Pol.001 – Política de Segurança da Informação

SB COMERCIAL

J PINTO DE ANDRADE SOBRINHO & CIA. LTDA
CNPJ 34.542.297/0001-39

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. Objetivo

Estabelecer diretrizes, normas e responsabilidades para garantir a proteção das informações da empresa, assegurando sua confidencialidade, integridade e disponibilidade, bem como a continuidade das operações e a conformidade com requisitos legais e regulatórios.

2. Abrangência

Esta política aplica-se a todos os colaboradores, terceiros, fornecedores e parceiros que tenham acesso às informações e aos sistemas da empresa, independentemente do meio ou local de acesso.

3. Princípios da Segurança da Informação

A segurança da informação será baseada nos seguintes princípios:

- **Confidencialidade:** acesso restrito às informações apenas a pessoas autorizadas.
- **Integridade:** garantia de que as informações não sejam alteradas indevidamente.
- **Disponibilidade:** acesso às informações sempre que necessário para o desempenho das atividades.
- **Autenticidade:** garantia da veracidade das informações e da identidade dos usuários.
- **Conformidade:** atendimento às legislações aplicáveis e normas internas.

4. Classificação da Informação

As informações devem ser classificadas conforme seu nível de sensibilidade:

- **Pública:** pode ser divulgada sem restrições.
- **Interna:** uso exclusivo da empresa.
- **Confidencial:** acesso restrito a grupos específicos.
- **Restrita:** acesso altamente controlado, com impacto significativo em caso de vazamento.

5. Controle de Acesso

- O acesso às informações deve ser concedido conforme a necessidade de trabalho (princípio do menor privilégio).
- Cada usuário deve possuir credenciais individuais e intransferíveis.
- Senhas devem seguir critérios mínimos de segurança (complexidade e periodicidade de troca).
- Acesso de terceiros deve ser controlado e formalmente autorizado.

6. Uso de Recursos Tecnológicos

- Equipamentos e sistemas devem ser utilizados exclusivamente para fins profissionais.
- É proibida a instalação de softwares não autorizados.
- O uso de dispositivos externos (pendrives, HDs) deve ser controlado.
- O acesso à internet deve respeitar as diretrizes corporativas.

7. Proteção de Dados e Informações

- Dados sensíveis, incluindo informações de clientes, fornecedores e processos produtivos, devem ser protegidos contra acessos não autorizados.
- Devem ser realizados backups periódicos das informações críticas.
- Informações impressas devem ser armazenadas de forma segura e descartadas adequadamente.

8. Segurança Física

- Áreas de produção, armazenamento e TI devem possuir controle de acesso físico.
- Visitantes devem ser identificados e acompanhados.
- Equipamentos críticos devem ser protegidos contra danos físicos, furtos ou acessos indevidos.

9. Segurança no Processo Produtivo

- Sistemas utilizados na produção e distribuição de alimentos devem ser protegidos contra falhas e interferências externas.
- Informações relacionadas à rastreabilidade dos alimentos devem ser mantidas íntegras e disponíveis.
- Procedimentos devem garantir a continuidade operacional em caso de incidentes.

10. Gestão de Incidentes de Segurança

- Todo incidente de segurança deve ser reportado imediatamente à área responsável.
- Deve existir um plano de resposta a incidentes com ações definidas.
- Incidentes devem ser registrados, analisados e tratados para evitar recorrências.

11. Treinamento e Conscientização

- Todos os colaboradores devem receber treinamento periódico em segurança da informação.
- A empresa deve promover a cultura de proteção de dados e boas práticas de segurança.

12. Conformidade Legal

- A empresa deve cumprir todas as legislações aplicáveis relacionadas à proteção de dados e segurança da informação.
- Auditorias periódicas devem ser realizadas para garantir conformidade.

13. Responsabilidades

- **Diretoria:** aprovar e apoiar a política.
- **Gestores:** garantir a aplicação das diretrizes em suas áreas.
- **Colaboradores:** cumprir as normas estabelecidas.
- **TI:** implementar e monitorar os controles de segurança.

14. Penalidades

O não cumprimento desta política poderá resultar em medidas disciplinares, conforme normas internas e legislação vigente.

15. Revisão da Política

Esta política deve ser revisada periodicamente ou sempre que houver mudanças significativas nos processos, tecnologias ou requisitos legais.

Data de aprovação:___/____/_____

Responsável: _____

Versão: 1.0