser prejudiciais, como queda da produtividade, ataque de hackers e outros problemas.  
   
**Sanções:** Geralmente, as penas padrão são avisos verbais e, se o problema persistir, [**demissão com justa causa**](http://marcusmarques.com.br/colaboradores/dispensa-por-justa-causa-guia-para-colaboradores-e-lideres/).

**Alguns exemplos:**

O descumprimento ou violação, pelo usuário, das regras previstas na Política de Segurança da Informação e Comunicações (PoSIC) poderá resultar na aplicação das sanções previstas em regulamentações internas e legislação em vigor.

O usuário responderá disciplinarmente e/ou civilmente pelo prejuízo que vier a ocasionar a empresa, podendo culminar com o seu desligamento e eventuais processos criminais, se aplicáveis.

1. **Política de Uso de Estação de Trabalho:**

### **Utilização**

* Antes de ausentar-se do seu local de trabalho, o usuário deverá fechar todos os programas acessados e efetuar o logout/logoff da rede ou bloquear do desktop através de senha, evitando, desta maneira, o acesso por pessoas não autorizadas.
* Não deverão ser armazenados arquivos de trabalho nas estações. É obrigatório armazenar os arquivos inerentes a Instituição no servidor de arquivos para garantir o backup dos mesmos.
* O usuário deve ainda fazer manutenção no diretório trabalho, onde devem ser mantidos somente arquivos da Instituição. Não deve haver arquivos do tipo fotos ou vídeos pessoais, músicas, jogos ou arquivos que não dizem respeito ao conteúdo do trabalho.
* A abertura de computadores para qualquer tipo de reparo deverá ser realizada pelo departamento técnico da Instituição.

### **Instalação de Softwares**

* Somente softwares homologados pela Instituição podem ser instalados nas estações de trabalho, o que deve ser feito, com exclusividade, pelo setor de Informática.
* Jogos ou qualquer tipo de software/aplicativo não autorizados não podem ser gravados ou instalados no computador local e em qualquer outro diretório da rede.

1. **Política Social:**

Ajudamos sociedade a realizar seu potencial, respeitando os direitos humanos e o meio ambiente, nos relacionando de forma responsável com as comunidades nos locais onde atuamos e superando os desafios de sustentabilidade relacionados ao nosso negócio.

**Em todas as nossas atividades, nos comprometemos a:**

* Identificar, analisar e tratar os riscos sociais decorrentes da interação entre os nossos negócios, a sociedade e o meio ambiente e fomentar a gestão de aspectos socioambientais na cadeia de fornecedores.
* Integrar as questões relacionadas à Responsabilidade Social na gestão do negócio e no processo decisório da companhia.
* Respeitar os direitos humanos, buscando prevenir e mitigar impactos negativos nas nossas atividades diretas, cadeia de fornecedores e parcerias, e combatendo a discriminação em todas as suas formas.
* Gerir o relacionamento com as comunidades situadas na área de abrangência, com base no diálogo contínuo e transparente, contribuindo para a viabilidade dos nossos negócios e o desenvolvimento local.
* Investir em programas e contribuindo para as comunidades onde atuamos e, de forma ampliada, para a sociedade em alinhamento aos objetivos do negócio.
* Estar preparados para atuar em situações de emergência e em potenciais conflitos e crises junto às comunidades da área de abrangência.
* Comunicar com clareza, objetividade e transparência as informações relativas à nossa atuação em sustentabilidade, alcançando todos os públicos de interesse.
* Contribuir para o desenvolvimento sustentável e para a mitigação da mudança do clima, atuando em alinhamento com os compromissos nacionais e internacionais dos quais somos signatários.
* Promover o pleno conhecimento e o compromisso da força de trabalho com a Política de Responsabilidade Social, para que nossas atividades sejam realizadas de forma socialmente responsável.

1. **Vírus e Códigos maliciosos:**

Programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.

A prevenção e o monitoramento periódico de sistemas são as principais medidas que usamos para nos proteger contra invasões. Para tanto, a mobilização de uma equipe de TI preparada para [traçar planos](https://www.penso.com.br/suporte-de-ti-precisa-de-diagnostico-planejamento-e-estrategia/), acompanhar processos regularmente e para [agir rapidamente](https://www.penso.com.br/qual-a-funcao-do-help-desk/) em momentos de ataque está entre as principais atitudes a serem tomadas.

Outras medidas também ajudam a aumentar a proteção contra-ataques, como a orientação aos funcionários sobre o melhor uso da internet e de equipamentos e sempre um bom antivírus busca por atualização constantes sobre os avanços na área de TI.

1. **Continuidade de Negócios:**

As tarefas que são realizadas no dia-a-dia em ordem a atender e estar sempre saudável, feliz e com retorno financeiro. Nossa empresa tem recursos tangíveis e intangíveis, propriedade intelectual, empregados, computadores, comunicações, links, locais e serviços locais de trabalho. Se qualquer destes recursos é danificado ou feito inacessível por qualquer razão, a empresa pode estar com problemas. Se mais de um destes recursos fica prejudicado a empresa pode sofrer riscos muito altos. Quanto mais tempo estes itens ficam sem uso, mais tempo será necessário para a organização voltar ao seu estado normal. Em determinados casos, algumas empresas não conseguem voltar ao estado normal após um desastre. Entretanto empresas que pensam na frente, planejam para a maioria dos desastres que podem acontecer, e não se arriscar, realizando desta forma um plano de continuidade.

O objetivo de recuperação de desastres é para minimizar os efeitos de um desastre e tomar os passos necessários para certificar que os recursos, pessoal, e os processos de negócios estejam aptos a continuar a operação em pouco tempo na eventualidade de desastres.

A recuperação de desastres é diferente da continuidade de negócios, onde o foco é em manter o negócio funcionando mesmo no caso de um problema, e no caso do último o foco é em voltar ao normal após a falha. Em geral, o foco de recuperação de desastres é mais no ambiente de Tecnologia da Informação.

Um plano de recuperação de desastres é utilizado quando tudo está em modo de emergência, e todos estão focados em retomar todos os sistemas em modo on-line. O plano de continuidade de negócios toma uma linha mais focada no problema. Isso inclui o propósito nos sistemas mais críticos, e leva-los para um ambiente alternativo onde o desastre ocorreu enquanto ocorre a reparação da unidade com problemas. Levando em conta todos os envolvidos na empresa e também os clientes, de uma forma que tudo volte à normalidade o mais breve e seguro possível.

É importante observar que a empresa pode estar muito mais vulnerável depois que ocorre o desastre, porque os sistemas de segurança ficam mais focados na continuidade dos negócios.

Procedimentos pré-planejados permitem a organização:

* Prover um imediato e apropriada resposta a situações de emergência
* Proteger vidas e garantir segurança
* Reduzir impacto aos negócios
* Retornar funções críticas de negócios à normalidade
* Reduzir confusão durante uma crise
* Garantir a sobrevivência do negocio

## Etapas do Plano de Continuidade de Negócios:

* Desenvolver uma política geral de continuidade de negócios: Escrever uma política que entregue e guie os passos necessários para desenvolver o Plano de Continuidade de Negócios, e onde quem assine tenha autoridade para com toda a organização.
* Conduzir uma Análise de Impacto de Negócios: Identificar as funções críticas e sistemas e permitir a organização priorizar dentre estas as suas necessidades reais. Identificar as vulnerabilidades, ameaças e calcular os riscos
* Identificar controles preventivos: Uma vez as ameaças conhecidas, identificar e implementar os controles e paliativos para reduzir o nível de risco da organização em uma maneira econômica.
* Desenvolver estratégias de recuperação: Formular métodos para garantir que sistemas e funções críticas possam ser trazidas de volta ao normal rapidamente.
* Desenvolver um plano de contingência: Escrever os procedimentos para como a organização pode continuar funcionando em caso de um estado crítico.
* Testar o plano e conduzir treinamento e exercícios: Testar o plano para identificar deficiências no Plano de Continuidade de Negócios e também conduzir treinamento para que os indivíduos estejam preparados para cumprir suas tarefas.
* Manter o plano: Efetivar que os passos seguidos garantam que o documento esteja regularmente atualizado.

**Observações Importantes:**

Algumas orientações básicas e necessárias quanto ao acesso às redes sociais e à empresa. Segue abaixo:

* Acesso via biometria à empresa: Todos os setores da empresa
* Marketing e Publicidade: Acesso à rede social, restrito a este setor.
* Facebook, Instagram, youtube
* Contabilidade: Acesso negado à internet
* Recursos Humanos: Acesso à internet, sem, contudo, acessar rede sociais.
* Atendimento: Acesso restrito aos sites de cadastramento
* Diretoria: Acesso irrestrito à internet
* Controle de Pátio: Acesso apenas a sites de informação da empresa e noticiário jornalístico;
* Equipe de TI (Os integrantes do grupo do projeto) -
* Chefe (diretor) e todo aquele que receber ordem para isso.