

1 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA EMPRESA COMERCIAL ITANGUÁ LTDA.

1.1 Introdução

A Política de Segurança, também referida como PSI é um conjunto de diretrizes, normas, procedimentos e instruções do COMERCIAL ITANGUÁ LTDA. para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários.

A presente PSI foi fundamentada de acordo com a norma ABNT NBR ISO/IEC 27002:2005, que é uma referência mundial, relacionada a um código de boas práticas para a gestão da segurança da informação e que está em conformidade com as leis vigentes em nosso país.

1.2 Definições

Os termos abaixo descritos, quando empregados na presente Política de Segurança do Portal do COMERCIAL ITANGUÁ LTDA., terão os seguintes significados:

- Classificam-se como “**visitantes**” todos aqueles que de alguma forma acessam o Portal do COMERCIAL ITANGUÁ LTDA., clientes ou não.
- Classificam-se como “**clientes**” todas pessoas que adquirem os produtos oferecidos pelo Portal do COMERCIAL ITANGUÁ LTDA., pagos ou não.
- Classificam-se como “**usuários**” todas pessoas que se cadastram no Portal do COMERCIAL ITANGUÁ LTDA. e recebem uma identificação individual e exclusiva.
- Entende-se por identificação individual toda informação que não está disponível para o público em geral e é atribuída, personalizadamente, a um determinado cliente/usuário. São exemplos de dados de identificação individual os números de CPF ou RG e dados para contato.
- **Minha conta e Meus pedidos:** Área restrita do site, onde os usuários inserem suas informações cadastrais.
- **Login:** Identificação de um usuário perante o sistema. Normalmente para ter acesso, é preciso digitar sua identificação (login), seguido de sua senha.
- **Senha:** Conjuntos de caracteres, de conhecimento único do usuário, utilizado no processo de verificação de sua identidade, assegurando que ele é realmente quem diz ser.

1.3 Classificação da Informação

1. O gerente da empresa tem o papel e responsabilidade de estabelecer critérios referentes ao nível de confidencialidade da informação.
2. As informações possuem quatro níveis de classificação: Pública, Interna, Restrita e Confidencial.
 - **Pública:** Consiste de toda informação que pode ser acessada por todos os colaboradores da organização, fornecedores, prestadores de serviços e público em geral.

- **Interna:** O uso dessa informação é permitido apenas aos funcionários da organização. É o mais baixo nível de confidencialidade, e é onde existe informações que podem afetar a imagem da organização.
- **Restrita:** O acesso a essas informações é permitido apenas por pessoas indicadas pelo nome. A divulgação não autorizada desta informação pode causar sérios impactos ao negócio e também comprometer possíveis estratégias da organização. Médio nível de confidencialidade.
- **Confidencial:** É a informação que pode ser acessada apenas por pessoal previamente autorizado, geralmente está acessível para alguns usuários da empresa e por parceiros externos. A divulgação de forma não autorizada desta informação pode impactar a organização de forma negativa, sendo o responsável pelo vazamento sujeito às penalidades cabíveis. É o mais alto nível de confidencialidade.

1.4 Princípios

Toda e qualquer informação produzida e/ou recebida como resultado de sua atividade profissional pertence ao COMERCIAL ITANGUÁ LTDA.. Divulgar informações confidenciais é crime previsto em lei (Lei nº 9279). Os equipamentos são utilizados pelos colaboradores para a realização de atividades profissionais. O uso pessoal é permitido desde que não prejudique o desempenho dos sistemas e da empresa.

1.5 A empresa e a PSI

1. É dever de todos os funcionários, parceiros e prestadores de serviços conhecer e seguir as normas estabelecidas neste documento;
2. Ao receber essa cópia da Política de Segurança, o *stakeholder* compromete-se a respeitar todos os tópicos nela abordados e está ciente de que toda e qualquer comunicação estabelecida dentro da empresa é monitorada;
3. Em caso de dúvidas sobre a PSI, procure o setor responsável pela segurança da informação.

1.6 Dados pessoais de Colaboradores e Clientes

Sobre os dados pessoais de *stakeholders* do COMERCIAL ITANGUÁ LTDA. essa política de segurança estabelece que:

1. A empresa se compromete em não acumular ou manter intencionalmente dados pessoais de colaboradores e clientes relacionados ao sistema de que mantém manutenção além daqueles relevantes na condução do seu negócio;
2. Todos os dados pessoais dos colaboradores e clientes serão considerados dados confidenciais;
3. Dados pessoais sob a responsabilidade da empresa não serão usados para fins diferentes daqueles para os quais foram coletados;

1.7 Política de Senhas

1. É recomendado que todas as suas senhas tenham no mínimo de oito dígitos e também contenha números e letras maiúsculas e minúsculas. Deve-se evitar o uso de senhas fracas como: 12345678, 87654321, número do seu telefone ou celular, nome da mãe, etc.
2. Sua senha é pessoal e intransferível.
3. Caso suspeite que alguém está utilizando sua senha ou suspeite que outra pessoa saiba a sua senha, é de sua responsabilidade alterá-la.
4. Será de responsabilidade própria, tudo que for utilizado com a sua senha, por isso tome todos os cuidados para manter o sigilo da mesma.

1.8 Políticas de acesso a Internet

1. O uso recreativo da internet não deverá ocorrer no horário de expediente;
2. É permitida a navegação somente no site relacionado ao contexto de trabalho;
3. A rede da empresa jamais deve ser utilizada para realização de trabalho de terceiros ou de atividades paralelas,
4. Acesso a sites com conteúdo pornográfico, jogos, bate-papo, apostas e afins é terminantemente proibido;
5. É proibido o uso de ferramentas P2P (BitTorrent, μ Torrent, etc);
6. É proibido o uso de *smartphones* não autorizados pela empresa.

1.9 Cópia de segurança (BACKUP) do sistema

Cópias de segurança do sistema integrado são de responsabilidade do nível tático e deverão ser feitas diariamente. Ao final de cada mês também deverá ser feita uma cópia de segurança com os dados de fechamento do mês, do sistema. Esta cópia será feita imediatamente após a comunicação formal do nível estratégico. Nos meses pares, o nível tático enviará 1 (uma) cópia do "backup" de fechamento do referido mês, para ser arquivada.

1.10 Segurança e integridade do Banco de Dados

O gerenciamento do(s) banco(s) de dados é responsabilidade exclusiva do nível tático, assim como a responsabilidade de contatar e contratar uma empresa responsável para fazer manutenção, alteração e atualização de equipamentos e programas, após ser aprovado pelo nível estratégico.

1.11 Responsabilidades do gerente

O gerente é responsável pelas definições dos direitos de acesso de seus funcionários ao sistema e informações do COMERCIAL ITANGUÁ LTDA, cabendo a ele verificar se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos.

1.12 O não cumprimento dessa política:

1.12.1

O não cumprimento desta Política de Segurança da Informação implicará em falta grave e poderá resultar nas seguintes ações:

- Advertência formal;
- Suspensão;
- Rescisão do contrato de trabalho;
- Outra ação disciplinar;
- Processo civil ou criminal;

1.13 Vigência e validade

1.13.1

A presente política passa a vigorar a partir da data de sua homologação e publicação como portaria interna do COMERCIAL ITANGUÁ LTDA. sendo válida por tempo indeterminado.