**Plano de Segurança da Informação Projeto integrador – Estoque e Vendas**

**1 - Tratamento de Dados e Informações:**

**1.0 - O Item 1 Consta Sobre Quem tem acesso as Informações do Usuário, e de que forma estas informações são utilizadas.**

**1.1 -** Os Responsáveis pela criação, manutenção e publicação do Projeto “Estoque e Vendas” são:

1 - Denis Alcântara.

2 - Ítalo César.

3 - Guilherme Moura.

**1.2 -** Por meio deste termo, nos afirmamos que, os integrantes do programa listados aqui, bem como terceiros, não poderão ter acesso a dados sigilosos, como CPF, RG, Endereço entre outros dados de caráter sigiloso, tendo a maior parte dos processos sendo realizada de forma automática.

**1.3 -** Somente terão acesso a dados como: Telefone, E-mail ou demais formas de contato disponibilizadas pelo usuário no cadastro apenas para fins comunicativos, ou para resolução de problemas.

**1.4 -** Informações de produtos, Fornecedores, Vendas, Estoque, CNPJ e outros dados referentes as funcionalidades do Projeto “Estoque e Vendas” só poderão ser vistas, editadas e compartilhadas exclusivamente pelo usuário do programa em questão, tendo em vista que para os responsáveis pela criação do programa tenham acesso a estes dados é necessária autorização do usuário, somente em casos de resoluções de problemas.

**1.5 - Cuidado, antes de instalar nosso programa verifique se está adquirindo o serviço original, danos causados por instalação de servidores piratas (vazamento de dados, malwares, entre outros...) não são de nossa responsabilidade.**

**1.6 -** Por fim no item 1.6 presente no item 1 do termo, garantimos que a segurança dos dados disponibilizados pelo usuário ao sistema, não terão influência alguma de terceiros, tendo em vista que apenas os detentores desse projeto poderão utilizar algumas dessas informações para fins comunicativos, como previstas nos itens 1.2,1.3 e 1.4 tendo suas respectivas formas de armazenamento no item 2 (armazenamento de informações).

**2 - Armazenamento de Informações**

**2.0 - O Item 2.0 trata de como são armazenadas as informações disponibilizadas ao sistema pelo usuário.**

**Algumas formas nas quais fazemos o armazenamento das informações, são:**

**2.1** - *Sistema de Versionamento das Informações*

**2.2** - *Backups em Nuvens*

**2.3** - *Pen Drives*

**2.1** - Sistema de Versionamento das Informações: Utilizamos o GIT e o GITHUB para o versionamento delas, tendo o total controle sobre quem e quando os dados foram adicionados e retirados para um disco local.

**2.2 -** Backups em Nuvens: Utilizamos variados tipos de nuvens, com proteção confirmada pela as empresas das mesmas, sendo elas, One Drive, Google Drive e Dropbox, assim conseguimos um ótimo armazenamento dos dados e uma boa segurança.

**2.3 -** Pen Drives: Utilizamos o armazenamento em pen drives, pelo fato deles serem locais, não correndo o risco de perdermos as informações por uma falha nos outros sistemas de armazenamentos. Fazemos o armazenamento no pen drive de semana em semana. O pen drive utilizado não sai da empresa.

**2.4 -** Ao fim do item 2 Garantimos que os dados guardados nos tipos de armazenamento listados nos itens 2.1,2.2 e 2.3 são de extrema segurança, nós nos comprometemos em guardar seguramente todos os dados fornecidos ao nosso sistema (Os quais também foram listados no item 1).

**3 - Comunicação:**

Nosso Projeto Integrador conta com um E-mail para casos de comunicação com os responsáveis pelo sistema. Se houver algum tipo de dúvida, denúncia ou reclamação sobre o sistema, o mesmo deverá ser redirecionado para o nosso e-mail do Projeto Estoque e Vendas.

**Nosso E-mail:** piestoquevendas@gmail.com

**4 – Plano de Contingência:**

**4.0 Introdução: Os responsáveis do programa “Estoque e Vendas”, conhecendo os problemas e incidentes envolvendo Segurança da Informação, tomou como resolução a criação de um Plano de Contingência, para ter o controle, de maneira eficaz, a desastres envolvendo vazamentos de dados etc.**

**4.1 - Objetivo:** Esse Plano de Contingência foi criado com o objetivo de estabelecer procedimentos de comunicação e mobilização para controle e tratamentos de incidentes relacionados à Segurança da Informação, com foco em diminuir os danos e impactos negativos causados por algum desastre ou anomalia nos serviços de Tecnologia da Informação (TI) Em caso de contingências e emergências que possam ocorrer durante as atividades na execução dos serviços de Tecnologia da Informação, o plano de contingência contém os procedimentos de correção e/ou eliminação dos problemas. Para tanto, esse plano deve assegurar que os processos críticos têm seus riscos identificados, avaliados, monitorados e controlados

**4.2 - Identificação:** Para estabelecer um conhecimento dos indevidos problemas à cerca da segurança dos dados e informações do sistema, existem formas de identificá-los, e é isso que essa atividade compreende.

(I) Por problemas reportados pelos usuários, podem ser identificados alertas de segurança que configurem incidentes de segurança. Portanto, esse alerta deverá ser analisado para que sejam tomadas as devidas providências, tanto no tratamento do incidente, quanto no encaminhamento do problema para a gestão;

(II) Essas são algumas das situações que podem ser consideradas na notificação de um evento de Segurança da Informação:

a. Violação da disponibilidade, confidencialidade e integridade da informação;

b. Inconformidade das políticas e/ou procedimentos;

c. Alterações de sistemas sem controle;

d. Funcionamento indevido de software ou hardware;

e. Violação de acesso lógico.

(III) Quaisquer tipos de anomalias devem ser analisadas e validadas rapidamente. Uma vez confirmada a ocorrência de um incidente, então a análise dele deverá ser executada para se obter informações suficientes que permitam identificar o problema.

(IV) os usuários são responsáveis por relatar qualquer tipo de eventos e fragilidades, que possam causar danos à segurança da Informação. A notificação do evento ou fragilidades por parte do usuário deverá ser registrada por e-mail, em caso de algumas suspeitas, enviar para o nosso e-mail do PI: piestoquevendas@gmail.com

**4.3 - Resposta:** Essa atividade compreende as reações que serão tomadas aos possíveis ataques e fragilidades encontradas no sistema.

(I) Logo após a identificação de algum problema no sistema, é importante controlá-lo antes que ele possa comprometer outros recursos.

(II) A estratégia de resposta ao incidente de segurança deverá ser classificada como:

\* Tipo de incidente: (ex: vírus, perda de arquivos, incêndio etc.)

\* Gravidade do incidente: (ex: impacto direto na funcionalidade do sistema, prejuízos com descontos indevidos etc.)

(III) Depois da averiguação do problema, deverá ser realizado uma restauração dos dados, através de um Backup do sistema, que estará guardado em outro dispositivo seguro e longe de situações vulneráveis.

**5 – Regras – Criadores e Colaboradores:**

**5.0 - O Item 3 apresenta todas as regras, nas quais devem ser seguidas de forma totalmente completa, por todos os envolvidos na Criação, Manutenção e Publicação do projeto.**

**5.1 - Os Responsáveis pelo Projeto em questão, não podem se apropriar ou ter acesso a dados sigilosos como: Nome Completo, Idade, CPF, Endereço ou CNPJ, informações estas pertencentes aos usuários como já foram tratadas no presente termo em itens anteriores.**

**5.2 - Fica Restrita o Uso de informações como E-mail e telefone apenas para fins comunicativos, pelos administradores do sistema como também já foi dita no presente termo e firmada como regra, no atual item 3.2.**

**5.3 - É de Total Responsabilidade dos detentores do sistema em questão, casos em que haja vazamentos de dados sigilosos, todavia garantimos que esta situação não irá ocorrer, tendo em vista todas as medidas de segurança adotadas por nós e mostradas através deste termo.**

**5.4 - Pedimos aos usuários do sistema, que em caso de Problemas, bugs ou dúvidas em relação ao sistema ou ao atual termo, entrem em contato conosco por meio das formas de contato disponibilizado no nosso sistema, poderemos lhe atender via WhatsApp ou através do e-mail comercial.**

**6 - Regras Aplicadas ao Usuário:**

**6.0 - Este tópico se refere a regras que devem ser compridas, pelo usuário do programa.**

**6.1 - O Usuário que tiver acesso ao programa não poderá em nenhuma circunstância realizar pirataria, tendo em vista que essa pratica é considerada ilegal, ressaltando que caso haja descumprimento da regra, iremos tomar as devidas medidas perante a lei prevista no artigo 184 do Código Penal.**

**6.2 - É Importante também, que caso haja algum caso de violação de nossos direitos autorais, usuários que pretendem adquirir nossos serviços, confiram se a versão que está instalando é original pelo motivo de que, instalar aplicações de fontes não oficiais, podem ser enquadrados no crime de violação de direitos autorais, bem como medidas cabíveis perante a lei de acordo com o código penal.**

**6.3 - Certifique-se de que apenas o administrador do sistema tenha acesso aos seus dados como E-mail e Senha, dados estes que dão acesso ao sistema de Estoque e Vendas, estas medidas devem ser tomadas para evitar problemas posteriores.**

**6.4 - Sendo assim encerramos o tópico 5 que tratou sobre regras aplicadas ao usuário.**

**\*Tendo em Vista que todos os itens já foram devidamente tratados no termo atual, faremos nossas ultimas considerações:**

**\*Obrigado a Todos que leram, e concordaram com o nosso PSI (Plano de Segurança da Informação) (**Plano de Segurança da Informação) e nos garantimos que trabalharemos para o comprimento total do termo em questão, trabalharemos arduamente para que suas informações se mantenham de forma mais sigilosa possível, sendo assim seja bem-vindo a nosso sistema.